Technische Universität Dresden

International Center for Computational Logic

COMPLEXITY THEORY

Lecture 24: Quantum Computing (1)

Stephan Mennicke

Knowledge-Based Systems

TU Dresden, 13 Jan 2026

More recent versions of this slide deck might be available.
For the most current version of this course, see
https://iccl.inf.tu-dresden.de/web/Complexity_Theory/en

Quantum computing

Quantum computing currently is our main hope for building physical computers that may in some cases perform exponentially better than deterministic Turing machines.

- Quantum computers exploit the rules of Quantum Mechanics
- Constructing a real quantum computer is an open engineering challenge of high complexity
- The properties of such computers, however, can be studied with relatively simple mathematical tools, and without any of the underlying physical interpretations of the theory

The quantum world

> The only difference between a probabilistic classical world and the equations of the quantum world is that somehow or other it appears as if the probabilities would have to go negative.
> – Richard Feynman, in “Simulating Physics with Computers,” 1982

Quantum mechanics has been proposed as a model of physical reality:

- We want to model the state of a physical system, e.g., its energy or spin
- Quantum mechanics asserts that states are eventually discrete (“quantised”)
- However, the model postulates that the system’s state might not be determined, but is governed by certain probabilities
- Simplified: it appears that the system is in several states at once
- When we measure the value of the system, the probability wave collapses, the system takes a determined (“classical”) state, and all information on the prior probability wave is lost

Probabilities in the quantum world

Let $E_1, \ldots, E_n$ be a finite set of possible events in a random experiment

Classical Probability Theory:

- The outcome X of an experiment is described by probabilities $\Pr[X = E_i]$
- The corresponding discrete probability distribution can be described as a vector $\langle p_1, \ldots, p_n \rangle$ with $p_i = \Pr[X = E_i]$ $(1 \leq i \leq n)$
- Classical probability theory requires that $p_i \in [0, 1]$ and $\sum_{i=1}^{n} p_i = 1$
  (this sum is called the 1-norm of the vector)

Quantum Mechanics:

- The probability distribution over the n events can be described by a vector $\langle q_1, \ldots, q_n \rangle$
- Quantum mechanics requires that ${q_i}^2 \in [0, 1]$ and $\sum_{i=1}^{n} {q_i}^2 = 1$
  (the square root of this sum is called the 2-norm of the vector)
- The probability of observing the outcomes E_i is ${q_i}^2$

Quantum systems

A state of a system with possible values $E_1, \ldots, E_n$ (of observable quantities) governed by probabilities as on the previous slide is often denoted as

$$q_1|E_1\rangle + \ldots + q_n|E_n\rangle$$

where

- $\langle q_1, \ldots, q_n \rangle$ defines the probability wave function
- with amplitudes q_i
- the Dirac ket notation with the non-matching parentheses is historical and non-negotiable with physicists

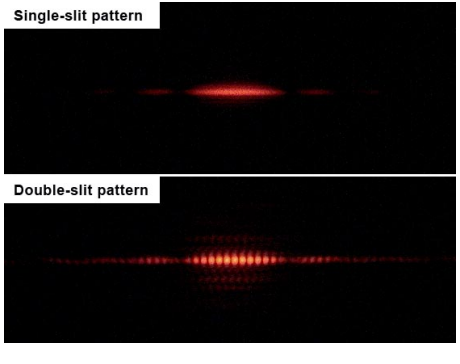
Remark 1: In quantum mechanics, one considers complex numbers for amplitudes, but real numbers are enough to show most aspects relevant to computing.

Remark 2: The above is what is called a pure state. Its probabilities express the fundamental "natural" uncertainty that is part of the model. If we are unsure which pure state a system is in, we may consider mixtures of several pure states, weighted by probabilities (which model our lack of knowledge rather than inherent quantum uncertainty). This is called a mixed state (we won't see much of this here).

Working with negative probabilities

The systems $\frac{1}{\sqrt{2}}|A\rangle + \frac{1}{\sqrt{2}}|B\rangle$ and $\frac{1}{\sqrt{2}}|A\rangle - \frac{1}{\sqrt{2}}|B\rangle$ will be measured in state A or B with the same probabilities $\frac{1}{2}$ each.

Yet, the states are different and can be distinguished, since wave functions may be in superposition so that positive and negative amplitudes cancel each other out



Double-slit experiment; ©Wikimedia User:Jordgette, 2010, CC-BY-SA 3.0

Qubits, and a geometrical intuition

We can use the state of a quantum system to represent one bit of information:

$$\alpha_0|0\rangle + \alpha_1|1\rangle$$

This is called a qubit.

Example 24.1: A classically true bit is $0|0\rangle + 1|1\rangle = |1\rangle$, while $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ is a system that will yield either of the two values with equal probability.

Geometrical intuition: (or: "The 2-norm is also called Euclidian norm for a reason")

- For real numbers α_0 and α_1, we can visualise a qubit as a vector of length $\sqrt{{\alpha_0}^2 + {\alpha_1}^2} = 1$.
- This unit vector has an angle of θ to the x-axis, where $\cos\theta = \alpha_0$ and $\sin\theta = \alpha_1$.

It's less obvious for complex amplitudes or systems with more than two possible values, but geometrical ideas may still be useful.
For example, we may "rotate" a qubit by a certain angle.

Operations on qubits

What kind of computational operations are possible on qubits?

(1) A qubit transformed by a valid operation should still have a valid probability wave (i.e., remain a unit vector in the 2-norm)

(2) The operation must be linear (i.e., if a vector $\vec{v}$ is a linear combination $\vec{v} = a\vec{w_1} + b\vec{w_2}$, then its image $F(\vec{v})$ is $F(\vec{v}) = aF(\vec{w_1}) + bF(\vec{w_2})$)

Item (1) is clearly necessary; (2) is a requirement imposed by Quantum Mechanics

Such operations can be expressed using a 2×2 matrix.

Example 24.2: The rotation of a qubit by an angle θ is captured by the matrix

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

For example, we can rotate $|0\rangle$ by 45 degrees ($\pi/4$) (recall: $\sin\frac{\pi}{4} = \cos\frac{\pi}{4} = \frac{1}{\sqrt{2}}$):

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

Unitary matrices

Recall: The conjugate of a complex number $z = a + ib$ is $\bar{z} = a - ib$. The conjugate $\bar{A}$ of a complex matrix A is the matrix of its conjugates. The transpose A^T of a matrix is such that $(A^T)_{ij} = A_{ji}$. By A^* we denote the conjugate transpose $\bar{A}^T$ of A.

In general, every linear, 2-norm preserving operation on an n-dimensional quantum system can be represented by an $n \times n$ matrix of the following special type:

Definition 24.3: A complex $n \times n$ matrix A is unitary if $AA^* = I$ (the identity matrix).

Fact 24.4: For a complex $n \times n$ matrix A, the following conditions are equivalent:

- A is unitary, i.e. $AA^* = I$.
- For every $\vec{v} \in \mathbb{C}^n$, the 2-norm $\|\vec{v}\|_2$ of $\vec{v}$ is the same as the 2-norm $\|A\vec{v}\|_2$ of $A\vec{v}$.
- The columns of A form an orthonormal basis of $\mathbb{C}^n$.
- The rows of A form an orthonormal basis of $\mathbb{C}^n$.
- For every orthonormal basis $(\vec{v_i})_{1 \le i \le n}$ of $\mathbb{C}^n$, the vectors $(A\vec{v_i})_{1 \le i \le n}$ also form an orthonormal basis of $\mathbb{C}^n$.

Combining and reversing transformations

Composing operations defined by unitary matrices is always allowed:

Lemma 24.5: If A and B are unitary matrices that represent quantum operations, then their composition (the mapping that first applies A, then B) is also unitary and is represented by the matrix BA.

In particular, for every unitary matrix A, the operation represented by A^* has the effect of reversing A, since $A^*A = I$ is the identity.

Observation 24.6: Every quantum operation is reversible.

Combining quantum systems

To compute interesting things, we usually need more than a single bit.

Two qubits $\alpha_0|0\rangle + \alpha_1|1\rangle$ and $\beta_0|0\rangle + \beta_1|1\rangle$, can be considered as a single, four-state quantum system of the form:

$$(\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle) = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle$$

That is, we use $|00\rangle$ as a shorthand for $|0\rangle|0\rangle$ etc. The tensor product (outer product) symbol $\otimes$ is often omitted.

Observations:

- This multiplication preserves our 2-norm:

$$(\alpha_0\beta_0)^2 + (\alpha_0\beta_1)^2 + (\alpha_1\beta_0)^2 + (\alpha_1\beta_1)^2 = ({\alpha_0}^2 + {\alpha_1}^2)({\beta_0}^2 + {\beta_1}^2) = 1 \cdot 1 = 1$$

- The probability of individual events is unchanged, e.g.,

$$\Pr[\text{first bit} = 0] = (\alpha_0\beta_0)^2 + (\alpha_0\beta_1)^2 = {\alpha_0}^2({\beta_0}^2 + {\beta_1}^2) = {\alpha_0}^2$$

Combining more bits leads to an m-bit quantum register with values of the form $|b_1 \cdots b_m\rangle$ with $b_i \in \{0, 1\}$.

Entanglement

Is every state of a 2-bit quantum register of the form

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

No!

Example 24.7: The 2-bit quantum state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ cannot be represented as the product of two independent qubits. This state is known as the EPR (Einstein-Podolsky-Rosenberg) state; it is also known as one of the four Bell states.

We call this situation entanglement: The outcomes of two experiments measuring the values of the first and second bit cannot be considered as the outcomes of two independent random experiments with any individual probability.

What makes this unusual is that the particles that constitute such an entangled system may be separated in space, yet seem to "influence" each other due to the joint probability wave governing them.

A simple game

For a classical example of quantum weirdness, let us look at a cooperative game:

Two players, Alice and Bob, are in physically separated locations:

- The game master throws two coins: $x, y \in \{0, 1\}$
- The value of x is communicated to Alice, the value of y to Bob
- Alice must answer with a bit $a \in \{0, 1\}$, and Bob with a bit $b \in \{0, 1\}$
- The players win if $a \oplus b = x \wedge y$.

What are their best chances in winning this game?

An optimal strategy

A simple strategy: Always return $a = b = 0$!
Chances of success: 75%

One can show that this is the best they can do:

Theorem 24.8 (Bell, 1964; Clauser et al. 1969): No probabilistic or deterministic strategy leads to a probability of $> \frac{3}{4}$ of winning this game.

Proof (sketch): Any probabilistic strategy that leads to an average success rate $p > \frac{3}{4}$ must involve single-case behaviours that succeed with probability $\geq p$. One can show that no such choice exists by a simple case distinction over the possible strategies (for each player, this corresponds to one of four possible functions $\{0,1\} \to \{0,1\}$). □

Quantum cheating

A strategy that uses Quantum Mechanics:

- Alice and Bob create an entangled quantum state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$
- Alice takes the first bit (particle); Bob the second – this is physically possible
- Alice's strategy: if $x = 1$, rotate the first bit by $\pi/8$ (22.5 degrees), otherwise do nothing; then measure the first bit and answer with its value
- Bob's strategy: if $y = 1$, rotate the second bit by $-\pi/8$ (–22.5 degrees), otherwise do nothing; then measure the second bit and answer with its value

"Rotating the first qubit"?

- Independent mappings on subspaces (e.g., the 2D-space of a qubit) are combined with a tensor product, represented by the Kronecker product on matrices:

$$\begin{pmatrix} \cos\frac{\pi}{8} & -\sin\frac{\pi}{8} \\ \sin\frac{\pi}{8} & \cos\frac{\pi}{8} \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \cos\frac{\pi}{8}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & -\sin\frac{\pi}{8}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \sin\frac{\pi}{8}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \cos\frac{\pi}{8}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \cos\frac{\pi}{8} & 0 & -\sin\frac{\pi}{8} & 0 \\ 0 & \cos\frac{\pi}{8} & 0 & -\sin\frac{\pi}{8} \\ \sin\frac{\pi}{8} & 0 & \cos\frac{\pi}{8} & 0 \\ 0 & \sin\frac{\pi}{8} & 0 & \cos\frac{\pi}{8} \end{pmatrix}$$

- Such local transformations on a qubit are possible in practical experiments

Analysing the quantum strategy (1)

Case $x = y = 0$:

- Then Alice and Bob just measure the qubits.
- The system's value will be either $|00\rangle$ or $|11\rangle$ with probability $\frac{1}{2}$ each; hence $a = b$ and $a \oplus b = 0 = x \wedge y$ with probability 1.

Case $x = 1$ and $y = 0$:

- Then the system will be transformed by Alice to become

$$\begin{pmatrix} \cos\frac{\pi}{8} & 0 & -\sin\frac{\pi}{8} & 0 \\ 0 & \cos\frac{\pi}{8} & 0 & -\sin\frac{\pi}{8} \\ \sin\frac{\pi}{8} & 0 & \cos\frac{\pi}{8} & 0 \\ 0 & \sin\frac{\pi}{8} & 0 & \cos\frac{\pi}{8} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}}\cos\frac{\pi}{8} \\ -\frac{1}{\sqrt{2}}\sin\frac{\pi}{8} \\ \frac{1}{\sqrt{2}}\sin\frac{\pi}{8} \\ \frac{1}{\sqrt{2}}\cos\frac{\pi}{8} \end{pmatrix} \begin{matrix} \text{corresponds to } |00\rangle \\ \text{corresponds to } |01\rangle \\ \text{corresponds to } |10\rangle \\ \text{corresponds to } |11\rangle \end{matrix}$$

- Hence the probability of $a = b$ is $2(\frac{1}{\sqrt{2}}\cos\frac{\pi}{8})^2 = (\cos\frac{\pi}{8})^2 > 0.853$

Case $x = 0$ and $y = 1$: This is similar to $x = 1$ and $y = 0$, and yields the same probability.

Analysing the quantum strategy (2)

Case $x = y = 1$:

- Then both Alice and Bob apply a rotation.
- Bob's transformation matrix is:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} \cos\frac{\pi}{8} & \sin\frac{\pi}{8} \\ -\sin\frac{\pi}{8} & \cos\frac{\pi}{8} \end{pmatrix} = \begin{pmatrix} \cos\frac{\pi}{8} & \sin\frac{\pi}{8} & 0 & 0 \\ -\sin\frac{\pi}{8} & \cos\frac{\pi}{8} & 0 & 0 \\ 0 & 0 & \cos\frac{\pi}{8} & \sin\frac{\pi}{8} \\ 0 & 0 & -\sin\frac{\pi}{8} & \cos\frac{\pi}{8} \end{pmatrix}$$

- Hence, the result of applying this to the state as transformed by Alice is:

$$\begin{pmatrix} \cos\frac{\pi}{8} & \sin\frac{\pi}{8} & 0 & 0 \\ -\sin\frac{\pi}{8} & \cos\frac{\pi}{8} & 0 & 0 \\ 0 & 0 & \cos\frac{\pi}{8} & \sin\frac{\pi}{8} \\ 0 & 0 & -\sin\frac{\pi}{8} & \cos\frac{\pi}{8} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}}\cos\frac{\pi}{8} \\ -\frac{1}{\sqrt{2}}\sin\frac{\pi}{8} \\ \frac{1}{\sqrt{2}}\sin\frac{\pi}{8} \\ \frac{1}{\sqrt{2}}\cos\frac{\pi}{8} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} (\cos\frac{\pi}{8})^2 - (\sin\frac{\pi}{8})^2 \\ -2\cos\frac{\pi}{8}\sin\frac{\pi}{8} \\ 2\cos\frac{\pi}{8}\sin\frac{\pi}{8} \\ (\cos\frac{\pi}{8})^2 - (\sin\frac{\pi}{8})^2 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}$$

- The probability of winning, i.e., $a \neq b$, therefore is $\left(-\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = 0.5$.

Analysing the quantum strategy (3)

In summary, the winning probabilities are:

- 1 if $x = y = 0$
- > 0.853 if $x \neq y$
- 0.5 if $x = y = 1$

Hence, in total we obtain a winning probability $> \frac{1}{4} \cdot 1 + \frac{1}{2} \cdot 0.853 + \frac{1}{4} \cdot 0.5 = 0.8015$, which is better than the classical 0.75.

This has been called the EPR-Paradox, since it seems to suggest faster-than-light communication between the entangled qubits. However, there is no real communication (that would be impossible). See the Web for discussions.

Important note: Our calculations assumed that Alice will transform the state first, followed by Bob, followed by the measurements. However, the same results are obtained for any order of transformations and measurements. As soon as Alice measures, e.g., the state collapses to one where Alice's result is known, and Bob may transform this remaining single qubit (corresponding to multiplication with a 2×2 matrix), and measure it later on. The result will be the same (exercise).

No cloning

A central feature of Quantum Mechanics is that it is impossible to produce an exact copy of an arbitrary quantum state:

Theorem 24.9 (No-Cloning Theorem): There is no quantum operation that effectively implements the mapping $|\varphi\rangle \otimes |e\rangle \mapsto |\varphi\rangle \otimes |\varphi\rangle$, for an arbitrary state $|\varphi\rangle$ (of some source system) and state $|e\rangle$ of some target system.

Proof sketch: We can take $|\varphi\rangle$ to be a qubit $\alpha|0\rangle + \beta|1\rangle$. The desired result state needs to have the form $|\varphi\rangle \otimes |\varphi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$. All of these factors are quadratic functions in the amplitudes of $|\varphi\rangle$, hence not linear. A unitary matrix can therefore not implement this. □

Cloning Heisenberg: No cloning relates to the Uncertainty Principle, which prevents us from learning exact values of all aspects of a quantum system. If we could make perfect copies, we could measure whatever we wanted as often as we wanted – and if we could measure all aspects, we could manufacture a copy.

Summary and Outlook

Quantum Mechanics is a highly successful theory of physical reality

At its heart, it is based on probability distributions represented by unit vectors in the Euclidian norm – called (pure) states.

Probabilities can be modified by performing linear, norm-preserving transformations, captured conveniently in unitary matrices.

What's next?

- Quantum Computation proper
- Interactive Proof Systems
- Summary & consultation