Quantum Computing
SS 2020

Erich Grädel

RWTH Aachen University

Objectives of this course

- Introduction to the mathematical model of quantum computing
- Qubits, quantum registers, and unitary transformations
- Quantum gate arrays
- The most important quantum algorithms, in particular quantum Fourier transformation and Shor's factoring algorithm.

Prerequisites: complex numbers, linear algebra, basics of the theory of computation

We shall not cover the physics of quantum computing and the question of how one could possibly build a quantum computer.

Unit 1

- A brief history (well, actually two)
- An experiment
- Postulates of Quantum Mechanics
- Hilbert spaces, unitary transformations, tensor products, and all that
- Qubits, quantum registers, and measurements
- Entanglement
- Sorry, no cloning!

A completely different story

Flying machines have been a dream of mankind for many centuries.

Leonardo da Vinci (1452-1519): Several proposals for the construction of flying machines.

George Cayley (1773-1857): First rigorous study of the physics of flight and theoretical design of a fixed-wing, self-propelled aircraft.

But is it really possible to actually build flying machines?

Scepticism

I can state flatly that heavier than air flying machines are impossible.

Lord Kelvin, 1895

It is apparent to me that the possibilities of the aeroplane, which two or three years ago were thought to hold the solution to the [flying machine] problem, have been exhausted, and that we must turn elsewhere.

Thomas Edison, 1895

Flight by machines heavier than air is unpractical and insignificant, if not utterly impossible.

Simon Newcomb, 1902

It is complete nonsense to believe flying machines will ever work.

Stanley Mosley, 1905

A breakthrough: The Wright Flyer

On 17th December 1903, at Kitty Hawk, North Carolina, the Wright brothers, Orville and Wilbur, made what is viewed today as the first controlled, sustained flights of a self-powered, heavier-than-air aircraft, the Wright Flyer. The longest of them took 59 seconds and covered 260 metres.

" It was not the first vehicle to fly,
it did not solve any pressing transportation problem,
it did not herald the widespread adoption of planes,
it did not mark the end of other modes of transportation.

But it has shown a new operational regime: the self-propelled flight of an aircraft that is heavier than air. This event has its place in history because of what it represents, not what it practically accomplished."

Wiliam D. Oliver: Quantum computing takes flight, Nature, October 2019

A brief history of quantum computing

1980/82: Yuri Manin and, independently, Richard Feynman make the point that certain physical phenomena cannot be efficiently simulated by a classical computer.

> *. . . because nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.*
>
> *Richard P. Feyman, 1982*

Speculation about the possibility to make use of quantum mechanical phenomena, such as superposition, entanglement and interference, to build quantum computers to accomplish tasks that would be impossible or prohibitively expensive for classical computers.

A brief history of quantum computing (2): Models and algorithms

1985 -1993: Deutsch, Bernstein-Varizani, and others develop theoretical models for quantum computing such as Quantum Turing Machines and Quantum Gate Arrays.

Quantum complexity classes

Simple quantum algorithms indicate that certain problems can be solved much more efficiently by quantum computers than classical ones. However, these were artificial problems without practical value.

1994: Peter Shor presents a polynomial-time quantum algorithm for the integer factorization problem.

Thus, quantum computers, if they can indeed be built, could break common and widely used encryption schemes such as RSA.

A brief history of quantum computing (3): A challenge

It is still unclear, whether sufficiently large and stable quantum computers can actually be built.

Quantum supremacy: A challenge formulated by Preskill (2012). Show that

> *. . . well controlled quantum systems can perform tasks surpassing what can be done in the classical world. One way to achieve such "quantum supremacy" would be to run an algorithm on a quantum computer which solves a problem with a super-polynomial speedup relative to classical computers . . .*

A brief history of quantum computing (4): Scepticism

Quantum computing is all the rage [. . .] Most commentators forget, or just gloss over, the fact that people have been working on quantum computing for decades — and without any practical results to show for it.

Mikhail Dyakonov, 2018

Noisy quantum systems will not allow building quantum error-correcting codes needed for quantum computation.

Gil Kalai, 2019

The quality of qubits and gates cannot be improved beyond a certain threshold that is quite close to the best currently existing qubits and gates.

Gil Kalai, 2019

A brief history of quantum computing (5): More scepticism

I believe that our universe is not a miraculous one, allowing exponential speed-ups over the natural model of computation.

Oded Goldreich, 2004

In light of all this, it's natural to wonder: When will useful quantum computers be constructed? The most optimistic experts estimate it will take 5 to 10 years. More cautious ones predict 20 to 30 years. (Similar predictions have been voiced, by the way, for the last 20 years.) I belong to a tiny minority that answers: Not in the foreseeable future.

Mikhail Dyakonov, 2018

A brief history of quantum computing (6): A breakthrough ?

2019: A team of researchers, led by the Google AI Quantum Group, reports on an experiment claimed to establish quantum supremacy.

Sycamore, a quantum processor with 53 qubits and 86 links between qubits, performed a task related to random number generating: sampling the output of a pseudo-random quantum circuit.

While Sycamore sampled the solutions in 200 seconds, classical sampling at the same fidelity is claimed to take 10.000 years, and full verification would take several million years.

It is not universally accepted that the experiment really establishes quantum supremacy, but some researchers see it as milestone comparable to the Wright brothers' first flights.

Wiliam D. Oliver: Quantum computing takes flight, Nature, October 2019

A simple experiment

Photons are the only particles we can directly observe. Illustrate some aspects of quantum mechanics through polarization of photons.

Equipment: A powerful light source and three polarisation filters, which polarise light horizontally ($\rightarrow$), vertically ($\uparrow$), and diagonally ($\nearrow$)

Observations:

- If only the horizontal filter ($\rightarrow$) is put in front of the light source, 50% of light passes through.
- If the vertical polarisation filter ($\uparrow$) is put in front of the horizontal filter, 50% of light passes through the first filter and the remaining light is completely blocked by the second filter.
- If the diagonal filter ($\nearrow$) is put between ($\rightarrow$) and ($\uparrow$), from the light emitted by the source, 50% passes through the first filter, 25% passes through the first two filters, and 12.5% passes through all three filters.

Explanation

Describe the polarisation state of a photon by $|\varphi\rangle := \alpha|\uparrow\rangle + \beta|\rightarrow\rangle$ in a two-dimensional vector space with basis $\{|\uparrow\rangle, |\rightarrow\rangle\}$.

The direction of the vector is all that matters: consider unit vectors with $|\alpha|^2 + |\beta|^2 = 1$.

Instead of the basis $\{|\uparrow\rangle, |\rightarrow\rangle\}$, we could also take $\{|\nearrow\rangle, |\searrow\rangle\}$ or any other pair of orthogonal unit vectors.

Measurement of a state $|\varphi\rangle$ wrt. basis $\{|\uparrow\rangle, |\rightarrow\rangle\}$:

Projection of $|\varphi\rangle = \alpha|\uparrow\rangle + \beta|\rightarrow\rangle$ to either $|\uparrow\rangle$ (with probability $|\alpha|^2$) or to $|\rightarrow\rangle$ (with probability $|\beta|^2$).

After the measurement, the state $|\varphi\rangle$ is destroyed: it has been transformed into one of the basic states $|\uparrow\rangle$ or $|\rightarrow\rangle$. There is no way to gain back $|\varphi\rangle$, and each successive measurement gives the same result as the first one.

Explanation

A filter with angle ϑ has basis $\{\sin\vartheta|\uparrow\rangle + \cos\vartheta|\rightarrow\rangle, \cos\vartheta|\uparrow\rangle - \sin\vartheta|\rightarrow\rangle\}$.

The horizontal and vertical filters have $\{|\uparrow\rangle, |\rightarrow\rangle\}$, whereas the diagonal filter $(\nearrow)$ has basis $\{|\nearrow\rangle, |\searrow\rangle\} = \left\{\frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle), \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\rightarrow\rangle)\right\}$.

The photons that, after measurement, correspond to the polarisation, pass through the filter; the others are reflected.

Filter $(\rightarrow)$ projects 50% of the photons to $|\rightarrow\rangle$ and lets them pass; the other 50% are projected to $|\uparrow\rangle$ and reflected. Filter $(\uparrow)$ reflects all photons projected to $|\rightarrow\rangle$. Hence, no light passes if filter $(\uparrow)$ if it is put behind filter $(\rightarrow)$.

Filter $(\nearrow)$ projects a photon in state $|\rightarrow\rangle = \frac{1}{\sqrt{2}}|\nearrow\rangle - \frac{1}{\sqrt{2}}|\searrow\rangle$ with probability $\frac{1}{2}$ to $|\nearrow\rangle$. If filter $(\nearrow)$ is put between filters $(\rightarrow)$ and $(\uparrow)$, then 25% of the photons pass through the first two filters and are then in state $|\nearrow\rangle$. Since $|\nearrow\rangle = \frac{1}{\sqrt{2}}|\rightarrow\rangle + \frac{1}{\sqrt{2}}|\uparrow\rangle$, half of these are projected by $(\uparrow)$ to $|\uparrow\rangle$ and pass.

Postulates of Quantum Mechanics

Four postulates of quantum mechanics for describing physical systems:

States. A state is a complete description of a physical system at a given time. It is described by a unit vector in a Hilbert space.

Compositions. The state space of a composite system is the tensor product of the state spaces of its components.

Dynamics. A closed physical system evolves by unitary transformations.

Measurements. A measurement with a set M of possible outcomes is given by a collection $\{P_m : m \in M\}$ of linear projection operators. Measurements are probabilistic, outcome m appears with a probability $p(m)$. A measurement of a state $|\psi\rangle$ with outcome m projects the state to $\frac{1}{\sqrt{p(m)}} P_m |\psi\rangle$.

We explain the meaning of the postulates in the context of quantum computing

Hilbert spaces

A Hilbert space H is a vector space over the field $\mathbb{C}$ of complex numbers, with inner product

$$\langle \cdot \mid \cdot \rangle : H \times H \to \mathbb{C}, \qquad \text{with}$$

- $\langle \psi \mid \varphi \rangle = \langle \varphi \mid \psi \rangle^*$
  (for a complex number $z = a + ib$, its conjugate is $z^* = a - ib$).
- $\langle \psi \mid \psi \rangle \geq 0$ (note that $\langle \psi \mid \psi \rangle \in \mathbb{R}$) and $\langle \psi \mid \psi \rangle = 0$ if, and only if, $|\psi\rangle = 0$.
- $\langle \psi \mid \alpha\varphi_1 + \beta\varphi_2 \rangle = \alpha\langle \psi \mid \varphi_1 \rangle + \beta\langle \psi \mid \varphi_2 \rangle$.

Note that $\||\psi\rangle\| := \sqrt{\langle \psi \mid \psi \rangle}$ defines a norm on H.

For infinite dimensional Hilbert spaces (not used in this course), it is further required that H is complete (with respect to $\|\cdot\|$), i.e. that any Cauchy sequence has a limit.

Dual vectors and orthonormal basis

In quantum mechanics, one uses Dirac notation $|\psi\rangle$ (read "ket ψ") for vectors. The zero vector is 0 (not $|0\rangle$, which might be a different vector).

For every vector $|\psi\rangle \in H$, its dual vector is the linear function

$$\langle\psi| : H \longrightarrow \mathbb{C} \quad \text{(read "bra } \psi\text{")}, \text{ with}$$
$$|\varphi\rangle \longmapsto \langle\psi\,|\,\varphi\rangle.$$

An orthonormal basis of a Hilbert space H is a basis $\{|e_1\rangle, \ldots, |e_n\rangle\}$ such that

$$\langle e_i\,|\,e_j\rangle = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j, \end{cases}$$

In particular, $\||e_i\rangle\| = 1$ for all $i = 1, \ldots, n$.

Outer product

With a pair of vectors $|\psi\rangle \in H_1$ and $|\varphi\rangle \in H_2$, we associate the linear operator $|\psi\rangle\langle\varphi| : H_2 \to H_1$, called the outer product of $|\psi\rangle$ and $|\varphi\rangle$,

$$(|\psi\rangle\langle\varphi|) : |\varphi'\rangle \longmapsto \langle\varphi \,|\, \varphi'\rangle|\psi\rangle$$

$|\psi\rangle\langle\psi|$ is the projection on the one-dimensional space generated by $|\psi\rangle$

Every linear operator can be written as a linear combination of outer products. Given a basis $\{|1\rangle, \ldots, |n\rangle\}$, we write

$$A = \sum_{i,j} a_{ij} |i\rangle\langle j|$$

Eigenvalues

An eigenvector of a linear operator $A : H \to H$ is a non-zero vector $|\psi\rangle$ with

$$A|\psi\rangle = \lambda|\psi\rangle, \text{ for some } \lambda \in \mathbb{C}.$$

λ ist the eigenvalue corresponding to $|\psi\rangle$.

A is diagonalisable if $A = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$ for an orthonormal basis of eigenvectors $|\psi_i\rangle$ with corresponding eigenvalues λ_i.

In this basis, we can the write A as a matrix

$$\begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$$

Adjoints

With any linear operator $A : H \to H$, we associate its adjoint $A^\dagger$ which satisfies

$$\langle \varphi \,|\, A\psi \rangle = \langle A^\dagger \varphi \,|\, \psi \rangle.$$

In terms of matrices, $A^\dagger = (A^*)^T$ (the conjugate transposed matrix to A)

Example: $$\begin{pmatrix} 1+\mathrm{i} & 1-\mathrm{i} \\ -1 & 1 \end{pmatrix}^\dagger = \begin{pmatrix} 1-\mathrm{i} & -1 \\ 1+\mathrm{i} & 1 \end{pmatrix}$$

Caution: The notation $A^\dagger$ is common in quantum mechanics. From mathematics, you may be used to a different notation such as A^* (used here for the conjugate of A).

Normal, Hermitian and unitary operators

A linear operator $A : H \to H$ is normal if $AA^\dagger = A^\dagger A$. This is necessary and sufficient for A being diagonalisable.

$A : H \to H$ is Hermitian if $A^\dagger = A$. A Hermitian operator is normal, hence diagonalisable and has only real eigenvalues.

A linear operator $A : H \to H$ is unitary if $AA^\dagger = A^\dagger A = I$

Unitary operators are diagonalisable, invertible, and preserve inner products: $\langle A\varphi \,|\, A\psi \rangle = \langle \varphi \,|\, \psi \rangle$, and hence $\|A|\psi\rangle\| = \||\psi\rangle\|$.

The eigenvalues of a unitary operator have the form $\lambda = e^{i\varphi}$

Qubits

Bit: Elementary building block for the state space of a classical computational system, with two possible states: 0 and 1

Quantum bit or qubit: Superposition of these states. Qubits are the elementary units for quantum computation.

Fix orthonormal basis vectors $|0\rangle$ and $|1\rangle$ of a two-dimensional Hilbert space H^2.

A qubit is a unit vector $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ in H^2, with $|\alpha|^2 + |\beta|^2 = 1$.

Measurement of a qubit

Any measurement (with the standard basis) of $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ results with probability $|\alpha|^2$ in $|0\rangle$, and with probability $|\beta|^2$ in $|1\rangle$.

The associated projection operators are $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$.

After the measurement, the qubit is in the measured state $|0\rangle$ or $|1\rangle$.

Any repeated measurement leads to the same result. Although a qubit can take infinitely (in fact, uncountably) many values, one can extract from it only one bit of classical information.

Measurement is a probabilistic process

n-Qubit Systems (Quantum Registers)

A classical system with n bits has 2^n states:

$$00\cdots00, \quad 00\cdots01, \quad \ldots \quad 11\cdots10, \quad 11\cdots11$$

A n-qubit system has 2^n base states

$$|00\cdots00\rangle, \quad |00\cdots01\rangle, \quad \ldots \quad |11\cdots10\rangle, \quad |11\cdots11\rangle$$

and its state can be any superposition

$\alpha_0|00\cdots0\rangle + \alpha_1|00\cdots1\rangle + \cdots + \alpha_{2^n-1}|11\cdots1\rangle$ with $\sum_{i<2^n} |\alpha_i|^2 = 1$

The state space of an n-qubit system is the 2^n-dimensional Hilbert space

$$H^{2^n} = H^2 \otimes H^2 \otimes \cdots \otimes H^2$$

Composition classically and quantum mechanically

Classical physics: Combining a state space V with basis $\{|v_1\rangle, \ldots, |v_m\rangle\}$ and a state space W with basis $\{|w_1\rangle, \ldots, |w_n\rangle\}$ produces a product space $V \times W$, with basis $\{|v_1\rangle, \ldots, |v_m\rangle, |w_1\rangle, \ldots, |w_m\rangle\}$ and $\dim(V \times W) = \dim V + \dim W$.

Quantum mechanics: Combining V and W as above results in the product space $V \otimes W$ with basis $\{|v_i\rangle \otimes |w_j\rangle : i = 1, \ldots, m, j = 1, \ldots n\}$ and $\dim(V \otimes W) = \dim V \cdot \dim W$

The dimension grows exponentially with the number of components

Notation: $|vw\rangle$ or $|v\rangle|w\rangle$ for $|v\rangle \otimes |w\rangle$ and
$|v_1 v_2 \cdots v_n\rangle$ for $|v_1\rangle \otimes |v_2\rangle \otimes \cdots \otimes |v_n\rangle$

Measuring one qubit

If we measure the first qubit of an n-qubit state

$$|\psi\rangle = \sum_{v \in \{0,1\}^n} \alpha_v |v\rangle$$

we obtain $|0\rangle$ with probability $p = \sum_{w \in \{0,1\}^{n-1}} |\alpha_{0w}|^2$, with projection to

$$|0\rangle \otimes \frac{1}{\sqrt{p}} \sum_{w \in \{0,1\}^{n-1}} \alpha_{0w} |w\rangle,$$

and we get $|1\rangle$ with probability $q = \sum_{w \in \{0,1\}^{n-1}} |\alpha_{1w}|^2$, with projection to

$$|1\rangle \otimes \frac{1}{\sqrt{q}} \sum_{w \in \{0,1\}^{n-1}} \alpha_{1w} |w\rangle.$$

Measurement in general

Any measurement is associated with a set M of possible outcomes, and with linear projection operators $\{P_m : m \in M\}$ with $\sum_{m \in M} P_m^\dagger P_m = I$.

A measurement of a state $|\psi\rangle$ produces outcome m with probability

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

and projects the the state to $\frac{1}{\sqrt{p(m)}} P_m |\psi\rangle$. Note that

$$\sum_{m \in M} p(m) = \sum_{m \in M} \langle \psi | P_m^\dagger P_m | \psi \rangle = \langle \psi | I | \psi \rangle = 1.$$

Entangled states

For every pair $|\psi\rangle = \sum_i a_i |v_i\rangle \in V$ and $|\varphi\rangle = \sum_j b_j |w_j\rangle \in W$, we have in $V \otimes W$ the vector $|\psi\rangle \otimes |\varphi\rangle = \sum_{i,j} a_i b_j (|v_i\rangle \otimes |w_j\rangle)$

But: Not every vector $|\vartheta\rangle \in V \otimes W$ can be written as a product $|\vartheta\rangle = |\psi\rangle \otimes |\varphi\rangle$ with $|\psi\rangle \in V$ and $|\varphi\rangle \in W$!

Example: For $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \in H^2 \otimes H^2$ there are no $|\varphi_1\rangle, |\varphi_2\rangle \in H^2$ with $|\psi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle$.

Otherwise,
$|\psi\rangle = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) = ac|00\rangle + ad|01\rangle + bc|01\rangle + bd|11\rangle$.
Hence $ad = bc = 0$ which implies that, also, either $ac = 0$ or $bd = 0$.
Contradiction!

Such non-decomposable states are called entangled.

Measuring entangled states

We compare the two (2 qubit) states

$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) \quad \text{and} \quad \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Measuring the first qubit for the left, decomposable, state gives $|0\rangle$ with probability 1, and the state remains unchanged.

However, measuring the first qubit in the right, entangled, state (called an EPR pair), gives $|0\rangle$ or $|1\rangle$ with equal probability $1/2$, and after this, the second qubit is also determined.

Dynamics

The evolution of a closed (unmeasured) quantum system is described by the Schrödinger equation

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle$$

where $\hbar$ is Planck's constant and H is a Hermitian operator, the Hamiltonian of the system.

If the system is in state $|\psi\rangle$ at time 0, then the state $|\psi(t)\rangle$ at time t is determined by $|\psi(t)\rangle = U(t)|\psi\rangle$, for the operator $U(t)$ with

$$U(t) = \exp(\frac{-iH(t)}{\hbar})$$

Lemma. If $H(t)$ is Hermitian, then $U(t)$ is unitary.

In quantum computing, time is discrete and we speak of computational steps.

Global phase and physical indistinguishable states

Consider two states $|\psi\rangle$ and $e^{i\varphi}|\psi\rangle$, for any $0 < \varphi < 2\pi$.

- For any unitary operator U, we have that $Ue^{i\varphi}|\psi\rangle = e^{i\varphi}U|\psi\rangle$.
- For any measurement operator P_m, we have that

$$\langle\psi|e^{-i\varphi}P_m^\dagger P_m e^{i\varphi}|\psi\rangle = \langle\psi|P_m^\dagger P_m|\psi\rangle.$$

Thus, such a global phase $e^{i\varphi}$ is unobservable and the two states are physically indistinguishable.

Caution. Even if $|\psi\rangle$ and $e^{i\varphi}|\psi\rangle$ are physically indistinguishable, this need not be the case for states $|\psi'\rangle + |\psi\rangle$ and $|\psi'\rangle + e^{i\varphi}|\psi\rangle$.

Quantum gates and quantum gate arrays

A quantum gate on m qubits is a unitary tranformation $U : H^{2^m} \to H^{2^m}$ on the 2^m-dimensional Hilbert space $H^{2^m} = H^2 \otimes \cdots \otimes H^2$.

A quantum gate array (or quantum circuit) is a sequence of applications of quantum gates to specific qubits.

The fact that quantum mechanical processes, and quantum computation in particular, can only evolve by unitary transformations, has severe consequences:

- Quantum computations are reversible
- It is not possible to simply copy arbitrary qubits

The No-Cloning Theorem

Theorem. Let H^n be any Hilbert space of dimension $n > 1$. There is no unitary transformation $\text{Copy} : H^n \otimes H^n \to H^n \otimes H^n$ such that,

$$\text{Copy}(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle$$

for some $|0\rangle \in H^n$ and all $|\psi\rangle \in H^n$.

Proof. Assume that Copy and $|0\rangle$ exist. Since $n > 1$, there exists a unit vector $|1\rangle$ that is orthogonal to $|0\rangle$. For $\psi = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, we have

$$\begin{aligned}\text{Copy}(|\psi\rangle|0\rangle) &= \tfrac{1}{\sqrt{2}}(\text{Copy}(|0\rangle|0\rangle) + \text{Copy}(|1\rangle|0\rangle)) \\ &= \tfrac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \neq |\psi\rangle|\psi\rangle\end{aligned}$$

because $|\psi\rangle|\psi\rangle = \frac{1}{2}(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle)$. Contradiction.