Quantum Computing and Quantum Communication

Lecture 1

Michal Kloc

http://quantumtheory-bruder.physik.unibas.ch

winter semester 2020

A little bit of historical context and timeline

- 1920s: foundations of quantum mechanics (QM)
  Schrödinger, Heisenberg, Planck...
- 1960s-70s: intersection of QM with information theory
  Bell, Bennett, Holevo...
- early 1980s: conceptual ideas of quantum computation
  Benioff, Feynman...

'The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines'

Paul Benioff, *J Stat Phys* 22, 563–591 (1980)

"How can we simulate the quantum mechanics?. . . .Can you do it with a new kind of computer - a quantum computer? It is not a Turing machine, but a machine of a different kind."

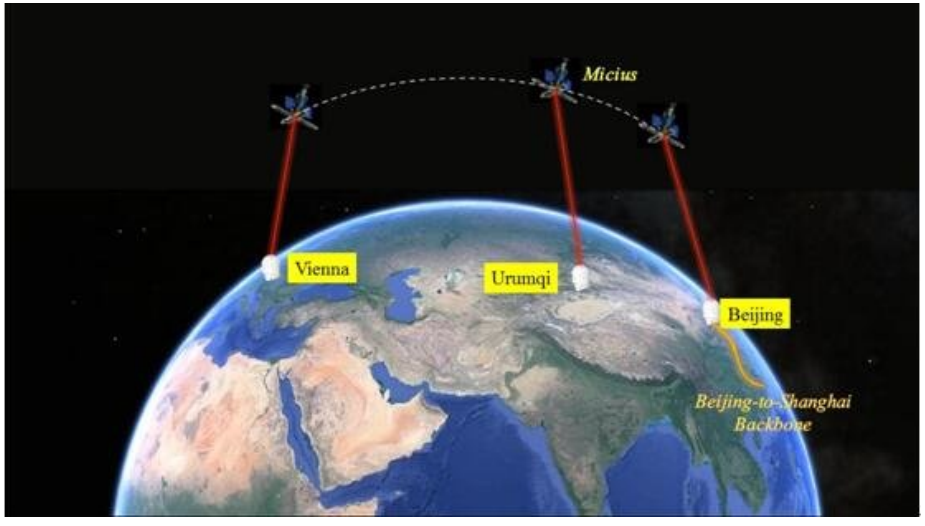
Richard Feynman, 1981

A little bit of historical context and timeline

- early 1990s: quantum algorithms

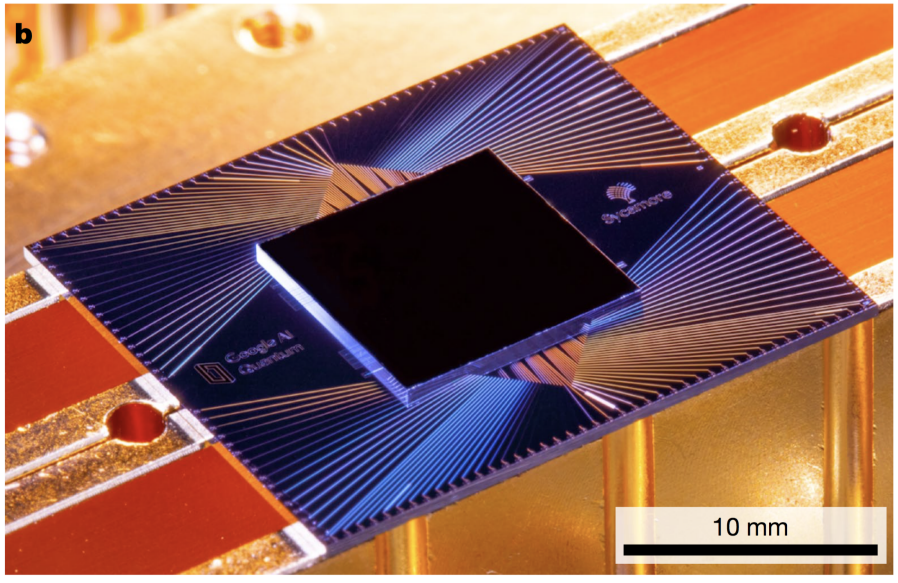
  Deutsch, Shor...
- after 2000: dramatic progress in realizations of experimental platforms
  - quantum annealers (D-Wave)
  - quantum simulators (cold atoms in optical lattices, trapped ions)
  - different qubit realizations (superconducting circuits etc.)
  - hybrid systems

Where are we now?



Quantum communication link over 7600 km distance established:

Phys. Rev. Lett. **120**, 030501 (2018)



"Quantum supremacy" demonstrated by Google:
quantum computer: 200 s
classical computer: 10.000 a (?)

Nature **574**, 505 (2019)

Outline of the lectures

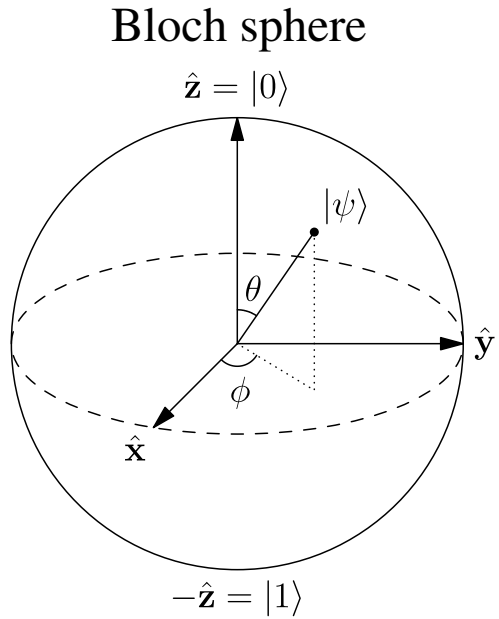
- building blocks of quantum information
  - quantum bits (qubits)
  - superposition and entanglement
  - gates and universal computation
  - Deutsch algorithm
- decoherence, quantum error correction, no-cloning theorem, quantum teleportation
- quantum cryptography, quantum "hardware"

References

- N. D. Mermin, *Quantum computer science*, Cambridge University Press
- M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*, Cambridge University Press
- Lecture notes by C. Bruder, R. Tiwari, N. Lörch and M. Koppenhöffer

Quantum bits

- a classical computer manipulates bits:
  possible states 0 or 1 are *discrete*
- a quantum computer manipulates qubits
  $\equiv$ *quantum two-level systems*:
  possible states $(\alpha|0\rangle + \beta|1\rangle)$ are *continuous*
  α, β are complex numbers, $|\alpha|^2 + |\beta|^2 = 1$.
- general qubit state parametrized by two angles $\theta \in [0, \pi]$, $\phi \in [0, 2\pi)$



$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{i\phi}|1\rangle$$

$$\alpha = |\alpha|\, e^{i\phi_\alpha},\ \beta = |\beta|\, e^{i\phi_\beta}$$

parametrize $|\alpha| = \cos\theta/2$, $|\beta| = \sin\theta/2$, $\phi = \phi_\beta - \phi_\alpha$

- state of a system = state vector $|\psi\rangle$ in a Hilbert space $\mathcal{H}$
- operators act on states (e.g., Hamiltonian operator $\hat{H}$)
- observables represented by Hermitian operators (real spectrum)

$$\hat{H}^\dagger = \hat{H}$$

- Schrödinger equation here for simplicity $\hat{H} \neq \hat{H}(t)$

$$i\hbar \frac{\mathrm{d}}{\mathrm{d}t}|\Psi\rangle = \hat{H}|\Psi\rangle \rightsquigarrow |\Psi(t)\rangle = \mathrm{e}^{-\frac{i}{\hbar}\hat{H}t}|\Psi(0)\rangle$$

$$\hat{U}(t) \equiv \mathrm{e}^{-\frac{i}{\hbar}\hat{H}t}, \text{ evolution operator}$$

$$\hat{U}^\dagger \hat{U} = \hat{U}\hat{U}^\dagger = 1, \text{ unitary evolution}$$

- states can be written as linear combination (*superposition*) of orthonormal basis states $\{|n\rangle\}$

$$|\Psi\rangle = \sum_n \gamma_n |n\rangle$$

- probabilistic outcomes of measurements
  probability of finding the state $|\Psi\rangle$ in some $|\tilde{n}\rangle \in \{|n\rangle\}$

$$P_\Psi(\tilde{n}) = |\langle\tilde{n}|\Psi\rangle|^2 = |\gamma_{\tilde{n}}|^2$$

- normalization requires

$$\sum_n |\gamma_n|^2 = 1$$

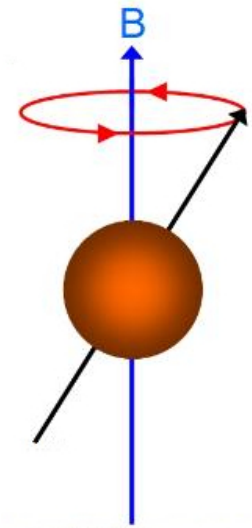
Example of a quantum two-level system: spin $\frac{1}{2}$

- $\dim \mathcal{H} = 2$
  - physical state $|\uparrow\rangle \rightarrow$ logical state $|0\rangle$
  - physical state $|\downarrow\rangle \rightarrow$ logical state $|1\rangle$
- operators acting on one qubit can be *represented* by 2×2 matrices
- e.g., in the basis of eigenstates of $\hat{\sigma}_z$, $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$:

  Pauli matrices:

$$\hat{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \ , \ \hat{\sigma}_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \ , \ \hat{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- all two-level systems are mathematically equivalent!



Multi-qubit states

- 2 bits can represent 4 numbers: 00, 01, 10, 11
- 2 qubits $\Rightarrow$ 4 basis states
  - $|0\rangle_1 \otimes |0\rangle_2$
  - $|0\rangle_1 \otimes |1\rangle_2$
  - $|1\rangle_1 \otimes |0\rangle_2$
  - $|1\rangle_1 \otimes |1\rangle_2$
- we omit the indices $1, 2$ and write $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$
- 2-qubit state: $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$, where $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$
- similarly, we define 3-qubit, 4-qubit, ... N-qubit states
- for N qubits, we have 2^N basis states
  $\Rightarrow$ simulating quantum systems on classical computers is hard!

remember Feynman's quote...

- quantum nature shows non-classical correlations: entanglement
- classical N-bit states can be "factorized"

Example: classical state (11)

- bit 1 is in state "1", bit 2 is in state "1"
- equivalent quantum state: $|11\rangle = |1\rangle \otimes |1\rangle$

- But there are quantum states that cannot be factorized

Example: state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \neq |\psi_1\rangle \otimes |\psi\rangle_2$

- system can only be described as a whole

entanglement (formal definition)

Let $\mathcal{H}$ be a composite system $\mathcal{H} = \mathcal{H}_\mathsf{l} \otimes \mathcal{H}_\mathsf{r}$. We denote orthonormal bases on $\mathcal{H}_\mathsf{l}$ and $\mathcal{H}_\mathsf{r}$ as $\{|\psi_{\mathsf{l}i}\rangle\}_{i=1}^m$ and $\{|\psi_{\mathsf{r}j}\rangle\}_{j=1}^n$. A general state $|\Psi\rangle \in \mathcal{H}$ can be expressed as

$$|\Psi\rangle = \sum_{i=1}^{m}\sum_{j=1}^{n} \gamma_{ij}|\psi_{\mathsf{l}i}\rangle|\psi_{\mathsf{r}j}\rangle \neq \sum_{i=1}^{m} \alpha_i|\psi_{\mathsf{l}i}\rangle \sum_{j=1}^{n} \beta_j|\psi_{\mathsf{r}j}\rangle,$$

i. e. the coefficients γ_{ij} cannot be generally factorized as $\gamma_{ij} \neq \alpha_i\beta_j$.

Informally: In the case of a general state I cannot tell which part of $|\Psi\rangle$ belongs to $\mathcal{H}_l$ and which to $\mathcal{H}_r$. They are entangled.

- where the non-classical correlations show up?

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

- What happens if we measure $\hat{\sigma}_z$ on qubit 1 and qubit 2?
- either we get 0 for qubit 1 and 0 for qubit 2 (probability $\frac{1}{2}$)
- or we get 1 for qubit 1 and 1 for qubit 2 (probability $\frac{1}{2}$)
- but never any "mixed" result

Multi-qubit states; Superposition vs. entanglement

- $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$: superposition of two 1-qubit states
- $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$: entangled superposition of two 2-qubit states

$$|\psi\rangle = \frac{1}{2}(|00\rangle + |10\rangle + |01\rangle + |11\rangle)$$

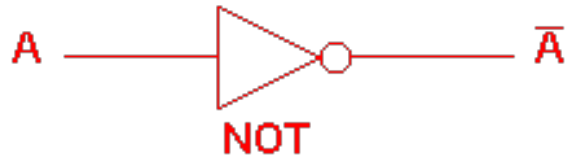
- superposition state?
- entangled state?
- $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
  $\Rightarrow$ non-entangled superposition of four 2-qubit states

Logical operations

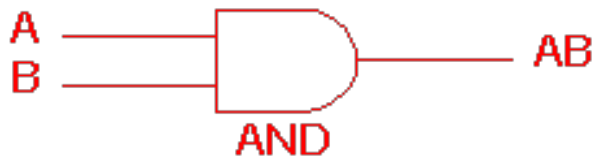
classical gates:
electronic circuits

Many gates process the classical information in a *non-reversible* way

From the output of AND one cannot restore A and B .



NOT gate	
A	$\overline{A}$
0	1
1	0



2 Input AND gate		
A	B	A.B
0	0	0
0	1	0
1	0	0
1	1	1

2 Input OR gate		
A	B	A+B
0	0	0
0	1	1
1	0	1
1	1	1

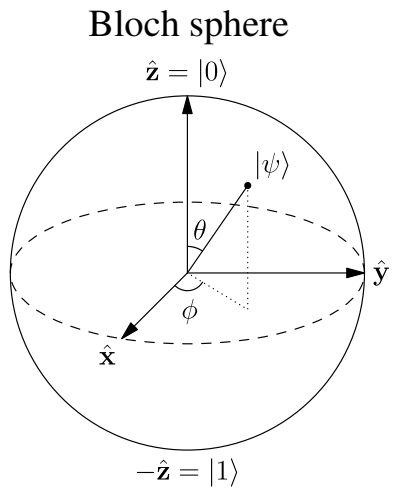
Logical operations

- classical NOT gate:

$$\text{NOT } 0 = 1$$
$$\text{NOT } 1 = 0$$

- quantum NOT gate: $\hat{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

- $\hat{\sigma}_x|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$
- $\hat{\sigma}_x|1\rangle = |0\rangle$
- $\hat{\sigma}_x\left(\alpha|0\rangle + \beta|1\rangle\right) = \alpha|1\rangle + \beta|0\rangle$



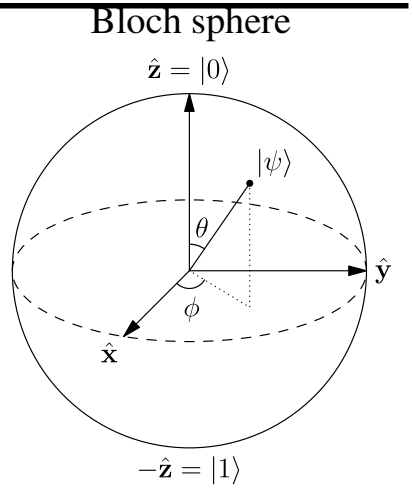
Properties of quantum gates

- quantum gates are linear transformations of state vectors
- N-qubit gate can be represented by a $2^N \times 2^N$ matrix $\hat{U}$
- $\hat{U}$ must be unitary to preserve normalization of state vector:

$$\hat{U}\hat{U}^\dagger = \hat{U}^\dagger\hat{U} = \mathbb{1}$$

$\Rightarrow$ quantum gates are *reversible*!

Single qubit gates



- NOT gate: $\hat{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$$\hat{\sigma}_x|0\rangle = |1\rangle$$
$$\hat{\sigma}_x|1\rangle = |0\rangle$$

- Hadamard gate: $\hat{H} = \frac{1}{\sqrt{2}}(\hat{\sigma}_x + \hat{\sigma}_z) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$$\hat{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \equiv |+\rangle, \quad \hat{\sigma_x}|+\rangle = |+\rangle$$
$$\hat{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \equiv |-\rangle, \quad \hat{\sigma_x}|-\rangle = -|-\rangle$$

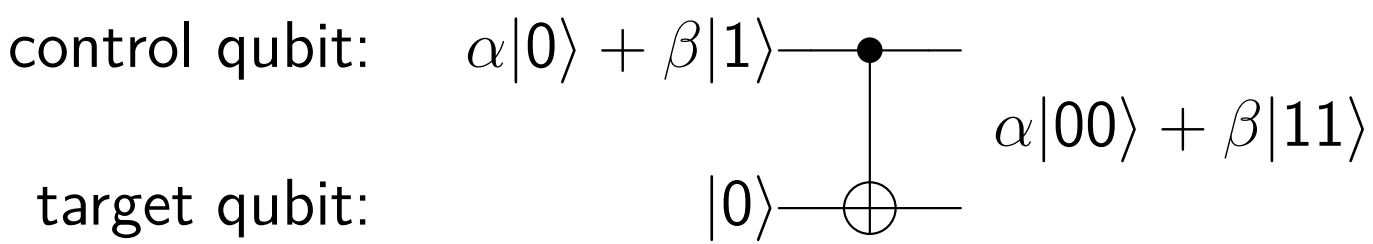
any single qubit gate can be decomposed into rotations on the Bloch sphere, see the exercise sheet...

Controlled NOT gate (CNOT)

- 2-qubit gate
- flip second (target) qubit if first (control) qubit is $|1\rangle$:

$$
\begin{aligned}
|00\rangle &\to |00\rangle \\
|01\rangle &\to |01\rangle \\
|10\rangle &\to |11\rangle \\
|11\rangle &\to |10\rangle
\end{aligned}
\qquad
\mathrm{CNOT} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & & 1 \\ & & 1 & \end{pmatrix}
$$

- circuit diagram:



Example: generating Bell states

maximally entangled
2-qubit states

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

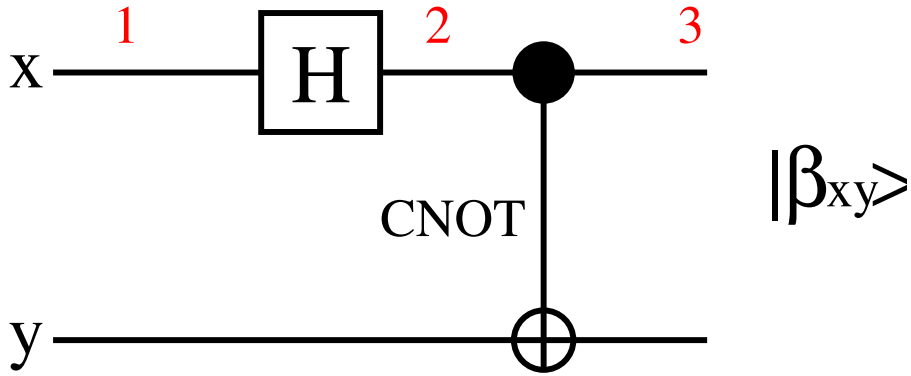
$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

General expression:

$$\boxed{|\beta_{xy}\rangle = \tfrac{1}{\sqrt{2}}(|0y\rangle + (-1)^x|1\bar{y}\rangle)}$$



1. input state: $|xy\rangle = |00\rangle$
2. apply Hadamard gate $\hat{H} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$: $\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$
3. apply CNOT gate: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\beta_{00}\rangle$

Toffoli gate

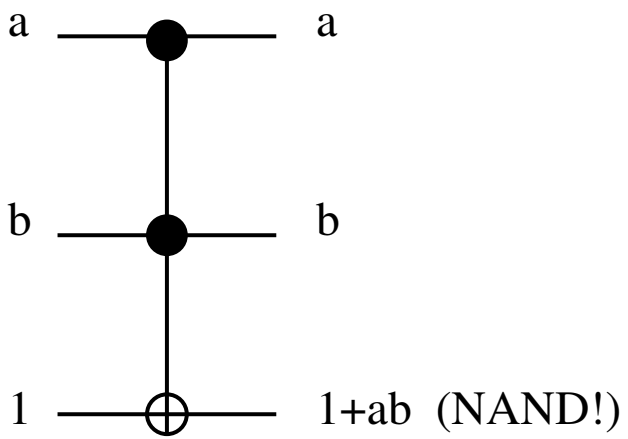
- 3-qubit gate
- flip third (target) qubit if the first two (control) qubits are $|1\rangle$
- in basis $|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, $|101\rangle$, $|110\rangle$, $|111\rangle$:

$$\mathcal{T} = \begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & & 1 \\ & & & & & & 1 & \end{pmatrix}$$

- $\mathcal{T}\mathcal{T} = \mathbb{1} \Rightarrow \mathcal{T}^{-1} = \mathcal{T}$, Toffoli gate is reversible

Toffoli gate

- Toffoli gate can simulate a classical NAND gate



input			output		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Can a quantum circuit simulate a classical logical circuit?

- of course (world around us is quantum !!)
- but: all unitary quantum logic gates are inherently reversible whereas many classical logic gates are irreversible
- classical NAND gate is universal, i.e., all classical logic gates can be built using only NAND gates
  $\{\mathrm{AND}, \mathrm{NOT}\}$ form a *functionally complete* set
- using Toffoli gates, any classical algorithm can be made reversible $\Rightarrow$ can be executed on a quantum computer

Note for universal quantum computation, one needs CNOT, $\hat{H}$, phase gate $\hat{S} = \begin{pmatrix} 1 & \\ & i \end{pmatrix}$, and $\pi/8$ gate $\hat{T} = \begin{pmatrix} 1 & \\ & e^{i\pi/4} \end{pmatrix}$

Is $f(x) : \{0,1\} \to \{0,1\}$ balanced or constant?

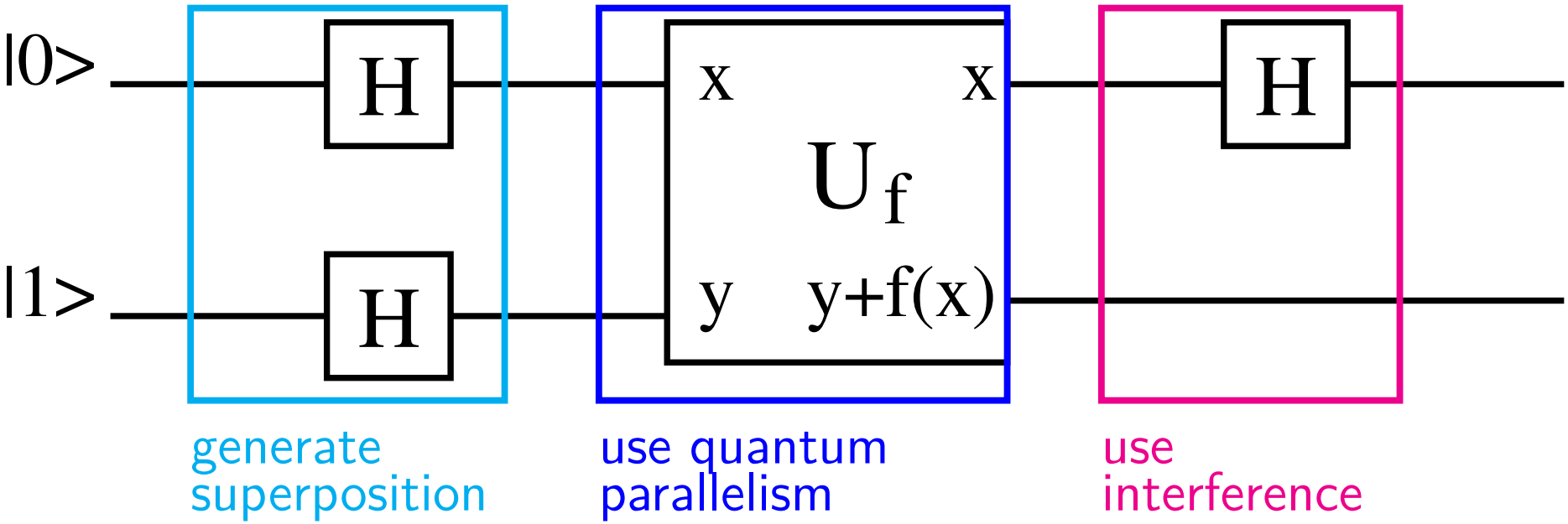
- balanced if $f(0) = \overline{f(1)} \Leftrightarrow f(0) \oplus f(1) = 1$
- constant if $f(0) = f(1) \Leftrightarrow f(0) \oplus f(1) = 0$

- $\hat{U}_f : |x, y\rangle \to |x, y \oplus f(x)\rangle$ quantum circuit implementing $y + f(x) \mod 2$ in the second qubit
- example: input $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|y\rangle = |0\rangle$ leads to

$$\frac{1}{\sqrt{2}} \left(|0, f(0)\rangle + |1, f(1)\rangle\right)$$

  $\Rightarrow$ one "application" of f results in both $f(0)$ and $f(1)$!
- but: measurement gives either $|0, f(0)\rangle$ or $|1, f(1)\rangle$
- so, quantum parallelism does not help ...?

- ...it does if we transform the information in a clever way:



- final state is $\propto |f(0) \oplus f(1)\rangle \otimes (|0\rangle - |1\rangle)$

  $\Rightarrow$ measuring the first qubit gives a global property of f, namely $f(0) \oplus f(1)$, using only one evaluation of $f(x)$

- this is impossible on a classical computer!

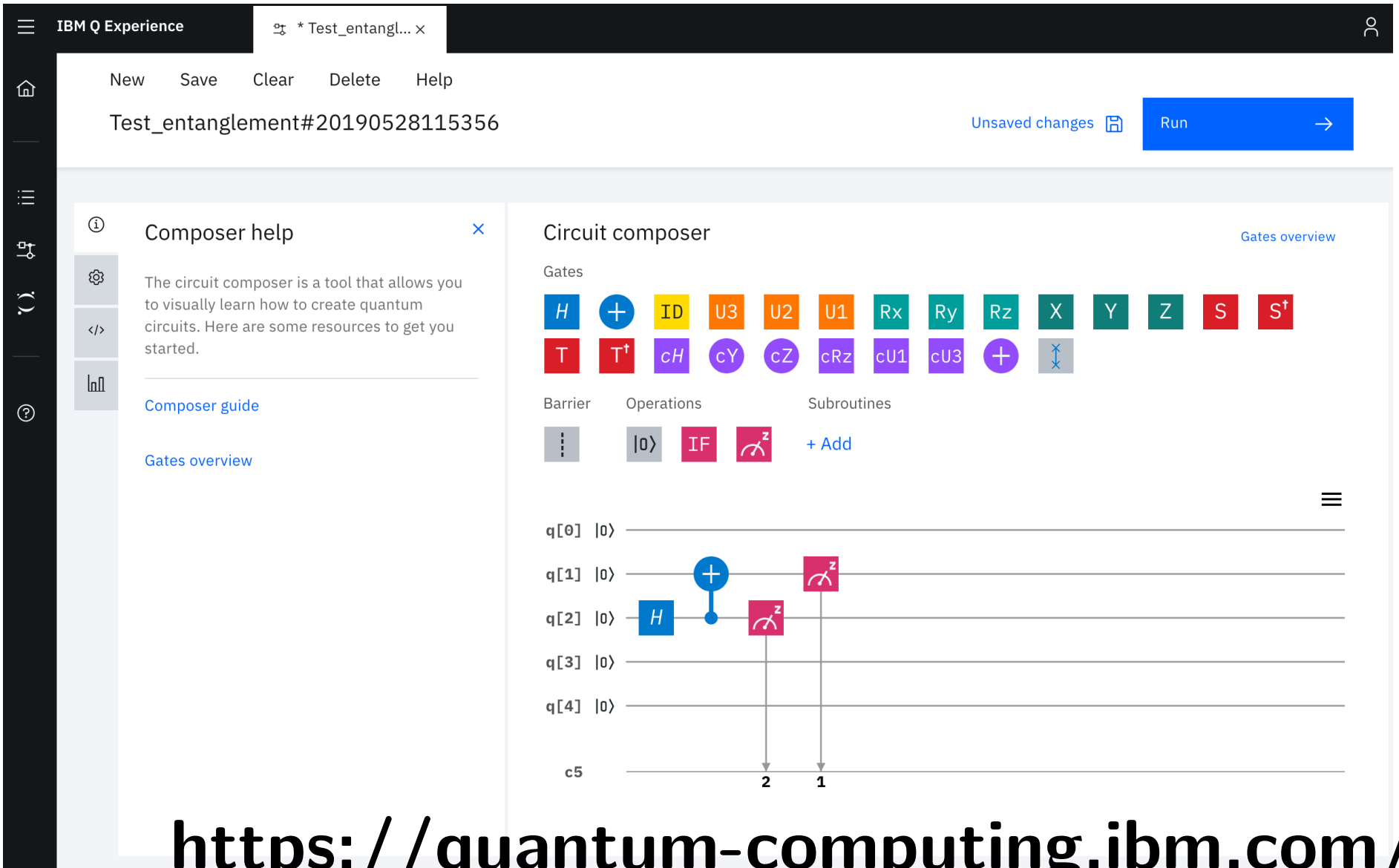
The power of quantum computing

- computation = unitary (reversible) evolution of a set of qubits
- gates act on (possibly entangled) superposition of states
  $\Rightarrow$ high degree of parallelism
- restrictions on readout of quantum information
  $\Rightarrow$ use interference to condense information for measurement
- N-qubit generalization of Deutsch algorithm and Shor's prime-factoring algorithm show exponential speedup compared to classical algorithms (but the same problems could in principle also be solved on a classical computer)

Main take-home messages of Lecture 1

- Any two-level quantum system can encode a qubit
- Logical operations performed by quantum gates = operators on the system's Hilbert space
- Quantum circuits can perform all operations performed by classical circuits
- Quantum superposition and entanglement allow for quantum parallelism = dramatic speedup in computational times

Try quantum computing yourself



https://quantum-computing.ibm.com/