INTRO TO QUANTUM INFORMATION (ECE 493-05 & 579-04)
Rutgers, Fall 2021 **Course Syllabus**

QUANTUM COMPUTING ALGORITHMS

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 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 has created a 10-year federal effort to boosting quantum science. Similar funding commitments have been made throughout the world.

This course provides an introduction to the theory of quantum computing and information. The covered topics include 1) the fundamental elements of quantum information processing (qubits, unitary transformations, density matrices, measurements), 2) entanglement based communications protocols (e.g., teleportation) and games (e.g., CHSH), the Bell inequalities, 3) quantum algorithms such as Shor's factoring and Grover's search, and 4) basic (quantum) error correction algorithms. 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, 3:00 – 4:20 PM, on Zoom

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.

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

Recommended reading:
N. D. Mermin, *Quantum Computer Science: An Introduction,* Cambridge Univ. Press 2007.
J. D. Hidary, *Quantum Computing: An Applied Approach,* Springer 2019.
M. A. Nielsen and I. L. Chuang *Quantum Computation and Quantum Information,* Cambridge 2010.
L. Susskind and A. Friedman, *Quantum Mechanics: The Theoretical Minimum,* Basic Books 2015
J. Preskill, *Lecture Notes for Physics 229: Quantum Information and Computation.*
F. W. Byron and R. W. Fuller, *Mathematics of Classical and Quantum Physics,* Dover 1992.

Grading: (weekly) quizzes 60%, final take-home exam 20%, project 20%.

Remarks on the topics: Many topics outlined above are typical for a quantum information science course at an advanced-undergraduate/graduate level. Such courses have been taught at several universities for many years, at ECE, CS, and Physics departments. The course usually covers selected topics of current interest as well. We encourage students to choose their project topics according to their own (research) interests.
Comparison with the Spring course: Both courses start by providing answers to the three essential questions that any newcomer to quantum computing needs to know: How is quantum information represented? How is quantum information processed? How is classical information extracted from quantum states? The Fall course then covers selected quantum algorithms. After the initial topics, the Spring (systems) course moves to selected topics in quantum computing, communications, and multi-particle systems.

Quantum Computing Algorithms[1]

[1] Rutgers, ECE 579, Fall 2021

Prof. Emina Soljanin

Lecture #1, September 8

This lesson introduces qubits and single qubit gates. It addresses the question how quantum information is represented and processed.

Classical Information and Bits

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. 4. What is the minimum number of yes/no questions you need to ask?

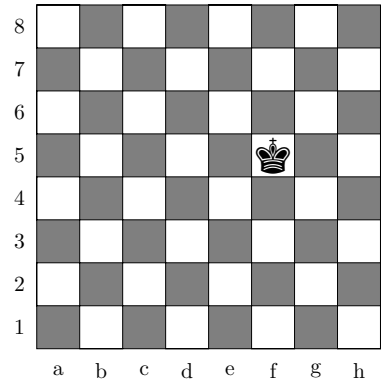


Figure 1: What is the minimum number of yes/no questions that have to be asked to locate the king on a chessboard?

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.

Operations on Bits and Gates

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 2: Binary arithmetics in $\mathbb{F}_2$.

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.

Quantum Information and Qubits

A *qubit* is a quantum information/computing counterpart to a bit. We will treat qubits as mathematical objects as well.[3] What we learn in this class is independent of a particular physical realization.

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

A qubit is represented by a unit-norm vector in a two dimensional complex vector space. 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 $|\alpha|^2 + |\beta|^2 = 1$. Observe that the coefficients α and β depend on the choice of the basis. What would these coefficients be if the basis vectors were

$$|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2} \text{ and } |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$$

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[4]. 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] 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.

Hilbert Space

[5] 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

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

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 ψ 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.

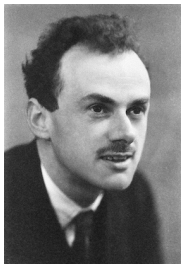


Figure 3: Paul Dirac

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* [6] 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[7]

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

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

[6] $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$
$\implies \langle\varphi| = \alpha^*\langle 0| + \beta^*\langle 1|$

[7] the outer product

Math Interlude - Unitary Matrices

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

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

$U^\dagger$ 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.

Reversible Acting on a Single Qubit

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[8] matrix. Any unitary matrix specifies a valid quantum gate.

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:

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

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

Some Single-Qubit Gates

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

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

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

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

- Pauli matrices:

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

$$|0\rangle \text{ —X— } |1\rangle$$

$$|1\rangle \text{ —X— } |0\rangle$$

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

$$|0\rangle \text{ —Y— } i|1\rangle$$

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

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

$$|0\rangle \text{ —Z— } |0\rangle$$

$$|1\rangle \text{ —Z— } -|1\rangle$$

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.

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

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

for some complex numbers α_I, α_X, α_Y, and α_Z.

Problem Set #1:

1. Show that the single qubit gates defined above are indeed unitary.
2. Express the Hadamard matrix H as a linear combination of of the identity I and the Pauli matrices σ_X, σ_Y, and σ_Z.
3. Verify that that the single qubit gates act on the basis vectors $|0\rangle$ and $|1\rangle$ as stated above.

Mapping the basis states

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

is obtained by matrix multiplication.

Figure 4: Wolfgang Pauli

Quantum Computing Algorithms[1]

Prof. Emina Soljanin

Lecture #2, September 13

[1] Rutgers, ECE 579, Fall 2021

This lecture provides mathematical background necessary to define states of (multiple) qubits and explain how they can be transformed.

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

Consider the set of integers $\mathbb{Z}$:

1. $(\mathbb{Z}, +)$ is an additive group.
2. $(\mathbb{Z}, \cdot)$ is not a group.

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 $v_1, \ldots, v_m$:

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

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[2] of vectors of a basis of V over $\mathbb{F}$.

[2] 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[3] of unitary spaces, known as the Hilbert space. Thus we say that a qubit is an element of a two dimensional Hilbert space.

[3] 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[4]

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

[4] the outer product

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

We have used $|0\rangle$ and $|1\rangle$ 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.

How is Quantum Information Represented?

Representation of quantum information is connected to a postulate of quantum mechanics which says that associated to any isolated physical system is a complex vector space with inner product. In this class, and quantum computing in general, we mostly deal with finite dimensional spaces $\mathbb{C}^N$ and often conventionally refer to them as Hilbert spaces $\mathcal{H}_N$.

The quantum information and computing counterpart to the bit is the *qubit*. Qubits (as bits) are represented by physical systems. Mathematically, independently of a particular physical realization, a qubit is represented by a unit-normvector in the two-dimensional unitary space $\mathbb{C}^2$. 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 $|1\rangle$, that is

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

where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$. Because we can easily normalize any vector to have a unit norm, a quantum state can be thought of as a ray in a Hilbert space. It is an equivalence class of vectors that differ by multiplication by a nonzero scalar.

We can represent a unit norm state $|\psi\rangle$ uniquely as follows:

$$|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle \tag{2}$$

where $0 \leqslant \theta \leqslant \pi$ and $0 \leqslant \phi < 2\pi$. Expression (2) can be visualised through the Bloch sphere representation of quantum states.

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. Rather than a *linear combination*, we say that the quantum state $|\psi\rangle$ above is a superposition of the two basis states. The basis $|0\rangle$, $|1\rangle$ in which the qubit is represented is called the *computational basis*. The superposition is instrumental in enabling quantum computing parallelism and speedup.

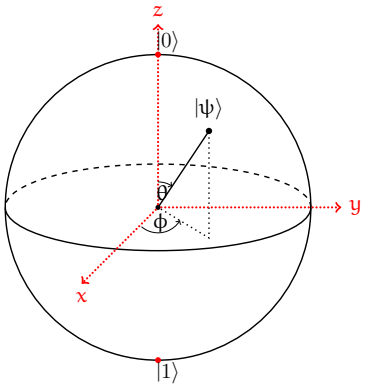


Figure 1: Bloch Sphere: Qubits $|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle$ are the points on the surface.

Quantum Computing Algorithms [1]

Prof. Emina Soljanin

Lecture #3, September 15

[1] Rutgers, ECE 579, Fall 2021

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

Math Interlude

Let A be an $m \times n$ matrix[2] and B a $p \times q$ matrix. The Kronecker product $A \otimes B$ is the $mp \times nq$ matrix given by

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

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

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 is distributive over the Kronecker product:

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

Compare the expressions for the transpose and inverse of the Kronecker product of matrices with their counterparts for the regular product of matrices?

- $A \otimes B$ has the inverse iff both A and B are invertible, and then

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

How is Quantum Information Represented?

Representation of quantum information is connected to a postulate of quantum mechanics which says that associated to any isolated physical system is a complex vector space with inner product. In this class, and quantum computing in general, we mostly deal with finite dimensional spaces $\mathbb{C}^N$ and often conventionally refer to them as Hilbert spaces $\mathcal{H}_N$.

Single Qubit

Mathematically, independently of a particular physical realization, a qubit is represented by a unit-norm[3] vector in the two-dimensional

[3] The norm is induced by the inner product.

unitary space $\mathbb{C}^2$. 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 $|1\rangle$, that is

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

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

Multiple Qubits

Consider following two qubits: $|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ and $|\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$. The joint state of the pair is the Kronecker product of the individual states:

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

where the vectors

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

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

form a basis for $\mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$. In general[4], 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*[5] states.

[4] separable and entangled stats

[5] 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. [6]

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

An n–qubit state $|\phi\rangle$ is a unit-norm vector in $\mathbb{C}^{2^n}$, which we commonly refer to as the Hilbert space $\mathcal{H}_{2^n} = \mathcal{H}_2^{\otimes n} = \underbrace{\mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_2}_{n}$. We will also often use the common notation $N = 2^n$. For an n–qubit state $|\phi\rangle \in \mathcal{H}_{2^n}$, we have

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

where the binary string $i_0 i_1 \dots i_{n-1}$ is the binary representation of i, and $|i_0 i_1 \dots i_{n-1}\rangle$ is a shorthand notation for $|i_0\rangle \otimes |i_1\rangle \otimes \cdots \otimes |i_{n-1}\rangle$ (the i-th basis vector of $\mathcal{H}_{2^n}$). Other commonly used shorthand notation is

$$\begin{aligned} |i_0\rangle \otimes |i_1\rangle \otimes \cdots \otimes |i_{n-1}\rangle &\equiv |i_0\rangle|i_1\rangle \dots |i_{n-1}\rangle \\ &\equiv |i_0, i_1, \dots, i_{n-1}\rangle \\ &\equiv |i_0 i_1 \dots i_{n-1}\rangle. \end{aligned}$$

There is a notion of a *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.

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.

How is Quantum Information Processed?

Processing of quantum information is connected to a postulate of quantum mechanics which says that the evolution of a closed quantum system is described by a unitary[7] transformation. Therefore, in a closed quantum system, a qubit state $|\psi\rangle \in \mathcal{H}$ can be transformed to some other state in $\mathcal{H}$, say $|\varphi\rangle$, only by some unitary operator U, that is,

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

where U is a 2×2 unitary matrix over $\mathbb{C}$. Note that quantum evolution is reversible. 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 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ since the evolution (matrix multiplication) is a linear operation, and thus

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

Unitary action U maps the computational basis $|0\rangle$, $|1\rangle$ into the basis $U|0\rangle$, $U|1\rangle$.

Actions on an n–qubit state are described by $2^n \times 2^n$ unitary matrices, which may or may not be Kronecker products of matrices of smaller dimensions. When $U = U_0 \otimes U_1 \otimes \cdots \otimes U_{n-1}$, where U_i is a 2×2 unitary matrix, then its action on the basis vector $|i_0\rangle \otimes |i_1\rangle \otimes \cdots \otimes |i_{n-1}\rangle \in \mathcal{H}_{2^n}$ is given by

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

Single Qubit Gates

In classical computing, `NOT` is the only single bit gate, that is, in addition to the `I` "gate" (identity). In quantum computing, any 2×2

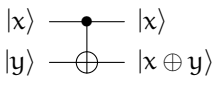
[7] Unitary evolution in a closed quantum system is a consequence of the Schrödinger equation.

unitary matrix specifies a single-qubit gate. The most commonly used single-qubit gates are the Pauli and Hadamard matrices, which we worked with in the previous classes.

Two Qubit Gates

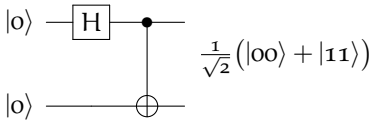
The two-qubit quantum gate known as quantum `XOR` or controlled-not gate `CNOT` is specified as a map and a circuit as follows:

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



An example ...

We can use the Hadamard and the `CNOT` gates to create entanglement:



The No-Cloning Theorem

The requirement that any evolution be unitary gives rise to the famous no-cloning theorem, which asserts that there is no unitary operator U_c on $\mathcal{H} \times \mathcal{H}$ that takes state $|\psi\rangle \otimes |\omega\rangle$ to $|\psi\rangle \otimes |\psi\rangle$ for all states $|\psi\rangle \in \mathcal{H}$ and some fixed state $\omega \in \mathcal{H}$.

To prove the no-cloning theorem, we suppose that there is a unitary matrix U_c such that for two arbitrary sates $|\psi\rangle$ and $|\varphi\rangle$, we have

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

where ω is some fixed 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 $U_c^\dagger \cdot U_c = I$, then by the properties of the Kronecker product, we have

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

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

The no-cloning theorem is often misunderstood to be more restrictive than it is. Note that it does not prohibit the following map:

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

Problem Set#2:

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

2. Show that the `CNOT` gate $|x, y\rangle \rightarrow |x, x \oplus y\rangle$ 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 operator that performs the following map:

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

   You are allowed to use additional fixed-state quantum systems. The operator can be a circuit consisting of gates you have seen in class.

4. Describe each of the following four vectors as linear combinations of either $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$ or $\langle 00|$, $\langle 01|$, $\langle 10|$, and $\langle 11|$:

$$\begin{bmatrix} \alpha \\ \beta \\ 0 \\ 0 \end{bmatrix}, \quad \begin{bmatrix} \alpha \\ \beta \\ 0 \\ 0 \end{bmatrix}^\dagger, \quad \begin{bmatrix} \alpha & \beta & \alpha & \beta \end{bmatrix}, \quad \begin{bmatrix} \alpha & \beta & \alpha & \beta \end{bmatrix}^\dagger, \text{ where } \alpha, \beta \in \mathbb{C}.$$

Introduction to Quantum Information Science [1]

[1] Rutgers, ECE 579, Fall 2021

Prof. Emina Soljanin

Lecture #4, September 20

This lecture reviews projection and Hermitian matrices, and introduces the notion of quantum measurement. We extract classical information from quantum states by measurements.

Math Interlude

Projection Matrices

A square matrix Π is a projection matrix iff $\Pi^2 = \Pi$. Note that a projection is a linear transformation from a vector space to itself. Recall that $|\varphi\rangle\langle\varphi|$ is a matrix. We say that $|\varphi\rangle\langle\varphi|$ is a rank-1 projection matrix. (Higher rank projection matrices project vectors onto subspaces.)

A projection Π on a Hilbert space $\mathcal{H}$ is an orthogonal projection iff it satisfies $\langle \Pi x, y\rangle = \langle x, \Pi y\rangle\langle \Pi x, y\rangle = \langle x, \Pi y\rangle$ for all $x, y \in \mathcal{H}$. Vector $|\varphi\rangle\langle\varphi| \cdot |\psi\rangle$ is the orthogonal[2] projection of vector $|\psi\rangle$ on vector $|\varphi\rangle$.

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

Orthogonal projections on the vectors that form a basis sum to the identity matrix. 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 H is a vector $|v\rangle$ such that

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

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

Hermitian Matrices

A Hermitian matrix H (or self-adjoint matrix) is a complex square matrix that is equal to its own conjugate transpose $H^\dagger$, 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 H is Hermitian if and only if $\langle x|Hx\rangle$ is real for all $|x\rangle$.

[4] Very frequently useful!

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

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

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

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

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

and thus $|u_1\rangle, \ldots, |u_m\rangle$ are eigenvectors of H and $\lambda_1, \ldots, \lambda_m$ are the corresponding eigenvalues. Since $|u_1\rangle, \ldots, |u_m\rangle$ are columns of a unitary matrix, they form a basis of $\mathcal{H}^m$. Therefore,

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

How is Classical Information Extracted?

Extraction of classical information from quantum states is connected to a postulate of quantum mechanics which says that 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 normalized (unit-norm) eigenvectors of its Hermitian matrix.

Quantum Observables

The measurement of an observable H always indicates an eigenvalue of H and turns any measured quantum state into the eigenstate of H corresponding to the indicated eigenvalue. The measured state only gives rise to a probability distribution on the set of outcomes, as we explain next.

Let $\lambda_1, \ldots, \lambda_m$ be the eigenvalues of an $m \times m$ Hermitian matrix H and $|u_1\rangle, \ldots, |u_m\rangle$ be the corresponding eigenvectors. (We assume, for the moment, that all λ_i are different.) Since H is hermitian, we have

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

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

Figure 1: What is the color of the shoe? What is the color of the shoelace?

A set of vectors $|u_1\rangle, \ldots, |u_m\rangle$ that satisfies the above two conditions is said to form a *resolution of the identity*. We refer to $|u_1\rangle, \ldots, |u_m\rangle$ as the measurement basis, and say that we *perform a measurement in the basis* or measure in the basis $|u_1\rangle, \ldots, |u_m\rangle$.

Let $|\psi\rangle$ be a state being measured by the observable described by H. Then the measurement result is λ_i and $|\psi\rangle$ collapses to $|u_i\rangle$ with probability (wp) $|\langle\psi|u_i\rangle|^2$, $1 \leqslant i \leqslant N$, as sketched in Fig. 2.

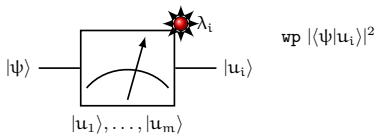


Figure 2: Quantum measurement: The only possible results of "measuring H" are its eigenvalues λ_i, and the only possible states after "measuring H" are its normalized eigenvectors $|u_i\rangle$. When we "see" λ_i (which happens wp $|\langle\psi|u_i\rangle|^2$ when state $|\psi\rangle$ is measured), we know that the state being measured $|\psi\rangle$ has collapsed to $|u_i\rangle$.

Example – Measuements defined by bases: What can we get if we measure qubit $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ in the computational basis $|0\rangle$, $|1\rangle$? What if we use the $|+\rangle$, $|-\rangle$ basis instead?

Example – Measurements defined by Pauli matrices Pauli Matrices are both unitary and Hermitian, and thus can serve to define both quantum gates and quantum measurements. Their eigenvalues with the corresponding eigenvectors are shown in Fig 3.

matrix	action	eigenvalue & eigenvector
$\sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\|0\rangle$ — X — $\|1\rangle$	$+1, \quad (\|0\rangle + \|1\rangle)/\sqrt{2}$
	$\|1\rangle$ — X — $\|0\rangle$	$-1, \quad (\|0\rangle - \|1\rangle)\sqrt{2}$
$\sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$	$\|0\rangle$ — Y — $i\|1\rangle$	$+1, \quad (\|0\rangle + i\|1\rangle)/\sqrt{2}$
	$\|1\rangle$ — Y — $-i\|0\rangle$	$-1, \quad (\|0\rangle - i\|1\rangle)/\sqrt{2}$
$\sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	$\|0\rangle$ — Z — $\|0\rangle$	$+1/\|0\rangle$
	$\|1\rangle$ — Z — $-\|1\rangle$	$-1/\|1\rangle$

Figure 3: Pauli matrices and their eigenvalues with the corresponding normalized eigenvectors.

Mathematical Description of the Quantum Measurement

We have seen above that a measurement on an n–qubit state is defined by a set of $N = 2^n$ basis vectors $|u_i\rangle$, $1 \leqslant i \leqslant N$. When state $|\psi\rangle$ enters the measuring apparatus, it collapses to the state $|u_i\rangle$ wp $|\langle\psi|u_i\rangle|^2$. If we denote by Π_i the rank–1 projection on $|u_i\rangle$, we can equivalently say the the measurement is defined by the set of N orthogonal rank–1 projections $\Pi_i = |u_i\rangle\langle u_i|$ and the measured state $|\psi\rangle$ collapses to $\frac{1}{\sqrt{\langle\psi|\Pi_i|\psi\rangle}}\Pi_i|\psi\rangle$ wp $\langle\psi|\Pi_i|\psi\rangle$. We can now easily generalize our basis defined measurement by removing the requirement that the projections Π_i be rank–1.

Von Neumann Measurement

An observable described by a Hermitian $N \times N$ matrix H may have $m \leqslant N$ different eignvalues. Let Π_i be the projection operator on the eigenspace i of H. The von Neumann projective measurement is defined as follows:

- A set of pairwise orthogonal projection operators $\{\Pi_i\}$ such that $\sum_i \Pi_i = I$.
- For input $|\psi\rangle$, output i happens wp $\langle\psi|\Pi_i|\psi\rangle$, and $|\psi\rangle$ collapses to $\frac{1}{\sqrt{\langle\psi|\Pi_i|\psi\rangle}}\Pi_i|\psi\rangle$.

Positive Operator-Valued Measure (POVM)

We can further generalize the von Neumann measurement of an n–qubit state $|\psi\rangle \in \mathcal{H}_{2^n}$ by observing that we can add an ancillary k–qubit state in $\mathcal{H}_{2^k}$ to $|\psi\rangle$ and perform a von Neumann measurement to the joint state in $\mathcal{H}_{2^n} \otimes \mathcal{H}_{2^k}$. If we restrict our attention[6] to $\mathcal{H}_{2^n}$, the measurement is defined as follows:

- Any set of positive-semidefinite operators $\{E_i\}$ such that $\sum_i E_i = I$.
- For input $|\psi\rangle$, output i happens wp $\langle\psi|E_i|\psi\rangle$, and $|\psi\rangle$ collapses to $\frac{1}{\sqrt{\langle\psi|E_i|\psi\rangle}}\Pi_i|\psi\rangle$.

[6] *Restricting our attention* to a part of the system is a formal mathematical notion, which will define when we learn about bipartite states.

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 4: 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.

Quantum Computing Algorithms [1]

Prof. Emina Soljanin

Lecture #5, September 22

[1] Rutgers, ECE 579, Fall 2021

This lecture reviews quantum measurement theory. It discusses quantum parallelism and introduces a quantum algorithm.

Mathematical Description of the Quantum Measurement

We have seen that a measurement on an n–qubit state is defined by a set of $N = 2^n$ basis vectors $|u_i\rangle$, $1 \leqslant i \leqslant N$. When state $|\psi\rangle$ enters the measuring apparatus, it collapses to the state $|u_i\rangle$ wp $|\langle\psi|u_i\rangle|^2$. If we denote by Π_i the rank–1 projection on $|u_i\rangle$, we can equivalently say the the measurement is defined by the set of N orthogonal rank–1 projections $\Pi_i = |u_i\rangle\langle u_i|$ and the measured state $|\psi\rangle$ collapses to $\frac{1}{\sqrt{\langle\psi|\Pi_i|\psi\rangle}}\Pi_i|\psi\rangle$ wp $\langle\psi|\Pi_i|\psi\rangle$. We can now easily generalize our basis defined measurement by removing the requirement that the projections Π_i be rank–1.

Von Neumann Measurement

An observable described by a Hermitian $N \times N$ matrix H may have $m \leqslant N$ different eignvalues. Let Π_i be the projection operator on the eigenspace i of H, $1 \leqslant i \leqslant m$. The von Neumann projective measurement is defined as follows:

- A set of pairwise orthogonal projection operators $\{\Pi_i\}$ such that $\sum_i \Pi_i = I$.
- For input $|\psi\rangle$, output i happens wp $\langle\psi|\Pi_i|\psi\rangle$, and $|\psi\rangle$ collapses to $\frac{1}{\sqrt{\langle\psi|\Pi_i|\psi\rangle}}\Pi_i|\psi\rangle$.

Von Neumann Measurement - Example

The measurement is defined by the computational basis vectors $|0\rangle$ and $|1\rangle$. The angle between $|\psi_0\rangle$ and $|0\rangle$ is $\pi/12$, and so is the angle between $|\psi_1\rangle$ and $|1\rangle$, as in Fig. 1.

Consider measuring two single-qubit states $|\psi_0\rangle$ and $|\psi_1\rangle$. The angle between these vectors is $2\pi/6$. No matter which state is measured, the resulting state after the measurement is either $|0\rangle$ or $|1\rangle$. If state $|\psi_0\rangle$ is measured, it will collapse either to state $|0\rangle$ with probability $|\langle\psi_0|0\rangle|^2 = \cos^2(\pi/12) = 1/2 + \sqrt{3}/4$ or to state $|1\rangle$ with probability $|\langle\psi_0|1\rangle|^2 = 1 - |\langle\psi_0|0\rangle|^2 = \sin^2(\pi/12) = 1/2 - \sqrt{3}/4$. We can make similar observations when state $|\psi_1\rangle$ is measured.

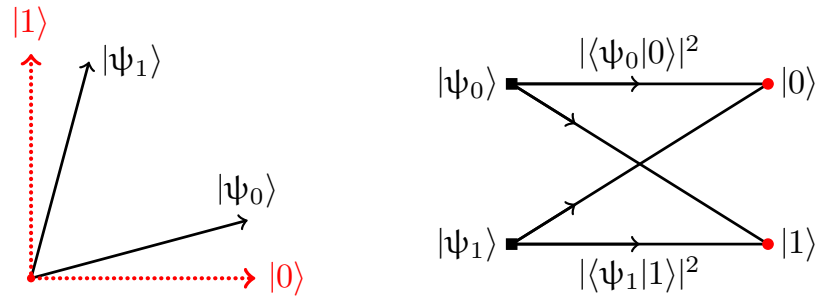


Figure 1: (left) States $|\psi_0\rangle$ and $|\psi_1\rangle$ with the bases $|0\rangle$, $|1\rangle$ used for a von Neumann measurement. (right) The states before and after the measurement with the possible transitions. (Some labels are omitted for clarity of the figure.)

Positive Operator-Valued Measure (POVM)

We can further generalize the von Neumann measurement of an n–qubit state $|\psi\rangle \in \mathcal{H}_{2^n}$ by observing that we can add an ancillary m–qubit state in $\mathcal{H}_{2^m}$ to $|\psi\rangle$ and perform a von Neumann measurement to the joint state in $\mathcal{H}_{2^n} \otimes \mathcal{H}_{2^m}$. If we restrict our attention[2] to $\mathcal{H}_{2^n}$, the measurement is defined as follows:

- Any set of positive-semidefinite operators $\{E_i\}$ such that $\sum_i E_i = I$.
- For input $|\psi\rangle$, output i happens wp $\langle\psi| E_i |\psi\rangle$, and $|\psi\rangle$ collapses to $\frac{1}{\sqrt{\langle\psi|E_i|\psi\rangle}} \Pi_i |\psi\rangle$.

[2] *Restricting our attention* to a part of the system is a formal mathematical notion.

Positive Operator Value Measure (POVM) - Example

The measurement is defined by the projections on vectors $|\varphi_0\rangle$, $|\varphi_1\rangle$, $|\varphi_2\rangle$. The angle between $|\varphi_0\rangle$ and $|\varphi_i\rangle$, $i = 1, 2$, is $2\pi/3$, and it is easy to see that properly normalized projections on these vectors form a resolution of the identity I_2. Vectors $|\psi_0\rangle$ and $|\varphi_1\rangle$ are orthogonal, and so are $|\varphi_0\rangle$ and $|\psi_1\rangle$, as in Fig. 2.

No matter which state is measured, the resulting state after the measurement is one of the states $|\varphi_0\rangle$, $|\varphi_1\rangle$, $|\varphi_2\rangle$. If state $|\psi_0\rangle$ is measured, it will collapse either to state $|\varphi_0\rangle$ with probability $|\langle\psi_0|\varphi_0\rangle|^2 = \cos^2(2\pi/6) = 1/4$ or to state $|\varphi_2\rangle$ with probability $|\langle\psi_0|\varphi_2\rangle|^2 = \cos^2(\pi/6) = 3/4$. Note that the probability of state $|\psi_0\rangle$ collapsing to $|\varphi_1\rangle$ is zero. We can make similar observations when state $|\psi_1\rangle$ is measured.

Measurements Defined by Pauli Matrices

Pauli Matrices are both unitary and Hermitian, and thus can serve to define both quantum gates and quantum measurements. Their eigenvalues with the corresponding eigenvectors are shown in Table 1.

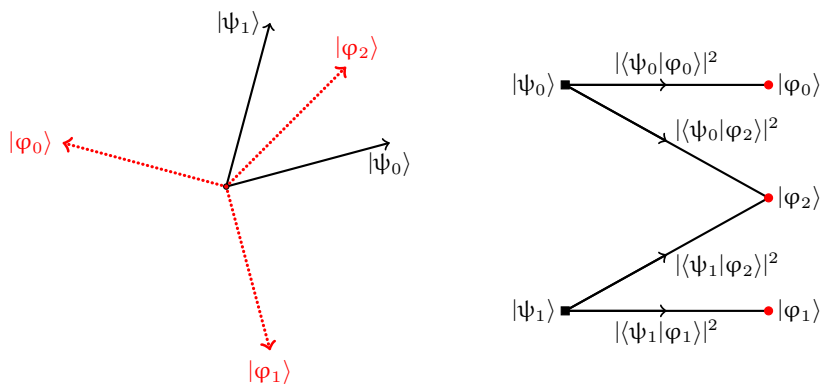


Figure 2: (left) States $|\psi_0\rangle$ and $|\psi_1\rangle$ with the vectors $|\varphi_0\rangle$, $|\varphi_1\rangle$, and $|\varphi_1\rangle$ used for a POVM. (right) The states before and after the measurement with the possible transitions.

matrix	eigenvalus and eigenvectors	
σ_X	$+1,\ (|0\rangle + |1\rangle)/\sqrt{2}$	$-1,\ (|0\rangle - |1\rangle)\sqrt{2}$
σ_Y	$+1,\ (|0\rangle + i|1\rangle)/\sqrt{2}$	$-1,\ (|0\rangle - i|1\rangle)/\sqrt{2}$
σ_Z	$+1,\ |0\rangle$	$-1,\ |1\rangle$

Table 1: Pauli matrices and their eigenvalues with the corresponding normalized eigenvectors.

The Expected Value of a Measurement

Regardless of which state $|\psi\rangle$ is being measured by the observable described by H, the only possible outcomes are the eigenvalues of H. The expected value of the measurement depends on $|\psi\rangle$ as follows:[3]

$$\begin{aligned}\sum_{i=1}^{N} \lambda_i |\langle\psi|u_i\rangle|^2 &= \sum_{i=1}^{N} \lambda_i \langle\psi|u_i\rangle\langle u_i|\psi\rangle \\ &= \langle\psi| \left(\textstyle\sum_{i=1}^{N} \lambda_i |u_i\rangle\langle u_i|\right) |\psi\rangle = \langle\psi| H |\psi\rangle\end{aligned}$$

where we have used the equality $H = \sum_{i=1}^{N} \lambda_i |u_i\rangle\langle u_i|$.

[3] Observe the convenience of the Dirac notation in this simple derivation.

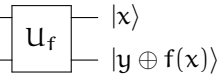
Creating Quantum Parallelism

We can evaluate an m-bit valued function f of an n-bit string by what is known as the *function evaluation gate*. The evaluation gate for a function

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

is described as follows:[4]

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



Note that U_f is a unitary operator acting on vectors in $\mathcal{H}_2^{\otimes n} \otimes \mathcal{H}_2^{\otimes m}$.

[4] U_{CNOT} is a special case of U_f.

We have seen above that the Hadamard gate action on $|0\rangle$ creates a uniform superposition of the computational basis states. It is easy to show that applying the n–qubit Hadamard product gate $H^{\otimes n}$ to $|0\rangle^{\otimes n}$ creates the uniform superposition of the computational basis of $\mathcal{H}_{2^n}$:

$$|0\rangle^{\otimes n} \;\boxed{H^{\otimes n}}\; \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle$$

Quantum function evaluation parallelism is achieved by first creating the uniform superposition of the computational basis of $\mathcal{H}_{2^n}$ and then applying the U_f unitary transform to simultaneously evaluate f on its entire domain, as follows:

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

If we could also simultaneously read all the evaluations (which we cannot), we would achieve a quantum speedup. We will see what is possible in the next section which describes how we can extract classical information from quantum states.

It is natural to wonder whether these probabilistic measurements can be useful. Recall that quantum parallelism allows us to evaluate $f : \{0,1\}^n \to \{0,1\}^m$ on its entire domain (see map (1)). But we have just seen that we cannot simultaneously extract all the values by a single measurement. How is then quantum speedup achieved? Many quantum algorithms prescribe further processing of the state $\frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x, f(x)\rangle$ so that, when a measurement is eventually performed, the probability of getting the answer to the posed question is (close to) 1. Moreover, the questions usually ask about some global property such as whether a function is balanced or constant or what is its period rather than the explicit function evaluation on its entire domain.

The Deutsch Problem

Problem Statement

In the Deutsch Problem, we are concerned with a binary function[5]

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

We know that the function 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.

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

An Algorithm

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

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

We are given a gate U_f, that is, a quantum implementation of the function f such that

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

Applying this function to the current register state $|\psi\rangle$, we obtain

$$\begin{aligned} U_f|\psi\rangle =& \frac{1}{2}\big(|0\rangle(|f(0)\oplus 0\rangle - |f(0)\oplus 1\rangle\big) + \frac{1}{2}|1\rangle\big(|f(1)\oplus 0\rangle - |f(1)\oplus 1\rangle\big) \\ =& \frac{1}{2}\big(|0\rangle(|f(0)\rangle - |\tilde{f}(0)\rangle\big) + |1\rangle\big(|f(1)\rangle - |\tilde{f}(1)\rangle\big) \end{aligned}$$

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

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

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. We also say *we measure the first qubit in the Hadamard basis.*

Quantum Computing Algorithms [1]

[1] Rutgers, ECE 579, Fall 2021

Prof. Emina Soljanin

Lecture #6, September 27

This lecture is about quantum parallelism and the Deutsch-Josza and Brnstain-Vazirani problems.

Creating Quantum Parallelism

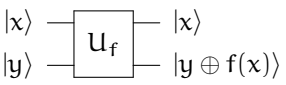
We can evaluate an m-bit valued function f of an n-bit string by what is known as the *function evaluation gate*. The evaluation gate for a function

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

is described as follows:[2]

[2] $U_{\texttt{CNOT}}$ is a special case of U_f.

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



Note that U_f is a unitary operator acting on vectors in $\mathcal{H}_2^{\otimes n} \otimes \mathcal{H}_2^{\otimes m}$.

We have seen above that the Hadamard gate action on $|0\rangle$ creates a uniform superposition of the computational basis states. It is easy to show that applying the n–qubit Hadamard product gate $H^{\otimes n}$ to $|0\rangle^{\otimes n}$ creates the uniform superposition of the computational basis of $\mathcal{H}_{2^n}$:

$$|0\rangle^{\otimes n} \boxed{H^{\otimes n}} \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle$$

Quantum function evaluation parallelism is achieved by first creating the uniform superposition of the computational basis of $\mathcal{H}_{2^n}$ and then applying the U_f unitary transform to simultaneously evaluate f on its entire domain, as follows:

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

If we could also simultaneously read all the evaluations (which we cannot), we would achieve a quantum speedup. We will see what is possible in the next section which describes how we can extract classical information from quantum states.

It is natural to wonder whether these probabilistic measurements can be useful. Recall that quantum parallelism allows us to evaluate $f : \{0,1\}^n \to \{0,1\}^m$ on its entire domain (see map (1)). But we have just seen that we cannot simultaneously extract all the values by a single measurement. How is then quantum speedup achieved? Many quantum algorithms prescribe further processing of the state

$\frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x, f(x)\rangle$ so that, when a measurement is eventually performed, the probability of getting the answer to the posed question is (close to) 1. Moreover, the questions usually ask about some global property such as whether a function is balanced or constant or what is its period rather than the explicit function evaluation on its entire domain.

Examples of n-bit Input & 1-bit Output Functions

- Let $n = 1$. There are only four different function f from $\{0,1\}$ to $\{0,1\}$, as given in the table below.

	$x = 0$	$x = 1$
f_0	0	0
f_1	1	1
f_I	0	1
f_N	1	0

Table 1: The four possible functions from $\{0,1\}$ to $\{0,1\}$.

  Note that each function is is either *constant* (0 on the entire domain as f_0 or 1 on the entire domain as f_1) or *balanced* (1 for half of the domain and 0 for the other half as as f_I and f_N).

- Let $n = 2$. There are 2^4 different functions f from $\{0,1\}^2$ to $\{0,1\}$. Some are listed in the table below. The first two functions listed in the table are constant: f_0 maps each input to 0 and f_1 maps each input to 1. The next three functions f_T, f_P, and f_{xor} are balanced, and the last three are neither constant nor balanced.

	$x = 00$	$x = 01$	$x = 10$	$x = 11$
f_0	0	0	0	0
f_1	1	1	1	1
f_T	0	0	1	1
f_P	0	1	0	1
f_{xor}	0	1	1	0
f_{and}	0	0	0	1
f_{nand}	1	1	1	0
f_{or}	0	1	1	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Table 2: Some possible functions from $\{0,1\}^2$ to $\{0,1\}$.

The Deutsch-Jozsa Problem

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 $\{0,1\}^n$: [3]

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

[3] 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.

Some Useful Observations:

1. For a binary function f, we have

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

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

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

3. Given $z \in \{0,1\}^n$, function $f(x) = z \cdot x$ is balanced unless $z = 0$.

$\implies \frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}(-1)^{z\cdot x} = 0$ when $z \neq 0$.

4. Recall the action of the single-qubit Hadamard gate on the basis vectors:

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

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

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

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

$x \in \{0,1\}$

It is easy to see that $H^{\otimes n}$ creates a uniform superposition of all basis states from the all-zero state.

$|0\rangle^{\otimes n}$ —$H^{\otimes n}$— $\frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}|y\rangle$

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:

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

where $x \cdot y = x_0 y_0 \oplus x_1 y_1 \oplus \cdots \oplus x_{n-1} y_{n-1}$ is the mod 2 sum of the bitwise product.

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

5. Recall the function evaluation gate:

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

$$|x\rangle \longrightarrow \boxed{U_f} \longrightarrow |x\rangle$$
$$|y\rangle \longrightarrow \qquad\quad \longrightarrow |y \oplus f(x)\rangle$$

The Algorithm

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.

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

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

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

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

5. We now can measure $|\psi_3\rangle$ 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.

The Bernstein–Vazirani Problem

Problem Statement

Given an oracle that implements function

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

of the form $f(x) = x \cdot s = x_1 s_1 + x_2 s_2 + \cdots + x_n s_n$, the goal is to find s.

Classical Algorithm

Any classical algorithm has to make n evaluations of $f(x)$, which would provide n equations with n unknowns. The most computationally efficient is to do the following evaluations:

$$\begin{aligned}
f(1000\cdots0) &= s_1 \\
f(0100\cdots0) &= s_2 \\
f(0010\cdots0) &= s_3 \\
&\vdots \\
f(0000\cdots1) &= s_n
\end{aligned}$$

Quantum Algorithm

We use the procedure we used in the Deutsch-Josza problem. Consider state $|\psi_3\rangle$ in step 4. above. We have

$$\begin{aligned}
|\psi_3\rangle &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left[\sum_{x=0}^{2^n-1} (-1)^{f(x)} (-1)^{x\cdot y} \right] |y\rangle \\
&= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left[\sum_{x=0}^{2^n-1} (-1)^{x\cdot(s+y)} \right] |y\rangle \\
&= |s\rangle
\end{aligned}$$

Therefore, we can find s by measuring $|\psi_3\rangle$ in the computational basis.

Quantum Computing Algorithms [1]

[1] Rutgers, ECE 579, Fall 2021

Prof. Emina Soljanin

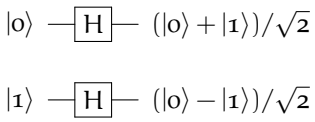
Lecture #7, September 29

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

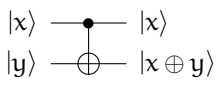
Hadamard gate is a single qubit gate:

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



`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.

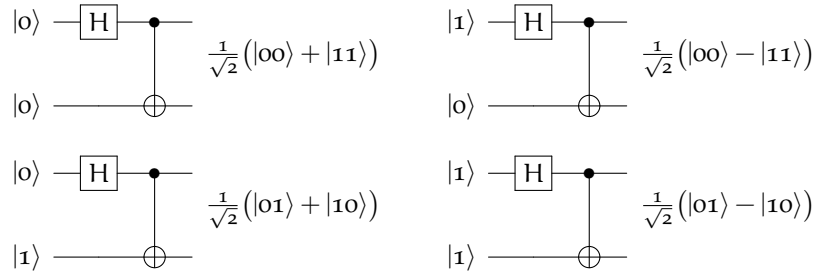


Figure 1: Creating Bell states by a 2-qubit entanglement gate.

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]

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

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.

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

[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

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

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:

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

Note that Alice is able to create 4 orthogonal states.[6] If after per-

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

forming 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 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

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

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

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

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?

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

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

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

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

[8] Is teleportation cloning?

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

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

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

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

   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.

Quantum Computing Algorithms [1]

[1] Rutgers, ECE 579, Fall 2021

Prof. Emina Soljanin

Lecture #8, October 4

This lecture is about the Grover 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,

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

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 know that f is either constant or balanced, and in 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 $1/N$, where $N = 2^n$. 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:

$$1 \cdot \frac{1}{N} + 2 \cdot \frac{1}{N} + \cdots + (N-1) \cdot \frac{1}{N} = \frac{N}{2}.$$

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. Suppose that 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 basis state in the input register can be described by the following unitary operator:[3]

[3] Check this claim as an exercise.

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

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 0:

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

This action results in state $|\psi_1\rangle$.

Grover's Algorithm

1. Perform the "Grover iteration" $\mathcal{O}(\sqrt{N})$ times:
   With the register in state $|\psi_i\rangle$, for $i = 0, 1, \ldots \mathcal{O}(\sqrt{N})$,

   apply the operator U_ω followed by the operator $U_{|\psi_i\rangle}$.

   to get state $|\psi_{i+1}\rangle$.

2. Perform the measurement in the computational basis.

3. Check the result by the oracle.
   If it does not pass the test, repeat the algorithm.

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

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

How do U_ω and $U_{|\psi_0\rangle}$ act on a superposition of basis states $\sum_{x=0}^{N-1} a_x |x\rangle$?

1. U_ω flips the phase of $|\omega\rangle$ and leaves other bases states unchanged.

2. $U_{|\psi_0\rangle}$ inverts the amplitudes a_x around their mean $\mu = \frac{1}{N}\sum_{x=0}^{N-1} a_x$, that is, maps a_x to $2\mu - a_x$.

The amplitude of the element of interest $|\omega\rangle$ has increased from $\langle\omega|\psi_0\rangle = 1/\sqrt{N}$ in the initial state $|\psi_0\rangle$ to $\langle\omega|\psi_1\rangle$ in the end state $|\psi_1\rangle$ after the first iteration. We have

$$\langle\omega|\psi_1\rangle = \tfrac{1}{\sqrt{N}} \cdot \tfrac{N-4}{N} + \tfrac{2}{\sqrt{N}} = \tfrac{1}{\sqrt{N}} \cdot \left(\tfrac{N-4}{N} + 2\right)$$

The amplitudes of any other basis state x after the first iteration is equal to

$$\langle x|\psi_1\rangle = \tfrac{1}{\sqrt{N}} \cdot \tfrac{N-4}{N}, \quad x \neq \omega.$$

Therefore, if we measure $|\psi_1\rangle$ in the computational basis, the most likely outcome is ω. This outcome probability is

$$\tfrac{(3N-4)^2}{N^3} = 9\left(1 - \tfrac{4}{3N}\right)^2 \cdot \tfrac{1}{N}.$$

which is still far from 1.

After $\mathcal{O}(\sqrt{N})$ iterations, the amplitude will be amplified to the value close to 1. A measurement of this state in the computational basis will then be very likely to reveal the state ω.

Grover has shown that a quantum computer can search N items, consulting the search oracle only $\mathcal{O}(\sqrt{N})$ times. Bennett et al. have shown that no quantum algorithm can perform this task by accessing the oracle fewer than $\mathcal{O}(\sqrt{N})$ times. .

Exercise

1. Find an environment to simulate Grover's algorithm, and perform some simulations.

2. Assume $N = 32$ and derive three Grover's iterations.

Quantum Computing Algorithms [1]

[1] Rutgers, ECE 579, Fall 2021

Prof. Emina Soljanin

Lecture #9, October 6

This lecture describes Simon's period finding problem.

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 task 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 $x = y$.

	$x = 00$	$x = 01$	$x = 10$	$x = 11$
f_1	00	00	00	00
f_2	00	01	10	11
f_3	00	00	01	01
f_4	01	10	11	00
f_5	00	01	01	00
f_6	00	00	00	11
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Table 1: Some functions from $\{0,1\}^2$ to $\{0,1\}^2$.

Classical Solution

If we check $2^{n/2} + 1$ different inputs, we will know a. Even if we use randomness and accept a small probability of error, we would need to $\Omega(\sqrt{2^n})$ different inputs before being likely to find a pair for which F gives identical outputs.[3]

[3] A *birthday problem* argument.

Simon's Algorithm

The algorithm has a quantum and a classical part.

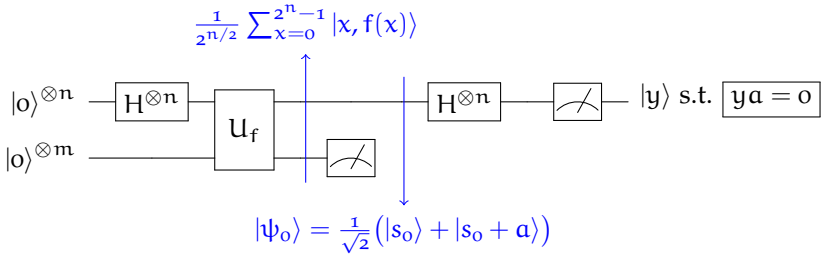


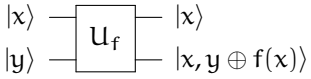
Figure 1: This is the quantum part of the algorithm. See the sections below for more detail.

Parallel Function Evaluation

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

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

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



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:[4]

[4] But can we see the result?

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

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

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

We next apply the Hadamard transform[5] on $|\psi_0\rangle$ and get $|\psi_1\rangle$:

[5] Recall that

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

$x \cdot y = x_0 y_0 \oplus x_1 y_1 \oplus \cdots \oplus x_{n-1} y_{n-1}$

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

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).[6]

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[7] by repeating the above procedure a a few times, and getting linearly independent[8] 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

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

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. Recall that a classical algorithm would have to make $\Omega(2^{n/2})$ calls to f.

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.

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

[7] requires proof

[8] Check for linear independence classically!

Quantum Computing Algorithms [1]

Prof. Emina Soljanin

Lecture #10, October 11

[1] Rutgers, ECE 579, Fall 2021

This lecture is about the measurements in the classical penny weighing problem.

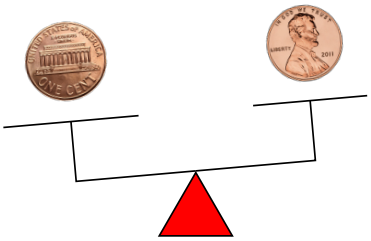


Figure 1: How would you use a balance scale to determine which of the 8 pennies has a different weight?

The Problem and the Algorithm

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[2] is given in Table 1. 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.

[2] 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 1: 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. 2.

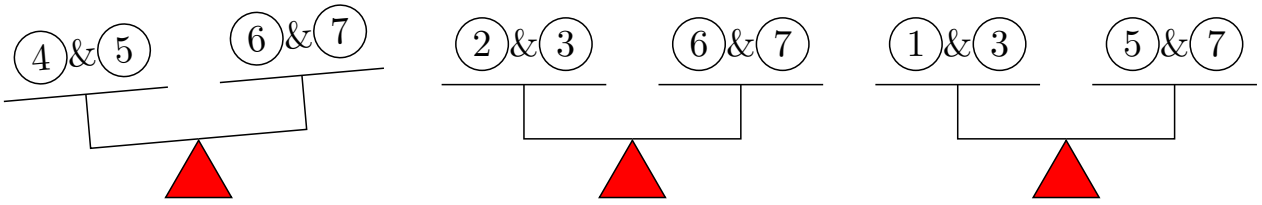


Figure 2: An example of measurement outcomes. Which penny has different weight?

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 2. 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 2: 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. 1. 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*[3] 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. 3, and you can only use the left tray to place pennies?

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

Problems

1. Suppose you have a balance scale and 3 pennies. You know that the pennies are either all genuine or exactly one is fake (has different weight). Describe two measurements that would allow you to find out which penny is fake, if any.

2. Suppose you have a balance scale as in Fig. 1. 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. 3. How many measurements would you need *on average* to find the single penny that does not have the unit weight? [4]

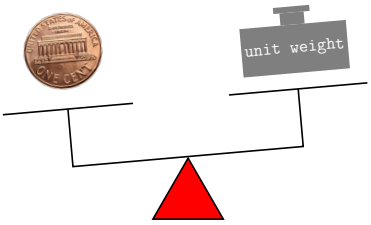


Figure 3: In this scale, there is some unit weight fixed to the right tray.

[4] We have seen such "measuring scales" when we studied Grover's quantum search algorithm.

Quantum Computing Algorithms [1]

Prof. Emina Soljanin

Lecture #11, October 13

[1] Rutgers, ECE 579, Fall 2021

This lecture introduces classical and quantum error correcting codes. Codes play indispensable roles in numerous scientific disciplines and virtually all telecommunications and computing systems. Today, we even ask if the space and timecould be a quantum error-correcting code.

Error correcting codes add redundancy to data in order to make it less sensitive to errors. The most basic form of redundancy is simple replication (cloning), 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, after first finding out (measuring) what the value of the majority is. But could there be a counterpart to this process in the quantum world where the no-cloning theorem holds and the measurements disturb the states?[2] We will first 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.

[2] *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.

A Classical Error Correcting Code

- Encoding is a map that introduces redundancy. In our 1-to-3 bits repetition code example, each bit x is mapped to a 3-bit string (codeward) $x\,x\,x$, that is, the encoding is the following map:

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

- Decoding is the inverse map of the encoding. It removes the redundancy by the encoder. In this example, decoding reduces to keeping the first bit of the 3-bit codeward.

- Error Model: In this example, 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 $y_0\,y_1\,y_2$:

additive 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: We perform the following matrix vector multiplication (cf. two measurements):

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

  We refer to the vector on the right-hand side in the above equation as the *error syndrome*. Observe that the first bit of the syndrome tells us if whether bits y_0 and y_1 have identical values and the second bit of the syndrome tells us if whether bits y_0 and y_2 have identical values.

- Error Correction: The 2-bit measurement result (syndrome bits $y_0 \oplus y_1$, $y_0 \oplus y_2$) tells us which bit is flipped, and thus instructs 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

  The error is corrected by adding the string in the last column to the received word.

A Quantum Error Correcting Code

Quantum error correction has to follow the laws of quantum mechanics. Therefore all actions on qubits (encoding, errors, decoding) have to be either unitary or measurements. We describe the simplest code only to show that quantum error correction under these constraints is feasible, and possibly make the reader interested in this fascinating subject. [3]

Building scalable quantum computers will require not only further research in quantum information processing, but also further research in many relevant classical fields. Error correcting codes will be an indispensable part of any quantum system regardless of its physical qubit realization. However, errors are realization-specific, and thus will require tailored as well as multi-purpose error correction, which will have to be done in both classical and quantum domain.

[3] *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.

- 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:

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

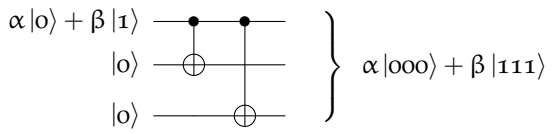


Figure 1: Quantum circuit that maps $(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle \otimes |0\rangle$ to $\alpha|000\rangle + \beta|111\rangle$.

The unitary map circuit shown in Fig. 1 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.

- Decoding is the inverse map of the encoding, as in the classical case. How does a unitary map circuit that reverses the action shown in Fig. 1 look like?
- Error Model: We assume that at most one qubit experiences the basis flip (i.e., is acted on by σ_X). The possible 3-qubit error operators and the resulting states they give when acting on $\alpha|000\rangle + \beta|111\rangle$ are 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: As in the classical case, the idea is to have two measurements such that one compares qubits 1 and 2, and the other compares qubits 1 and 3. The additional constraint here is that the measuring process leave the measured states unchanged. We perform the following two measurements:

  $\boxed{M_1}$: This measurement is defined by the Hermitian operator $\sigma_Z \otimes \sigma_Z \otimes I$, i.e., the following two orthogonal projection operators:

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

  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.

  $\boxed{M_2}$: This measurement is defined by the Hermitian operator $\sigma_Z \otimes I \otimes \sigma_Z$, i.e., the following two orthogonal projection operators:

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

  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 measurements are two eigenvalues (M_1 and M_2 in the table below). 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	$I \otimes I \otimes \sigma_X$

  The error is corrected by applying the unitary operator in the last column to the three received qubits.

Remark: The error detecting and correcting procedure we used 1) follows directly from classical error correction and 2) it 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 von Neumann measurement defined by the following set of projectors:

$$\Pi_0 = |000\rangle\langle 000| + |111\rangle\langle 111| \quad \text{no error}$$
$$\Pi_1 = |100\rangle\langle 100| + |011\rangle\langle 011| \quad \text{bit flip on qubit one}$$
$$\Pi_2 = |010\rangle\langle 010| + |101\rangle\langle 101| \quad \text{bit flip on qubit two}$$
$$\Pi_3 = |001\rangle\langle 001| + |110\rangle\langle 110| \quad \text{bit flip on qubit three}$$

The result of the measurement M (error syndrome) takes values in the set $\{0, 1, 2, 3\}$ corresponding to the four projectors. A measurement result different than 0 means that an error has been detected. Errors are corrected based on the measurement result as follows:

corrupted state	M	apply
$\alpha\|000\rangle + \beta\|111\rangle$	0	$I \otimes I \otimes I$
$\alpha\|100\rangle + \beta\|011\rangle$	1	$\sigma_X \otimes I \otimes I$
$\alpha\|010\rangle + \beta\|101\rangle$	2	$I \otimes \sigma_X \otimes I$
$\alpha\|001\rangle + \beta\|110\rangle$	3	$I \otimes I \otimes \sigma_X$

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.

As their classical counterparts, decoders of quantum error correcting codes can miss-correct or not-detect certain errors. For example, the decoder above will miss-correct the two-qubit error introduced by the operator $\sigma_X \otimes \sigma_X \otimes I$, and it will not detect three-qubit error $\sigma_X \otimes \sigma_X \otimes \sigma_X$ and even a single-qubit error $\sigma_Z \otimes I \otimes I$.

Quantum Computing Algorithms [1]

[1] Rutgers, ECE 579, Fall 2021

Prof. Emina Soljanin

Lecture #12, October 18

This lecture uncovers a little more about quantum error correction.

Consider again the code that maps a single-qubit state into a 3-qubit state as follows:

$$\alpha\,|0\rangle + \beta\,|1\rangle \to \alpha\,|000\rangle + \beta\,|111\rangle$$

Recall that this code corrects single σ_X errors[2] that can be identified by e.g., the von Neumann measurement defined by the following set of projectors:

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

[2]

$$\Pi_0 = |000\rangle\langle 000| + |111\rangle\langle 111| \quad \text{no error}$$
$$\Pi_1 = |100\rangle\langle 100| + |011\rangle\langle 011| \quad \text{bit flip on qubit one}$$
$$\Pi_2 = |010\rangle\langle 010| + |101\rangle\langle 101| \quad \text{bit flip on qubit two}$$
$$\Pi_3 = |001\rangle\langle 001| + |110\rangle\langle 110| \quad \text{bit flip on qubit three}$$

We need to know which errors are possible before we design a code.

Correcting Phase Flips

When the error operator $E = \sigma_Z \otimes I \otimes I$ acts on the encoded state $|\psi\rangle$, the result is the corrupted state $|\varphi\rangle$:

$$E(\underbrace{\alpha|000\rangle + \beta|111\rangle}_{|\psi\rangle}) = \underbrace{\alpha|000\rangle - \beta|111\rangle}_{|\varphi\rangle}.$$

Observe that both $|\psi\rangle$ and $|\varphi\rangle = E|\psi\rangle$ belong to the subspace of $\mathbb{C}^8$ spanned by $|000\rangle$ and $|111\rangle$, and are, in general, not orthogonal.[3]

[3] Is there a quantum measurement that can distinguish between $|\psi\rangle$ and $|\varphi\rangle$, that is, error and no-error?

Consider the code that maps one information qubit (and some ancillary qubits) into three encoded qubits by the encoder shown in Fig. 1.

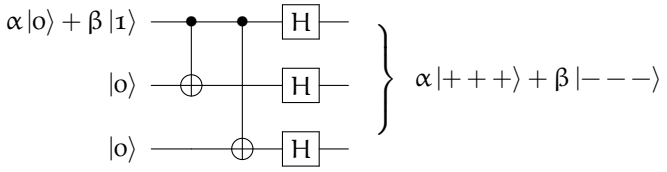


Figure 1: Quantum circuit that maps $(\alpha\,|0\rangle + \beta\,|1\rangle) \otimes |0\rangle \otimes |0\rangle$ to $\alpha|+++\rangle + \beta|---\rangle$.

Note that the basis vectors are mapped as follows:

$$\begin{aligned} |0\rangle &\to \big((|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)\big)/2\sqrt{2} \\ |1\rangle &\to \big((|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle)\big)/2\sqrt{2} \end{aligned}$$

Show that this code correct single σ_Z (phase) errors but not single σ_X errors (bit flips).

Correcting Both Bit and Phase Flips

We can correct both bit and phase flips, if we first encode the qubit using the phase flip code into three qubits, and then encode each of these three qubits using the bit flip code.[4] This code maps one information qubit (and some ancillary qubits) into nine encoded qubits as follows:

[4] This code is known as Shor's Code.

$$\begin{aligned} |0\rangle &\rightarrow (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \\ |1\rangle &\rightarrow (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \end{aligned}$$

We can use the measurements defined by the following observables to learn about the error syndrome, and make error corrections accordingly.

$$\begin{aligned} &(\sigma_Z \otimes \sigma_Z \otimes I) \otimes (I \otimes I \otimes I) \otimes (I \otimes I \otimes I) \\ &(\sigma_Z \otimes I \otimes \sigma_Z) \otimes (I \otimes I \otimes I) \otimes (I \otimes I \otimes I) \end{aligned}$$

$$\begin{aligned} &(I \otimes I \otimes I) \otimes (\sigma_Z \otimes \sigma_Z \otimes I) \otimes (I \otimes I \otimes I) \\ &(I \otimes I \otimes I) \otimes (\sigma_Z \otimes I \otimes \sigma_Z) \otimes (I \otimes I \otimes I) \end{aligned}$$

$$\begin{aligned} &(I \otimes I \otimes I) \otimes (I \otimes I \otimes I) \otimes (\sigma_Z \otimes \sigma_Z \otimes I) \\ &(I \otimes I \otimes I) \otimes (I \otimes I \otimes I) \otimes (\sigma_Z \otimes I \otimes \sigma_Z) \end{aligned}$$

$$\begin{aligned} &(\sigma_X \otimes \sigma_X \otimes \sigma_X) \otimes (\sigma_X \otimes \sigma_X \otimes \sigma_X) \otimes (I \otimes I \otimes I) \\ &(I \otimes I \otimes I) \otimes (\sigma_X \otimes \sigma_X \otimes \sigma_X) \otimes (\sigma_X \otimes \sigma_X \otimes \sigma_X) \end{aligned}$$

Quantum Computing Algorithms [1]

[1] Rutgers, ECE 579, Fall 2021

Prof. Emina Soljanin

Lecture #13, October 20

This lecture uncovers a little more about quantum error correction.

Consider again the code that maps a single-qubit state into a 3-qubit state as follows:

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

If σ_X operator acts to at most one qubit, the possible resulting states are given in the following table:

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

Observe that the four possible resulting states are orthogonal. Which state the system is in (and thus the error) can be unambiguously determined by the von Neumann measurement defined by the following set of projectors:[2]

[2] This measurement does not disturb the state. It only identifies the error that has happened.

$$\Pi_0 = |000\rangle\langle 000| + |111\rangle\langle 111| \quad \text{no error}$$
$$\Pi_1 = |100\rangle\langle 100| + |011\rangle\langle 011| \quad \text{bit flip on qubit one}$$
$$\Pi_2 = |010\rangle\langle 010| + |101\rangle\langle 101| \quad \text{bit flip on qubit two}$$
$$\Pi_3 = |001\rangle\langle 001| + |110\rangle\langle 110| \quad \text{bit flip on qubit three}$$

If σ_Z operator acts to at most one qubit, the possible resulting states are given in the following table:

error operators	resulting state
$I \otimes I \otimes I$	$\alpha\|000\rangle + \beta\|111\rangle$
$\sigma_Z \otimes I \otimes I$	$\alpha\|000\rangle - \beta\|111\rangle$
$I \otimes \sigma_Z \otimes I$	$\alpha\|000\rangle - \beta\|111\rangle$
$I \otimes I \otimes \sigma_Z$	$\alpha\|000\rangle - \beta\|111\rangle$

Observe that the three error states are identical and not orthogonal to the no-error state. Therefore, no measurement can identify the error; not even unambiguously determine whether there was an error ot not.

Quantum and Classical Error Correcting Codes

An $[n, k]_q$ classical linear error correcting code (ECC) is a k dimensional subspace $\mathcal{C}$ of $\mathbb{F}_q^n$. The encoder for an $[n, k]_q$ linear code is a linear map $\mathbb{F}_q^k \to \mathbb{F}_q^n$, which maps k bit-strings (data words, information words) into n-bit strings (codewords).

A quantum error-correcting encoder maps k data qubits and $n - k$ ancillary qubits into n qubits.[3] To describe the encoder, it is sufficient to specify how each of the 2^k basis states of $\mathbb{C}^{2^k}$ ()together with the ancillary states) is mapped to $\mathbb{C}^{2^k}$. A quantum error-correcting code is a 2^k dimensional subspace $\mathcal{C}$ of the 2^n-dimensional Hilbert space.

[3] The encoder is a unitary map that acts on an n-qubit register.

Requirements for Error Correction

For a classical ECC, errors $\boldsymbol{e}_p$ and $\boldsymbol{e}_q$ are both correctable if and only if they send different codewords into different bit-strings, that is,

$$(\mathbf{c}_i \oplus \boldsymbol{e}_p) \oplus (\mathbf{c}_j \oplus \boldsymbol{e}_q) \neq 0$$

for all codewords $\mathbf{c}_i$ and $\mathbf{c}_j$.

For a quantum error correcting code (QECC), we consider P, a $2^n \times 2^n$ projector onto the code subspace $\mathcal{C}$ and the basis vectors of $|i\rangle$ of $\mathcal{C}$. Errors E and F are correctable if and only if the following holds:

1. We can distinguish error events from no-error events, that is,

$$\langle\psi| \cdot E |\psi\rangle = 0 \quad \text{for all} \quad |\psi\rangle \in \mathcal{C}.$$

2. We can distinguish error E from any other error F,[4] that is,

$$\langle i| E^\dagger \cdot F |j\rangle = 0$$

for all basis states $|i\rangle$ and $|j\rangle$ (including $i = j$). Note that if we include the identity (no error) as a possibility for E or F, we obtain the first condition above.

[4] Otherwise, we may attempt to correct error E when error F occurred.

We have assumed that both error and correction operators are unitary. In a more general setting, the above correctable-error conditions become the Knill-Laflame conditions.

Correcting Errors described by Kronecker Products of Pauli Matrices

Why is it important to be able to correct errors described by Kronecker products of Pauli matrices? If a QECC corrects errors E and F, it also corrects any linear combination of E and F. Recall that σ_X, σ_Y, σ_Z, and I span the space of 2×2 matrices, and matrices $E_0 \otimes \cdots \otimes E_{n-1}$, $E_i \in \{I, \sigma_X, \sigma_Y, \sigma_Z\}$, span the space of $2^n \times 2^n$ matrices.

The Stabilizer Codes – A General Class of QECCs

One way to ensure that the conditions we listed above for quantum error correction hold is to have code $\mathcal{C}$ lie in the +1-eigenspace of some operator M:

$$\mathcal{C} = \{|\psi\rangle : M|\psi\rangle = |\psi\rangle\}$$

Note that if errors E and F anticommute[5] with M, then EF will take states from the +1-eigenspace of M to the -1-eigenspace of M, which is orthogonal to the +1-eigenspace, that is,

[5] Matrices A and B anticommute if $AB = -BA$.

$$\langle i|EF|j\rangle = \langle i|EF \cdot M|j\rangle = -\langle i|M \cdot EF|j\rangle = -\langle i|EF|j\rangle$$
$$\implies \langle i|EF|j\rangle = 0.$$

It is convenient to pick M to be a Kronecker product of the Pauli matrices, because then other products of Pauli matrices[6] will always either commute or anticommute with M. By choosing our QECC $\mathcal{C}$ to be in the +1-eigenspace of enough such operators,[7] we can make sure that EF anticommutes with one of the M's for any pair of E and F. The set of such operators is called the *stabilizer* of the code.

[6] the errors we want to correct

[7] $\implies$ the operators must commute with each other.

Example: A one-to-five qubit QECC that corrects one general error[8] has the following stabilizer:

[8] The highest rate such code.

$$M_1 = X \otimes Z \otimes Z \otimes X \otimes I$$
$$M_2 = I \otimes X \otimes Z \otimes Z \otimes X$$
$$M_3 = X \otimes I \otimes X \otimes Z \otimes Z$$
$$M_4 = Z \otimes X \otimes I \otimes X \otimes Z$$

Not all codes can be described by a stabilizer.

Outline of a Formal Definition – Advanced

- $\mathcal{G}_n$: the group of $2^n \times 2^n$ matrices of the form

  $$U = U_0 \otimes U_1 \otimes \cdots \otimes U_{n-1},$$

  $U_i \in \{\pm I, \pm X, \pm Y, \pm Z\}$, $X = \sigma_X$, $Z = \sigma_Z$, $Y = -i\sigma_Y$.
- $\mathcal{S}$: an Abelian subgroup of $\mathcal{G}_n$.
- $\mathcal{C}$: the simultaneous eigenspace of the elements of $\mathcal{S}$ corresponding to the trivial character:

  $$\mathcal{S} = \{M \in \mathcal{G}_n : M|\psi\rangle = |\psi\rangle \text{ if } |\psi\rangle \in \mathcal{C}\}$$
- $\mathcal{C}$ is a QECC and $\mathcal{S}$ its *stabilizer*.

The Hamming (Sphere Packing) Bound

Classical Hamming Bound

Let $\mathcal{C}$ be a binary code with length n that can correct t errors. We have

$$\sum_{\mathbf{c}\in\mathcal{C}} \sum_{\ell=0}^{t} \binom{n}{\ell} \leqslant 2^n,$$

which gives the following upper bound on the size of any binary code $\mathcal{C}$:

$$|\mathcal{C}| \leqslant \frac{2^n}{\sum_{\ell=0}^{t} \binom{n}{\ell}}$$

$\Longrightarrow$

A binary code single-error correcting coed has at most $2^n/(1+n)$ codewords.

Codes which achieve the sphere packing bound with equality are called *perfect codes*.

Quantum Hamming Bound

Let $\mathcal{C}$ be a quantum code that maps k data qubits and $n-k$ ancillary qubits into n qubits. Assume that the code can correct up to t-qubit errors of the type X or Y or Z single-qubit action. We have

$$2^k \sum_{\ell=0}^{t} 3 \cdot \binom{n}{\ell} \leqslant 2^n.$$

What is the minimum length of a code that can correct any single qubit error when $k = 1$?

Quantum Computing Algorithms [1]

[1] Rutgers, ECE 579, Fall 2021

Prof. Emina Soljanin

Lecture #14, October 25

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

Alice and Bob Share an EPR Pair

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

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

Alice gets qubit A and Bob gets qubit B. 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.

Local Measurements in the Computational Basis

What happens if Alice measures her qubit in the computational basis[2] and Bob does nothing? We know that Alice's state will collapse to either $|0\rangle_A$ or $|1\rangle_A$.What happes to the joint state $|\varphi\rangle$? There are two possibilities:[3]

[2] σ_Z measurement

[3] This measurement is described by two projectors:
$\Pi_0 = |0\rangle\langle 0| \otimes I$ and $\Pi_1 = |1\rangle\langle 1| \otimes I$.

1. $|\varphi\rangle$ collapses to state

$$\frac{\Pi_0 |\varphi\rangle}{\|\Pi_0 |\varphi\rangle\|} = \frac{(|0\rangle\langle 0| \otimes I) \cdot |\varphi\rangle}{\|(|0\rangle\langle 0| \otimes I) \cdot |\varphi\rangle\|} = |0\rangle_A \otimes |0\rangle_B,$$

   which happens with probability $\langle\varphi| \cdot |0\rangle\langle 0| \otimes I \cdot |\varphi\rangle = 1/2$

2. $|\varphi\rangle$ collapses to state

$$\frac{\Pi_1 |\varphi\rangle}{\|\Pi_1 |\varphi\rangle\|} = \frac{(|1\rangle\langle 1| \otimes I) \cdot |\varphi\rangle}{\|(|1\rangle\langle 1| \otimes I) \cdot |\varphi\rangle\|} = |1\rangle_A \otimes |1\rangle_B,$$

   which happens with probability $\langle\varphi| \cdot |1\rangle\langle 1| \otimes I \cdot |\varphi\rangle = 1/2$

Observe that if Bob now measures his qubit in the computational basis, he will get a state that is identical to Alice's.[4]

[4] Einstain called to this phenomenon "spooky action at the distance" or *quantum non-locality*.

What happens if Alice and Bob measure their qubits simultaneously in the computational basis? This measurement is described by the following four projectors:

$$\Pi_{00} = |0\rangle\langle 0| \otimes |0\rangle\langle 0| \quad \Pi_{01} = |0\rangle\langle 0| \otimes |1\rangle\langle 1|$$
$$\Pi_{10} = |1\rangle\langle 1| \otimes |0\rangle\langle 0| \quad \Pi_{11} = |1\rangle\langle 1| \otimes |1\rangle\langle 1|$$

Local Measurements in the Hadamard Basis

What happens if Alice measures her qubit in the Hadamard basis[5] and Bob does nothing? There are two possibilities:

[5] σ_X measurement

1. $|\varphi\rangle$ collapses to state

$$\frac{(|+\rangle\langle+|\otimes I)\cdot|\varphi\rangle}{\|(|+\rangle\langle+|\otimes I)\cdot|\varphi\rangle\|} = |+\rangle_A\otimes|+\rangle_B,$$

   which happens with probability $\langle\varphi|\cdot|+\rangle\langle+|\otimes I\cdot|\varphi\rangle = 1/2$

2. $|\varphi\rangle$ collapses to state

$$\frac{(|1\rangle\langle1|\otimes I)\cdot|\varphi\rangle}{\|(|-\rangle\langle-|\otimes I)\cdot|\varphi\rangle\|} = |-\rangle_A\otimes|-\rangle_B,$$

   which happens with probability $\langle\varphi|\cdot|-\rangle\langle-|\otimes I\cdot|\varphi\rangle = 1/2$

Observe that if Bob now measures his qubit in the Hadamard basis, he will get a state that is identical to Alice's.

Local Measurements in Different Bases

What happens if Alice measures her qubit in the computational basis and Bob measures his qubit in the Hadamard basis? This measurement is described by the following four projectors:

$$\Pi_{0+} = |0\rangle\langle0|\otimes|+\rangle\langle+| \quad \Pi_{0-} = |0\rangle\langle0|\otimes|-\rangle\langle-|$$
$$\Pi_{1+} = |1\rangle\langle1|\otimes|+\rangle\langle+| \quad \Pi_{1-} = |1\rangle\langle1|\otimes|-\rangle\langle-|$$

Simultaneous Local Measurements

Suppose that Alice measures her qubit in the basis $\{|A_0\rangle, |A_1\rangle\}$ and Bob measurews his qubit in the basis $\{|B_0\rangle, |B_1\rangle\}$, where $|A_0\rangle$ and $|B_0\rangle$ can be expressed in the computational basis as follows:

$$|A_0\rangle = \cos\alpha|0\rangle + \sin\alpha|1\rangle \text{ and } |B_0\rangle = \cos\beta|0\rangle + \sin\beta|1\rangle$$

Note that Bob's basis can be obtained from Alice's by rotation, where the rotation angle is $\theta = \alpha - \beta$.

We denote Alice's measurement result by a where $a \in \{0,1\}$, and when Bob's measurement by b where $b \in \{0,1\}$. We next show that Alice and Bob will have identical outputs wp $\cos^2\theta$. Since Alice and Bob perform their measurements locally, the measurement on the shared EPR pair $|\varphi\rangle$ is effectively performed in the Kronceker product basis $|A_i\rangle\langle A_i|\otimes|B_j\rangle\langle B_j|$, $i,j\in\{0,1\}$. Furthermore, we have[6]

[6] We use the following identities:

$$\langle0|A_0\rangle = \langle A_0|0\rangle = \cos\alpha$$
$$\langle0|B_0\rangle = \langle B_0|0\rangle = \cos\beta$$

$$\begin{aligned}
P(a = b = 0) &= \langle\varphi| \left(|A_0\rangle\langle A_0| \otimes |B_0\rangle\langle B_0|\right) |\varphi\rangle \\
&= \frac{1}{\sqrt{2}}\left(\langle 0|A_0\rangle \langle A_0| \otimes \langle 0|B_0\rangle \langle B_0| + \langle 1|A_0\rangle \langle A_0| \otimes \langle 1|B_0\rangle \langle B_0|\right) |\varphi\rangle \\
&= \cos^2\alpha\cos^2\beta + 2\cos\alpha\cos\beta\sin\alpha\sin\beta + \sin^2\alpha\sin^2\beta \\
&= \frac{1}{2}(\cos\alpha\cos\beta + \sin\alpha\sin\beta)^2 = \frac{1}{2}\cos^2(\alpha-\beta)
\end{aligned}$$

It follows from a simple geometric argument that

$$P(a = b = 0) = P(a = b = 1)$$

Therefore, when Bob's basis can be obtained from Alice's by the angle $\alpha - \beta$ rotation, we have

$$P(a = b) = \cos^2(\alpha-\beta) \quad \text{and} \quad P(a \neq b) = \sin^2(\alpha-\beta).$$

We conclude that when Alice and Bob measure in the same basis (i.e., $\alpha - \beta = 0$), they get identical results.

Hidden Variables and Bell's Inequalities

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 the 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 the 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 century, many such experiments were conducted, but it was only in 2015 that the experiments showed nonexistence of hidden variables in the 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.

Quantum Computing Algorithms [1]

[1] Rutgers, ECE 579, Fall 2021

Prof. Emina Soljanin

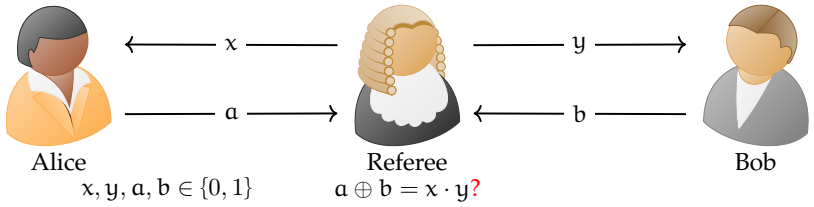
Lecture #15, October 27

This lecture explains the famous CHSH game and discusses quantum vs. classical correlations.

The CHSH Game

The CHSH game demonstrates how two players Alice and Bob, who cannot communicate with each other once the game starts, can benefit from shared entanglement much more than from shared classical randomness in winning the game. It is rooted in a paper by Clauser, Horne, Shimony, and Holt, hence the name.

In the CHSH game, Alice is given a binary input $x \in \{0, 1\}$ and Bob is given a binary input $y \in \{0, 1\}$ by a referee who guarantees that each combination of the inputs is equally likely. Upon receiving the input, Alice generates her output a and Bob his output b. They send the outputs to the referee who declares them the winners if $x \cdot y = a \texttt{ xor } b$. In other words, if $x = y = 1$, Alice and Bob win if their outputs are different. In all other cases, they win if their outputs are identical. Alice and Bob are allowed to agree on a strategy in advance, and to share random bits or entangled qubits, but once the game starts, they cannot communicate. Is there any advantage to be had from sharing entangled qubits?

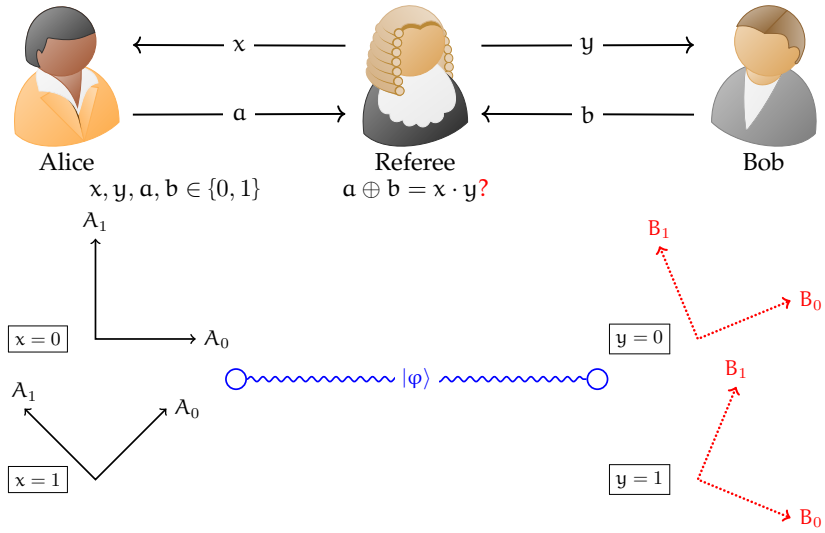


The Best Classical Strategy

A classical strategy to maximize the winning probability is that Alice sends to the referee $a = 0$ regardless of the value of her input, and Bob does the same. With this strategy, we always have $a = b$, and Alice and Bob loose only when x and y are both 1. Therefore, they win the game with probability 0.75. It is straightforward to check that this is an optimal strategy among the 16 different deterministic strategies (ways to map four possible inputs to four possible outputs). Any shared classical randomness would essentially randomize among the 16 possible deterministic strategies, and thus cannot beat the best.

The question then becomes if Alice and Bob can benefit from sharing EPR pairs. The answer to this question is yes, and we next describe a strategy with the winning probability of about 0.85.

The Best Quantum Strategy



Consider a strategy where Alice and Bob share an entangled pair of qubits in the state $|\varphi\rangle$ given as

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

Upon receiving the input, each player measures his/her qubit in one of the two possible bases depending on whether the input is 0 or 1. They then generate their outputs according to the result of the measurement. Alice's chooses the computational basis for her input $x = 0$, and the Hadamard basis for her input $x = 1$. Bob's chooses the computational basis rotated by $\pi/8$ for his input $y = 0$ and the computational basis rotated by $-\pi/8$ for his input $y = 1$. Thus, there are four possible combinations of Alice/Bob measurement bases corresponding to the four different input pairs x and y, as shown in Fig. 1. To find the winning probability of this strategy, we next prove a general result about local measurements of entangled qubits.

Recall that Alice and Bob share an EPR pair in the state $|\varphi\rangle$ given by (1). Suppose that Alice measures her qubit in the basis $\{|A_0\rangle, |A_1\rangle\}$ and Bob measurews his qubit in the basis $\{|B_0\rangle, |B_1\rangle\}$, where $|A_0\rangle$ and $|B_0\rangle$ can be expressed in the computational basis as follows:

$$|A_0\rangle = \cos\alpha|0\rangle + \sin\alpha|1\rangle \quad \text{and} \quad |B_0\rangle = \cos\beta|0\rangle + \sin\beta|1\rangle$$

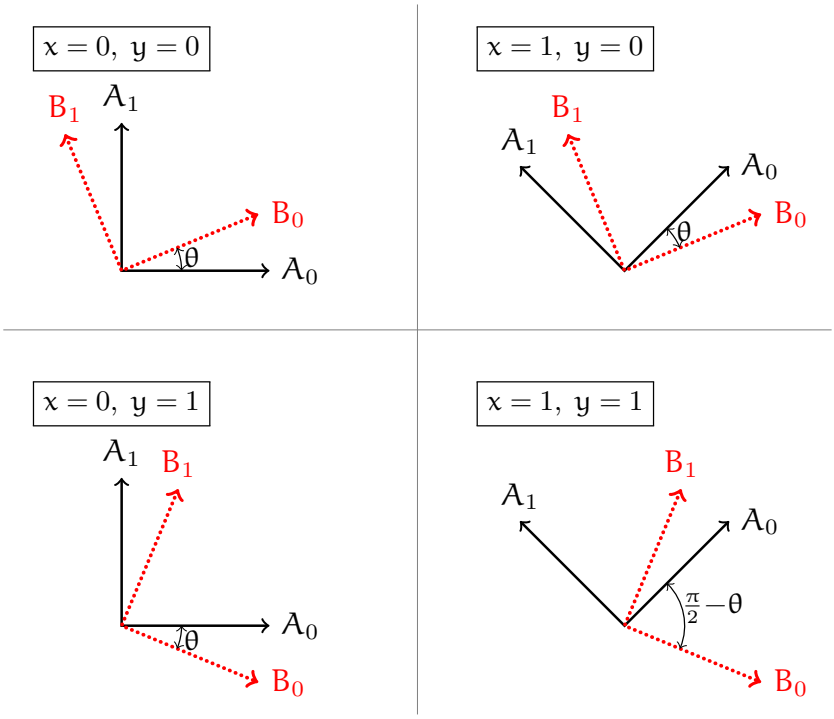


Figure 1: Choices of bases that Alice and Bob make based on their respective inputs x and y to measure their respective qubits. Each player selects the basis to measure based solely on the local input. The angle θ is chosen to be $\pi/8$. The strategy of the game is that, regardless of which basis is used, when Alice's measurement result is $i \in \{0, 1\}$, she outputs $a = i$, and when Bob's measurement result is $j \in \{0, 1\}$, he outputs $b = j$.

Note that Bob's basis can be obtained from Alice's by rotation, where the rotation angle is $\alpha - \beta$.

The strategy of the game is that, regardless of which basis is used, when Alice's measurement result is $i \in \{0, 1\}$, she outputs $a = i$, and when Bob's measurement result is $j \in \{0, 1\}$, he outputs is $b = j$. We have shown that, when Bob's basis can be obtained from Alice's by the angle $\alpha - \beta$ rotation, we have

$$P(a = b) = \cos^2(\alpha - \beta) \quad \text{and} \quad P(a \neq b) = \sin^2(\alpha - \beta). \tag{2}$$

We are now ready to derive the probability that Alice and Bob win the CHSH game. Observe that 1) the angle between Alice's and Bob's measurement bases is $3\pi/8$ when $x = y = 1$, and $\pi/8$ for all other input combinations (see Fig. 1), and 2) Alice and Bob win if they generate different outputs $a \neq b$ for inputs $x = y = 1$, and identical outputs for all other input combinations. Therefore, by (2), the winning probability

P_{win} can be computed as follows:

$$\begin{aligned} P_{win} &= P(xy = 0)P(a + b = 0|xy = 0)| + \\ &\quad P(xy = 1)P(a + b = 1|xy = 1) \\ &= \frac{3}{4}P(a = b|xy = 0)| + \frac{1}{4}P(a \neq b|xy = 1)] \\ &= \frac{3}{4} \cdot \cos^2(\pi/8) + \frac{1}{4} \cdot \sin^2(3\pi/8) \\ &= \cos^2(\pi/8) = (2 + \sqrt{2})/4 \gtrsim 0.853. \end{aligned}$$

A natural question to ask is whether Alice and Bob can achieve even better winning probability by sharing some other entangled state or by using some other sets of bases or both. The answer to these questions is no.

The significance of the CHSH game and similar tools is that they show that there is a limit to what can be done with classical (possibly hidden) randomness. If experiments involving shared entanglement show that this limit can be beaten (as they have), then there must be some "spooky action at a distance" like the one reflected in (2). And that is where the weirdness and the power of quantum computing reside.

Quantum Computing Algorithms [1]

[1] Rutgers, ECE 579, Fall 2021

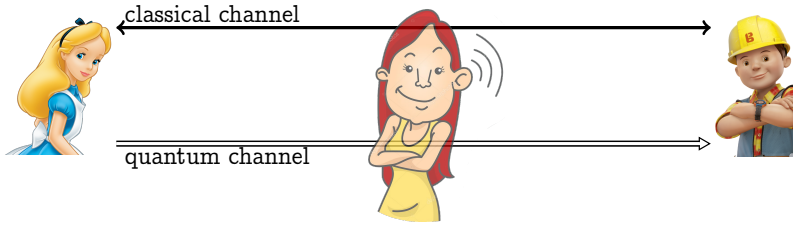
Prof. Emina Soljanin

Lecture #16, November 1

This lecture describes the fundamental principles and two protocols for quantum key distribution (QKD).

Traditional data encryption methods, based on using public keys, are threatened by the advances in quantum computing algorithms promising to efficiently solve so far intractable problems that make public key encryption currently secure. However, it is precisely quantum information processing advances that are also expected to enable secure communications by allowing efficient and secure private key distribution. The main advantage of private key encryption is that as long as the key strings are truly secret, it is provably secure, that is, insensitive to advances in computing.

A Quantum Key Distribution (QKD) protocol describes how two parties, commonly referred to as Alice and Bob, can establish a secret key by communicating over a quantum and a public classical channel when both channels can be accessed by an eavesdropper Eve.



The basic observation behind QKD protocols is that, since Eve cannot clone qubits, she can only gain information by measuring the original qubit. Therefore, when non-orthogonal qubits are transmitted from Alice to Bob, then Eve cannot gain any information from the qubits without disturbing their states, thus alerting Alice and Bob of her presence. We next describe two important QKD protocols. Substantial progress has been made towards building practical schemes based on these protocols.

BB84 Protocol

The BB84 was developed by Bennett and Brassard in 1984, hence the name. We outline the steps that Alice and Bob make under this protocol in order to generate a secret key of $O(n)$ bits for an arbitrary integer n.

1. Alice creates a sequence of $(4+\delta)n$ random data bits B_A, 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 tail (T), 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 head (H), she maps her data bit into either $|+\rangle$ (if her data bit is 0) or $|-\rangle$ (if her data bit is 1).

   We will refer to the sequence of heads and tails that Alice generated as C_A, and to the sequence of qbits she prepares as Q_A. We will call $\{|0\rangle, |1\rangle\}$ the T basis and $\{|-\rangle, |+\rangle\}$ the H basis, according to the corresponding coin faces.

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. 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.

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 T bases and gets $|0\rangle$, or the H bases and gets $|+\rangle$, he records bit 0; otherwise he records bit 1.

   We will refer to the sequence of heads and tails generated by Bob as C_B, and to the sequence of bits generated by his measurements as B_B. Here is a possible outcome of this protocol:

B_A	0	1	0	1	0	0	0	1	1	0	1	1
C_A	H	H	T	H	H	T	H	T	T	H	H	H
Q_A	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$
C_B:	H	T	H	H	T	T	H	H	T	T	T	H
B_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 from B_A and B_B 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 remaining $2n$ that will serve to check 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 number disagree, they abort the protocol. (The acceptable number is determined by e.g., the noise in the channels.)

9. Alice and Bob perform classical information reconciliation and privacy amplification on the remaining n bits to obtain $O(n)$ shared key bits.

E91-like Protocols

The E91 protocol for quantum key distribution was proposed by Ekert in 1991, hence the name. The scheme distributes entangled pairs of photons so that Alice and Bob each end up with one photon from each entangled pair. The creation and distribution of photons can be done by Alice, by Bob, or by some third party.

Suppose Alice and Bob share a set of n entangled pairs of qubits in the state $(|00\rangle + |11\rangle)/\sqrt{2}$ and Eve is not present. If they measure their respective states in the computational basis, they will get identical sequences of completely random bits. Thus, the scheme benefits from two properties of shared entanglement: randomness and correlation. To check if Eve was present, Alice and Bob can, for example, select a random subset of the shared entangled pairs, and test to see if they are entangled (instead of using them to generate the key bits). They can do that, e.g., by playing the CHSH game.

Quantum Computing Algorithms [1]

Prof. Emina Soljanin

Lecture #17, November 3

[1] Rutgers, ECE 579, Fall 2021

This lecture introduces the notion of mixed state, and is only concerned with representing, processing, and measuring mixed states.

Mixed States

There are many scenarios when we do not know the state of a quantum system, but do know that it is in the state $|\psi_j\rangle$ with probability p_j, $j = 1, \dots, k$. We say then that the quantum system is in a *mixed state*, and refer to the collection of pairs $\{|\psi_j\rangle, p_j\}_{j=1}^{k}$ as an *ensemble of states*. The states we worked with so far, which can be described by a vector, are known as *pure states*. A mixed state arises e.g., when we know that a measurement of a pure state has been performed but do not know the outcome.

The Density Matrix Formalism

So far, we used unit-norm vectors in Hilbert spaces to mathematically specify quantum states. We can instead describe a quantum state, say $|\psi\rangle$, by the projection matrix $\rho_\psi = |\psi\rangle\langle\psi|$. We refer to ρ_ψ as the *density matrix* of $|\psi\rangle$. To verify that this is a valid model, we need 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.

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

$$\mathrm{Tr}(A) = \sum_{i=1}^{n} a_{ii}$$

The trace is invariant under cyclic permutations, e.g.,

$$\mathrm{Tr}(ABCD) = \mathrm{Tr}(BCDA)$$

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, $|\psi\rangle \xrightarrow{U} U|\psi\rangle$ is replaced by $\rho_\psi \xrightarrow{U} U\rho_\psi U^\dagger$.

2. Suppose that a measurement defined by the basis $|u_1\rangle, \dots, |u_N\rangle$ is performed on the state $|\psi\rangle$. We know that the resulting state will be $|u_i\rangle$ with probability (wp) $|\langle\psi|u_i\rangle|^2$, $1 \leqslant i \leqslant N$. We observe that $|\langle\psi|u_i\rangle|^2 = \langle\psi|u_i\rangle\langle u_i|\psi\rangle = \mathrm{Tr}\big(|u_i\rangle\langle u_i| \cdot |\psi\rangle\langle\psi|\big) = \mathrm{Tr}\big(|u_i\rangle\langle u_i| \cdot \rho_\psi\big)$.

   Therefore, in terms of density matrices, we have
   $\rho_\psi \to |u_i\rangle\langle u_i|$ wp $\mathrm{Tr}\big(|u_i\rangle\langle u_i|\rho_\psi\big)$.

Note that to describe the state, evolution, and measurement, we used density matrices rather than state vectors. The advantage of the density matrix formalism is that it allows us to compactly describe mixed states. A mixed state, that is, a quantum system about which we only know that it is in the state $|\psi_j\rangle$ with probability p_j has a

density matrix defined as follows:

$$\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|. \tag{1}$$

The states that have rank–1 density matrices $\rho_\psi = |\psi\rangle\langle\psi|$ are known as *pure states*. In general, a density matrix ρ is a Hermitian, positive semi-definite, trace–1 matrix. These properties easily follow from (1).

Observe that two different ensembles of states can have identical density matrices, and therefore quantum mechanically represent identical states. Fig. 1 shows two different ensembles with the density matrix equal to $\frac{1}{2}\mathrm{I}$.

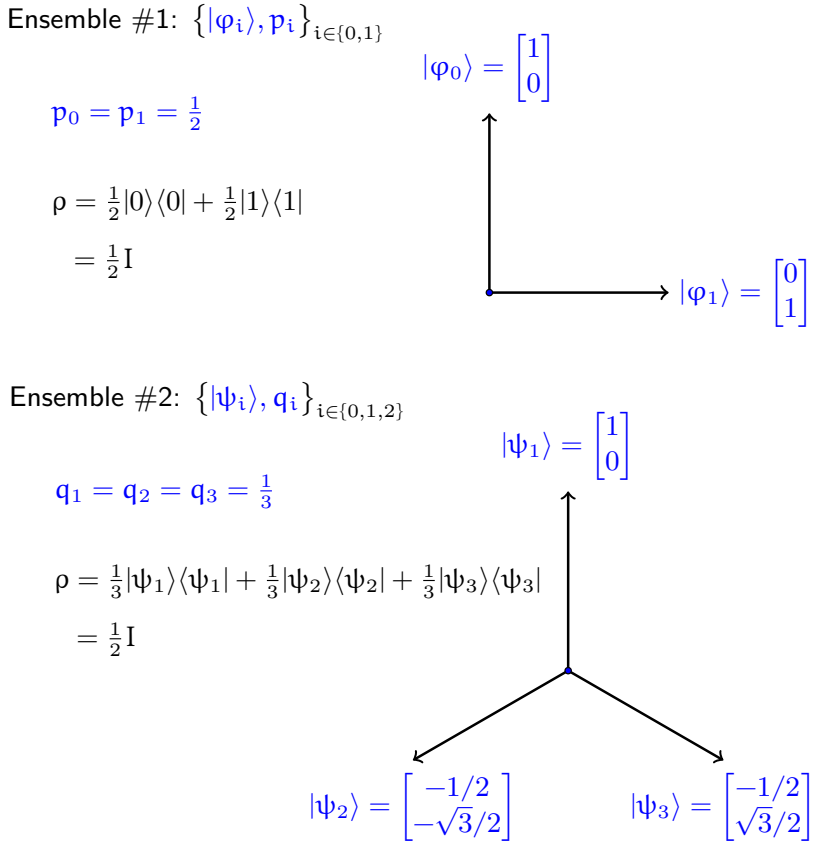


Figure 1: Two "different" ensembles of pure states with identical density matrices equal to $\frac{1}{2}\mathrm{I}$.

When a $d \times d$ density matrix is equal to $\frac{1}{2}\mathrm{I}$, we say that the system is in the maximally mixed state. These density matrices are quantum counterparts to classical uniform distributions.

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 $U\rho_j U^\dagger$, as we showed above. 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. Therefore, the system with density matrix (1) will evolve into another mixed state, whose density matrix is given by

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

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

Measuring Mixed States

We next look into what happens when we perform a quantum measurement defined by operators Π_i on a mixed state whose density matrix is $\rho = \sum_j p_j|\psi_j\rangle\langle\psi_j|$. Again, let $\rho_j = |\psi_j\rangle\langle\psi_j|$. If the state being measured is $|\psi_j\rangle$ (which happens with probability p_j), then the probability of getting measurement result i is $\mathrm{Tr}(\Pi_i\rho_j)$. Therefore, by the total probability formula, when measuring ρ, we get outcome i with probability

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

Note that different ensembles $\{\psi_j, p_j\}$ with the same ρ will give outcome i with the same probability $\mathrm{Tr}(\Pi_i\rho)$, 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 $\frac{\Pi_i\rho_j\Pi_i}{\mathrm{Tr}(\Pi_i\rho_j)}$. Therefore, if we observe outcome i, the system is in the mixed state

$$\sum_j p_j \frac{\Pi_i\rho_j\Pi_i}{\mathrm{Tr}(\Pi_i\rho_j)} = \frac{\Pi_i\rho\Pi_i}{\mathrm{Tr}(\Pi_i\rho)}.$$

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 lost the measurement record? Note that, mathematically, the state of the system is for us described based on our *ignorance/knowledge*. We saw that we get state $\frac{\Pi_i\rho\Pi_i}{\mathrm{Tr}(\Pi_i\rho)}$ wp $\mathrm{Tr}(\Pi_i\rho)$. If we lost the measurement record, we would have a state described by the density matrix

$$\sum_{i=1} \mathrm{Tr}(\Pi_i\rho) \cdot \frac{\Pi_i\rho\Pi_i}{\mathrm{Tr}(\Pi_i\rho)} = \sum_{i=1} \Pi_i\rho\Pi_i. \tag{2}$$

Elementary probability (e.g., the total probability expression) is used for derivations.

Quantum Computing Algorithms [1]

[1] Rutgers, ECE 579, Fall 2021

Prof. Emina Soljanin

Lecture #18, November 8

This lecture talks about the Bloch sphere and Schrödinger equation.

Density Matrix Review

Recall that the density matrix formalism of quantum mechanics is equivalent to the vector formalism for pure states. Dealing with vectors may be easier but, for mixed states, we can only use the density matrix formalism. Here are some properties of density matrices.

A pure quantum state, say $|\psi\rangle$, can be described by the projection matrix $\rho_\psi = |\psi\rangle\langle\psi|$. We refer to ρ_ψ as the *density matrix* of $|\psi\rangle$. A mixed state is a quantum system about which we only know that it is in the state $|\psi_j\rangle$ with probability p_j. It is described by the following density matrix:

$$\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|. \tag{1}$$

For pure states, the following holds:

1. ρ is Hermitian. Check if $\rho^\dagger = \rho$.
2. ρ is idempotent (a projection). Check if $\rho^2 = \rho$.
3. $\mathrm{Tr}(\rho) = 1$

For mixed states, the following holds:

1. ρ is Hermitian. Check if $\rho^\dagger = \rho$.
2. ρ is positive semidefinite. (ρ is not a projection.) $\implies \det(\rho) \geqslant 0$
3. $\mathrm{Tr}(\rho^2) \leqslant 1$

Bloch Sphere

The Bloch sphere provides a useful way to represent and visualize both pure and mixed qubit states, and is traditionally used in quantum mechanics. It is also used in quantum computing platforms, such as IBM-Q, since actions of single-qubit gates on pure states are easy to see within the Bloch sphere framework.

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

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

where β_X, β_Y, and β_Z are real numbers. The latter holds because ρ is a Hermitian matrix and

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

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

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

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.*

For pure states, we have $\mathrm{Tr}(\rho^2) = 1$, and thus

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

Therefore, 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.

We can also see that pure states are points on the Bloch sphere by considering the representation of $|\psi\rangle$ we introduced earlier in the class:

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

Comparing $|\psi\rangle\langle\psi|$ with the matrix (2), we find that the Bloch vector of $|\psi\rangle$ makes an angle of θ with the z axis, and its projection in the $x-y$ plane makes an angle of ϕ with the x axis, as shown in Fig. 1. With this representation, it is easy to see that any two diametrically opposite (antipodal) points correspond to a pair of mutually orthogonal pure state vectors. In particular, $\beta_X = \beta_Y = 0$ and $\beta_Z = 1$ gives $\rho = |0\rangle\langle 0|$, while $\beta_X = \beta_Y = 0$ and $\beta_Z = -1$ gives $\rho = |1\rangle\langle 1|$.

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 $\mathbb{C}^{2\times 2}$.

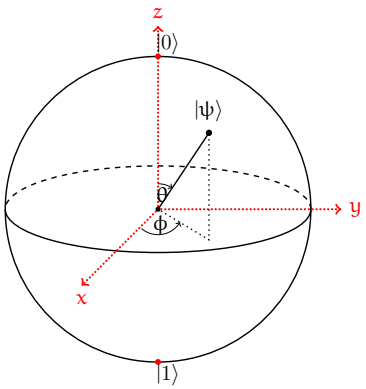


Figure 1: Bloch Sphere

Schrödinger Equation

Unitary evolution in a closed quantum system is a consequence of the Schrödinger equation. In a closed system, the state (wave function) $|\psi(t)\rangle$ evolves according to the Schrödinger equation:

$$i\hbar \frac{d}{dt} |\psi(t)\rangle = H \cdot |\psi(t)\rangle$$

where $\hbar$ is the reduced Plank's constant and H is a fixed Hermitian matrix known as the system's Hamiltonian. If H does not depend on time, the solution of this equation is

$$|\psi(t)\rangle = U(t) |\psi(o)\rangle , \quad U(t) = \exp\left(-\frac{i}{\hbar} Ht\right)$$

The Hamiltonian describes the physical model. The Schrödinger equation tells us how a state-vector evolves in time given the physical model described by the Hamiltonian. Show that $U(t)$, defend above, is a unitary matrix.

The exponential of an $n \times n$ complex matrix X, denoted by e^X or $\exp(X)$, is the $n \times n$ matrix given by the power series

$$e^X = \sum_{k=0}^{\infty} \frac{1}{k!} X^k$$

where X^0 is defined to be the $n \times n$ identity matrix.

Quantum Computing Algorithms [1]

[1] Rutgers, ECE 579, Fall 2021

Prof. Emina Soljanin

Lecture #19, November 22

This lecture explains the quantum Fourier transform (QFT), which we need for the Shor factoring algorithm.

Quantum Fourier Transform

Definition

The quantum Fourier transform (QFT) on n qubits[2] is the map that can be described by its action on the basis states $|j\rangle$ of $\mathcal{H}^{\otimes n}$ as follows:

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

$$\text{QFT}: \quad |j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^{jk} |k\rangle.$$

where $N = 2^n$ and $\omega_N = e^{2\pi i/N}$ is a primitive[3] N-th root of unity. Note that jk is an integer product and $|j\rangle$ stands for $|j_1 j_2 \dots j_n\rangle$ where $j_1 j_2 \dots j_n$ is the binary representation of j.

[3] What does primitive mean?

Therefore, the QFT of an arbitrary state $|x\rangle$ is given by

$$|x\rangle = \sum_{j=0}^{N-1} x_j |j\rangle \mapsto |y\rangle = \sum_{k=0}^{N-1} y_k |k\rangle \quad \text{where} \quad y_k = \sum_{j=0}^{N-1} x_j \omega_N^{jk}.$$

In the matrix form, we have $|y\rangle = U_{\text{QFT}} |x\rangle$ where

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

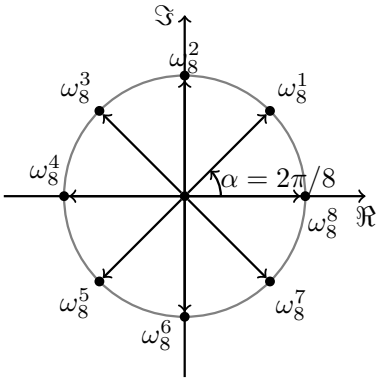


Figure 1: The 8th roots of unity.

Show that U_{QFT} is a unitary matrix.

The Quantum Fourier transform is related to the Quantum Hadamard transform, which is given by

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

where yx is the binary inner product. These two transforms are not identical except for $n = 1$.

Examples

For $n = 1$, we have

$$U_{\text{QFT}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

For $n = 2$, we have

$$U_{QFT} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$$

Implementation

QFT can be carried out by a quantum circuit built entirely out of 1-qubit and 2-qubit gates.[4] The quantum gates used in the circuit are the single-qubit Hadamard gate

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

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

and the two-qubit controlled phase gate

$$cR_k = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{\frac{2\pi i}{2^k}} \end{bmatrix} \quad \text{where} \quad R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{bmatrix}$$

Interlude

Controlled Single-Qubit Gates

A single-qubit gate and its controlled version are given as follows: [5]

[5] Do you know of a controlled gate? What is its U?

$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix} \quad \text{and} \quad cU = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}$$

In the controlled-U gate, the first qubit controls whether U acts to the second qubit. [6] The controlled-U maps the basis states as follows:

[6] U is applied to the second qubit only if the first qubit is $|1\rangle$.

$$|00\rangle \mapsto |00\rangle \qquad |10\rangle \mapsto |1\rangle \otimes U|0\rangle = |1\rangle \otimes (u_{00}|0\rangle + u_{10}|1\rangle)$$
$$|01\rangle \mapsto |01\rangle \qquad |11\rangle \mapsto |1\rangle \otimes U|1\rangle = |1\rangle \otimes (u_{01}|0\rangle + u_{11}|1\rangle)$$

Binary Representation of Numbers

- If $j = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n 2^0$
  then $j_1 j_2 \ldots j_n$ is the binary representation of j.
- $0.j_m j_{m+1} \ldots j_\ell$ represents $j_m 2^{-1} + j_{m+1} 2^{-2} + \cdots + j_\ell 2^{-(\ell - m + 1)}$

Exercises

1. Show that for $j \in \{0,1\}$, we have $H|j\rangle = \frac{|0\rangle + e^{2\pi i 0.j}|1\rangle}{\sqrt{2}}$
2. Show that for $j \in \{0,1\}$, we have $R_k|j\rangle = \exp(2\pi i 0.\underbrace{0\ldots0}_{k-1}j)|j\rangle$

Gate Implementation of QFT

We start with $U_{QFT}|j\rangle = \frac{1}{2^{n/2}}\sum_{k=0}^{2^n-1} e^{\frac{2\pi i}{2^n}\cdot jk}|k\rangle$ which gives

$$
\begin{aligned}
U_{QFT}|j_1\ldots j_n\rangle =& \frac{1}{2^{n/2}}\sum_{k_1\ldots k_n\in\{0,1\}^n}\exp\Big(\frac{2\pi i}{2^n}\cdot j\cdot\textstyle\sum_{\ell=1}^n k_\ell 2^{n-\ell}\Big)|k_1\ldots k_n\rangle\\
=&\frac{1}{2^{n/2}}\sum_{k_1\ldots k_n\in\{0,1\}^n}\exp\Big(2\pi i\cdot j\cdot\textstyle\sum_{\ell=1}^n k_\ell 2^{-\ell}\Big)|k_1\ldots k_n\rangle\\
=&\frac{1}{2^{n/2}}\sum_{k_1\ldots k_n\in\{0,1\}^n}\bigotimes_{\ell=1}^n\exp(2\pi i j k_\ell 2^{-\ell})|k_\ell\rangle\\
=&\frac{1}{2^{n/2}}\sum_{k_1\in\{0,1\}}\cdots\sum_{k_n\in\{0,1\}}\bigotimes_{\ell=1}^n\exp(2\pi i j k_\ell 2^{-\ell})|k_\ell\rangle\\
=&\bigotimes_{\ell=1}^n\sum_{k_\ell\in\{0,1\}}\exp(2\pi i j k_\ell 2^{-\ell})|k_\ell\rangle = \bigotimes_{\ell=1}^n\big(|0\rangle+\exp(2\pi i j 2^{-\ell})|1\rangle\big)\\
=&\bigotimes_{\ell=1}^n\big(|0\rangle+\exp(2\pi i 2^{-\ell}\textstyle\sum_{k=1}^n j_k 2^{n-k})|1\rangle\big)\\
=&\bigotimes_{\ell=1}^n\big(|0\rangle+\exp(2\pi i 0.j_\ell\ldots j_n)|1\rangle\big)\\
=&\frac{|0\rangle+e^{2\pi i 0.j_1 j_2\ldots j_n}|1\rangle}{\sqrt{2}}\otimes\frac{|0\rangle+e^{2\pi i 0.j_2 j_3\ldots j_n}|1\rangle}{\sqrt{2}}\otimes\cdots\otimes\\
&\frac{|0\rangle+e^{2\pi i 0.j_{n-1}j_n}|1\rangle}{\sqrt{2}}\otimes\underbrace{\frac{|0\rangle+e^{2\pi i 0.j_n}|1\rangle}{\sqrt{2}}}_{H|j_n\rangle}
\end{aligned}
$$

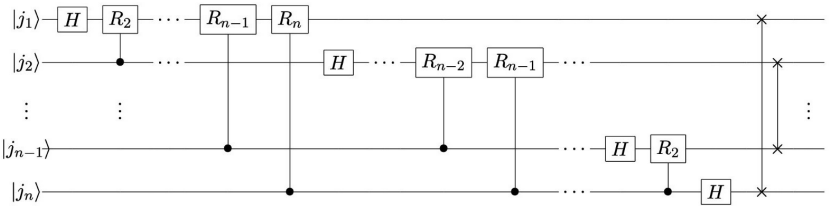


Figure 2: Quantum circuit for QFT.

Introduction to Quantum Information Science [1]

[1] Rutgers, ECE 579, Fall 2021

Prof. Emina Soljanin

Lecture #20, November 29

This lecture outlines 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 f b modulo M is said to be infinite. We know that r is finite when b and M are relatively prime.[2]

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

Let f be the following function:

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

Is f periodic? Consider $f(x+r)$. 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 $f(x) = b^x \mod M$.

Let r be an even number. Finding the period of $f(x) = b^x \mod M$ allows us to find a factor of M. To see that, note that $b^r - 1 = 0 \mod M$, and thus

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

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 and 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. Therefore, there exists an integer $r > 0$ such that $b^r = 1 \mod M$.

[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
$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x, f(x)\rangle$$
Recall that r is the period of f.

3. Measure the target (right) register. If the state of the right register after the measurement is f_0, the resulting state in the data registar will be
$$|\psi_0\rangle = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + kr\rangle$$
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.

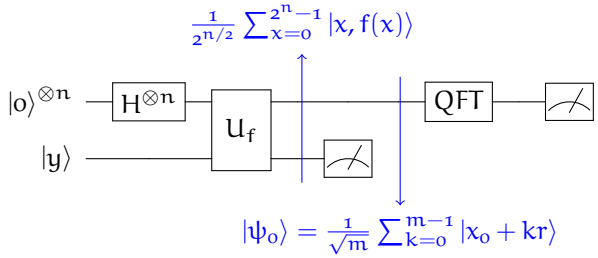


Figure 1: Steps 2 – 5. This is the quantum part of the algorithm. See the sections below for more detail.

6. Use classical methods to obtain a conjectured period r from the value v.

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.