Introduction to Quantum Computation

Overview:

- From bits to qubits: Dirac notation, multipartite quantum states, measurements
- Quantum gates & quantum circuits: circuit model, basic gates, oracles, Deutsch-Jozsa algorithm

From bits to qubits

- classical states for computation are either "0" or "1"
- in quantum mechanics, a state can be in superposition, i.e., simultaneously in "0" and "1"
  - → superpositions allow to perform calculations on many states at the same time
    - ⇒ quantum algorithms with exponential speed-up

  BUT: once we measure the superposition state, it collapses to one of its states
  (→ we can only get one "answer" and not all answers to all states in the superposition)
  - ⇒ it is not THAT easy to design quantum algorithms, but we can use interference effects
    (→ "wrong answers" cancel each other out, while the "right answer" remains)

Dirac notation

- used to describe quantum states: Let $a, b \in \mathbb{C}^d$ (→ d-dimensional vectors with complex entries)
  - ket: $|a\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_d \end{pmatrix}$
  - bra: $\langle b| = |b\rangle^\dagger = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_d \end{pmatrix}^\dagger = (b_1^* \; b_2^* \; \dots \; b_d^*)$ (complex conjugated & transposed)
  - bra ket: $\langle b|a\rangle = a_1 b_1^* + a_2 b_2^* + \dots + a_d b_d^* = \langle a|b\rangle^* \in \mathbb{C}$ (→ complex number) (inner product)
  - ket-bra: $|a\rangle\langle b| = \begin{pmatrix} a_1 b_1^* & a_1 b_2^* & \dots & a_1 b_d^* \\ a_2 b_1^* & & & \vdots \\ \vdots & & & \\ a_d b_1^* & & \dots & a_d b_d^* \end{pmatrix}$ (→ d x d - matrix) (not an "X" ☺)
- usually we look at qubits ($d=2$) and set $|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
  - → $|0\rangle$ and $|1\rangle$ are orthogonal: $\langle 0|1\rangle = 1 \cdot 0 + 0 \cdot 1 = 0$
- all quantum states are normalized, i.e. $\langle \psi|\psi\rangle = 1$, e.g. $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Multipartite quantum states

- we use tensor products to describe multiple states: $|a\rangle \otimes |b\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ \vdots \\ b_d \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ \vdots \\ a_1 b_d \\ a_2 b_1 \\ \vdots \\ a_d b_d \end{pmatrix}$
- example: system A is in state $|\psi\rangle_A = |1\rangle_A$ and system B in state $|\psi\rangle_B = |0\rangle_B$
  - ⇒ the total (bipartite) state is $|\psi\rangle_{AB} = |1\rangle_A \otimes |0\rangle_B = |10\rangle_{AB} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$

  ↳ remark: states of this form are called uncorrelated, but there are also bipartite states that cannot be written as $|\psi\rangle_A \otimes |\psi\rangle_B$. These states are correlated and sometimes even entangled (very strong correlation), e.g. $|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$
  a so-called Bell state, used for teleportation, cryptography, Bell tests, etc.

Measurements

- we choose orthogonal bases to describe & measure quantum states (→ projective measurement)
  e.g. we could measure whether the spin of an electron is "up" or "down", corresp. to a projection onto the basis $\{|\uparrow\rangle := |0\rangle,\ |\downarrow\rangle := |1\rangle\}$ (most common)
- there are infinitely many different bases, but another common one is $\{|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),\ |-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$, which corresponds to spin "right" or "left"
- **Born rule**: the probability that a state $|\psi\rangle$ collapses during a projective meas. onto the basis $\{|x_i\rangle\}_i$ to the state $|x_i\rangle$ is given by

$$P(x_i) = |\langle x_i|\psi\rangle|^2, \qquad \sum_i P(x_i) = 1$$

- example: - $|\psi\rangle = \frac{1}{\sqrt{3}}\cdot(|0\rangle + \sqrt{2}\cdot|1\rangle)$ is measured in the basis $\{|0\rangle, |1\rangle\}$:

$$\rightarrow P(0) = |\langle 0|\tfrac{1}{\sqrt{3}}(|0\rangle + \sqrt{2}|1\rangle)|^2 = |\tfrac{1}{\sqrt{3}}\underbrace{\langle 0|0\rangle}_{1} + \sqrt{\tfrac{2}{3}}\underbrace{\langle 0|1\rangle}_{0}|^2 = \frac{1}{3} \rightarrow \text{analogously } P(1) = \frac{2}{3}$$

- $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ is measured in the basis $\{|+\rangle, |-\rangle\}$:

$$P(+) = |\langle +|\psi\rangle|^2 = |\tfrac{1}{\sqrt{2}}(\langle 0| + \langle 1|)\cdot\tfrac{1}{\sqrt{2}}\cdot(|0\rangle - |1\rangle)|^2 = \frac{1}{4}|\underbrace{\langle 0|0\rangle}_{1} - \underbrace{\langle 0|1\rangle}_{0} + \underbrace{\langle 1|0\rangle}_{0} - \underbrace{\langle 1|1\rangle}_{1}|^2$$

$= 0$ → expected, as $\langle +|\psi\rangle = \underbrace{\langle +|-\rangle}_{\text{orthogonal}} = 0$

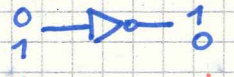
Quantum gates & circuits

- "circuit model": sequence of building blocks that carry out elementary computations, called gates, connected by wires

input → [algorithm] → output

Single-qubit gates

- classical example: NOT



- basic quantum gates: as quantum theory is unitary, gates are represented by unitary matrices: $U^\dagger U = \mathbb{1}$
  - $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$

Dirac notation

$\hookrightarrow \sigma_x\cdot|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\cdot\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$, $\sigma_x|1\rangle = (|0\rangle\langle 1| + |1\rangle\langle 0|)\cdot|1\rangle = |0\rangle\underbrace{\langle 1|1\rangle}_{1} + |1\rangle\underbrace{\langle 0|1\rangle}_{0} = |0\rangle$

⇒ bit flip ≙ NOT gate e.g. $|0\rangle$ — [σ_x] — $|1\rangle$

  - $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$

$\hookrightarrow \sigma_z\cdot|+\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\cdot\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle$, $\sigma_z|-\rangle = (|0\rangle\langle 0| - |1\rangle\langle 1|)\cdot\frac{1}{\sqrt{2}}\cdot(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$

⇒ phase flip

  - $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = i\cdot\sigma_x\cdot\sigma_z$ ⇒ bit & phase flip

⇒ σ_x, σ_y & σ_z are the so-called Pauli-matrices and $\sigma_i^2 = \mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (does nothing)

→ together with identity $\mathbb{1}$ they form a basis of 2×2 matrices
(→ any 1-qubit rotation can be written as a linear combination of them)

  - Hadamard gate: one of the most important gates for quantum circuits

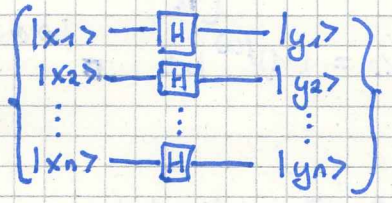
$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)$$

$\hookrightarrow H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\cdot\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\cdot\begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle$, $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)\cdot|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$

· for $x \in \{0,1\}^n$: $|x\rangle$ — H — $|y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle) = \frac{1}{\sqrt{2}}\left((-1)^{0\cdot x}|0\rangle + (-1)^{1\cdot x}|1\rangle\right)$

$= \frac{1}{\sqrt{2}} \cdot \sum_{k\in\{0,1\}} (-1)^{k\cdot x}|k\rangle$

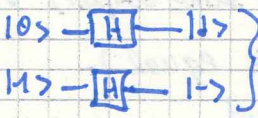
· for $x \in \{0,1\}^n$:



$|x\rangle \to |y\rangle = H^{\otimes n}\cdot|x\rangle = \frac{1}{\sqrt{2^n}} \cdot \sum_{k\in\{0,1\}^n} (-1)^{\langle k|x\rangle}|k\rangle$ (inner product)

↳ every $|y_i\rangle$ is either $|+\rangle$ or $|-\rangle$, so $|y\rangle$ must be a superposition of all possible 2^n bit strings

e.g. $|x\rangle = |01\rangle$:



$\to |y\rangle = |+\rangle \otimes |-\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$

Two-qubit gates

· classical example: XOR

→ irreversible (↳ given the output we cannot recover the input)

BUT: as quantum theory is unitary, we only consider unitary and therefore reversible gates

· quantum example: $CNOT = \begin{pmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&0&1\\ 0&0&1&0 \end{pmatrix} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|$

↳ $CNOT \cdot |00\rangle_{xy} = CNOT \cdot \begin{pmatrix}1\\0\\0\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} = |00\rangle_{xy}$, $CNOT \cdot |10\rangle_{xy} = |11\rangle_{xy}$

input x y	output x $x \oplus y$
0 0	0 0
0 1	0 1
1 0	1 1
1 1	1 0

⇒ circuit:

≙ reversible XOR

⇒ we can show that every function f can be described by a reversible circuit

⇒ quantum circuits can perform all functions that can be calculated classically

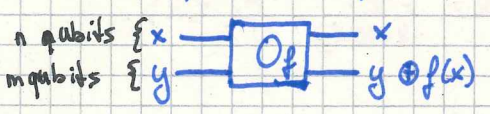
Oracles

· we use the model of query complexity: assume we have access to an oracle, e.g. a physical device that we cannot look inside, to which we can pass queries and which returns answers

→ goal: determine some property of the oracle using the minimal number of queries

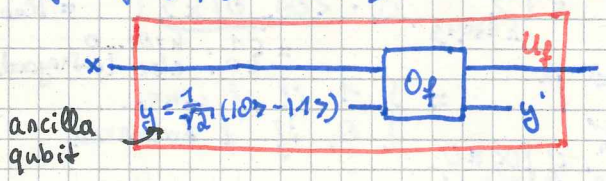
· on a classical computer, the oracle is given by a fct. $f: \underbrace{\{0,1\}^n}_{\text{input string}} \to \underbrace{\{0,1\}^m}_{\text{output string}}$

· on a quantum computer, the oracle must be reversible:



O_f: bit oracle, can be seen as a unitary which performs the map $O_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$

→ for $f: \{0,1\}^n \to \{0,1\}$, we can construct U_f:



U_f: phase oracle, which performs the map

$U_f|x\rangle = (-1)^{f(x)}\cdot|x\rangle$

↳ homework (or for the coffee break): check this!

in case there is enough time:

$$O_f|x\rangle|y\rangle = \frac{1}{\sqrt{2}}\left(|x\rangle|0\oplus f(x)\rangle - |x\rangle|1\oplus f(x)\rangle\right) = \begin{cases} \frac{1}{\sqrt{2}}|x\rangle\cdot(|0\rangle-|1\rangle) = |xy\rangle, & \text{if } f(x)=0 \\ \frac{1}{\sqrt{2}}|x\rangle\cdot(|1\rangle-|0\rangle) = -|xy\rangle, & \text{if } f(x)=1 \end{cases}$$

$$= (-1)^{f(x)}\cdot|xy\rangle$$

$|x\rangle\otimes(-|y\rangle) = -|xy\rangle = (-|x\rangle)\otimes|y\rangle$

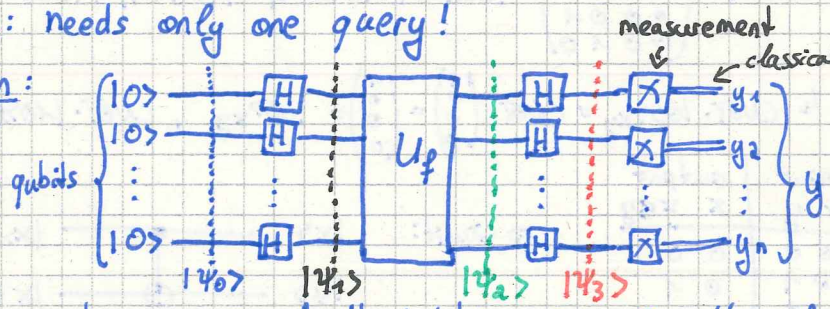
$\Rightarrow$ independent of $|y\rangle$: $O_f|x\rangle = (-1)^{f(x)}|x\rangle$ ■

Deutsch-Jozsa algorithm

- We are given a fct. $f: \{0,1\}^n \to \{0,1\}$, realized by an oracle, of which we know that it is either constant (→ all inputs map to the same output) or balanced (# inputs that map to '0' and '1' is equal).
- Task: Determine whether f is constant or balanced.
- classical solution: we need to ask the oracle at least twice, but if we get twice the same value, we need to ask again, ...
  → at most $\frac{N}{2}+1 = 2^{n-1}+1$ queries, n: # input bits, $N=2^n$: # realizable bitstrings

  demonstrative example: 2^n different ways to throw a coin → is the coin fair?
- quantum solution: needs only one query!

DJ-algorithm:



Claim: If the outcome y equals the bitstring $\underbrace{00\ldots0}_{n}$, then f is constant, otherwise it is balanced.

Proof: Let us check the state after every step:

- $|\psi_0\rangle = |0\rangle^{\otimes n} = |00\ldots0\rangle$
- $|\psi_1\rangle = H^{\otimes n}\cdot|\psi_0\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}\underbrace{(-1)^{\langle x|\psi_0\rangle}}_{=+1}\cdot|x\rangle = \frac{1}{\sqrt{2^n}}\cdot\sum_{x\in\{0,1\}^n}|x\rangle$ ($\langle x|\psi_0\rangle = \langle x|00\ldots0\rangle$)
- $|\psi_2\rangle = U_f\cdot|\psi_1\rangle \overset{\text{linearity}}{=} \frac{1}{\sqrt{2^n}}\cdot\sum_{x\in\{0,1\}^n}U_f\cdot|x\rangle = \frac{1}{\sqrt{2^n}}\cdot\sum_{x\in\{0,1\}^n}(-1)^{f(x)}\cdot|x\rangle$
- $|\psi_3\rangle = H^{\otimes n}\cdot|\psi_2\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}\cdot H^{\otimes n}\cdot|x\rangle$

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

$$= \sum_{k\in\{0,1\}^n}\underbrace{\left[\frac{1}{2^n}\cdot\sum_{x\in\{0,1\}^n}(-1)^{f(x)+\langle k|x\rangle}\right]}_{=:c_k}\cdot|k\rangle = \sum_{k\in\{0,1\}^n}c_k\cdot|k\rangle$$

$\Rightarrow$ probability to measure the zero-string $|00\ldots0\rangle$:

$$P[y=00\ldots0] \overset{\text{Born rule}}{=} |\langle 00\ldots0|\psi_3\rangle|^2 = \left|\sum_{k\in\{0,1\}^n}c_k\cdot\underbrace{\langle 00\ldots0|k\rangle}_{=\begin{cases}1, & k=00\ldots0\\ 0, & \text{else (orthogonal)}\end{cases}}\right|^2 = |c_{00\ldots0}|^2$$

$$= \left|\frac{1}{2^n}\cdot\sum_{x\in\{0,1\}^n}(-1)^{f(x)}\right|^2 = \begin{cases}1, & \text{if } f \text{ const.}\\ 0, & \text{if } f \text{ balanced}\end{cases}$$

$\underbrace{\quad}_{=\begin{cases}+2^n, & \text{if } f(x)\equiv 0\\ -2^n, & \text{if } f(x)\equiv 1\\ 0, & \text{if } f(x) \text{ balanced}\end{cases}}$

■