Quantum Computing and Quantum Communication

Lecture 2

Michal Kloc

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

winter semester 2020

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

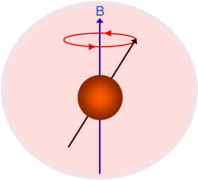
Main take-home messages of Lecture 1

- 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

So far perfectly *isolated* systems $\leftrightarrow$ *unitary* evolution

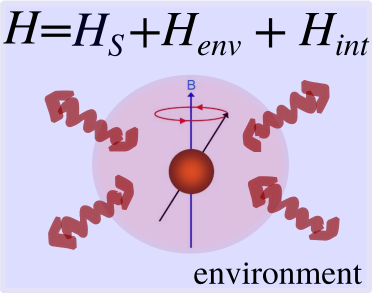
$$|\Psi(t)\rangle = \hat{U}(t)|\Psi(0)\rangle, \ \hat{U}^\dagger \hat{U} = \hat{U}\hat{U}^\dagger = 1$$

H_S



So far perfectly *isolated* systems $\leftrightarrow$ *unitary* evolution

$$|\Psi(t)\rangle = \hat{U}(t)|\Psi(0)\rangle, \; \hat{U}^\dagger \hat{U} = \hat{U}\hat{U}^\dagger = 1$$



In reality no system is perfectly isolated from its environment

Density matrix formalism

pure state $|\Psi\rangle$:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightsquigarrow \rho = |\Psi\rangle\langle\Psi|,$$

$$\text{density matrix: } \rho = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix}$$

- off-diagonal elements: coherences $\leftrightarrow$ ‘quantumness’
- probabilistic interpretation: $\mathrm{Tr}\{\rho\} = 1$
  diagonal terms: populations w.r.t the given basis $\{|0\rangle, |1\rangle\}$
- for pure states $\mathrm{Tr}\{\rho^2\} = 1$

Density matrix formalism, decoherence

$|\Psi\rangle \rightsquigarrow$ measurement in $\{|0\rangle, |1\rangle\}$ basis but no access to the results $\rightsquigarrow$ What can I say about the state of the system?

- with probability $|\alpha|^2$ in $|0\rangle$, with probability $|\beta|^2$ in $|1\rangle$
- *statistical mixture*: $\rho = |\alpha|^2 |0\rangle\langle 0| + |\beta|^2 |1\rangle\langle 1|$

$$\rho = \begin{pmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{pmatrix}$$

- no coherences
- $\mathrm{Tr}\{\rho\} = 1$, $\mathrm{Tr}\{\rho^2\} < 1$

- effectively, that is what environment does! $\rightsquigarrow$ decoherence
- coherences decay over a specific time scale τ_D
- operations on a quantum computer must we significantly faster! $\tau_{\mathrm{switch}} \ll \tau_D$
- For more on this topic see the relevant literature
  - H.-P. Breuer, F. Petruccione, *The theory of open quantum systems*, Oxford University Press

Already at the classical level $\rightsquigarrow$
classical error correction

- bit flip $(0 \leftrightarrow 1)$ is the most general classical single-bit error
- assume a bit-flip error happens at probability p per unit time
  $\Rightarrow$ a bit is corrupted after $\mathcal{O}(1/p)$ steps

Introduce redundancy:

- two-bit encoding: $0 \to 00$ and $1 \to 11$
- the strings 00 and 11 both have even parity
- if we detect an odd parity string, an error has occurred
- but how to correct it?

Increase redundancy:

- three-bit encoding: $0 \to 000$, $1 \to 111$ — error probability
- what if one error occurs? — $\to 3p(1-p)^2$

  $\Rightarrow$ can be corrected by "majority voting"
- what if two errors occur simultaneously? — $\to 3p^2(1-p)$

  $\Rightarrow$ error correction works incorrectly
- what if three errors occur simultaneously? — $\to p^3$

  $\Rightarrow$ error is undetectable

error correction is worth doing if $3p^2(1-p) + p^3 < 3p(1-p)^2$
(i.e., two and three bit flip errors are much rarer that single bit flips)
$\Rightarrow$ need $p \ll 1$

Adopt the ideas from the classical error correction, but carefully!

No-cloning theorem

Copying an arbitrary quantum state is impossible.

- Assume there is a "cloning operator" $\hat{A}$:

$$\hat{A}|\alpha\rangle|0\rangle = |\alpha\rangle|\alpha\rangle \text{ for all initial states } \alpha$$

- For $|\alpha\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$: $\hat{A}|\alpha\rangle|0\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)$
- On the other hand, $\hat{A}$ must be **linear**:

$$\hat{A}|\alpha\rangle|0\rangle = \frac{1}{\sqrt{2}}(\hat{A}|0\rangle|0\rangle + \hat{A}|1\rangle|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$$

- Contradiction!

Note however, recreating a state in one location is possible at the expense of destroying it in another location (teleportation)

Obstacles to quantum error correction?

- no-cloning theorem $\Rightarrow$ we cannot copy qubits
- detecting errors needs measurements $\Rightarrow$ destroys quantum superposition

Surprisingly, we can still correct errors:

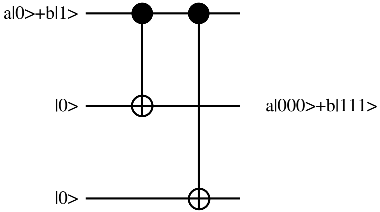
- consider bit-flip error $|0\rangle \leftrightarrow |1\rangle$
- corresponds to NOT gate $\hat{\sigma}_x$
- embed single-qubit state in a three-qubit state:

$$|\psi_{\mathrm{logical}}\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow |\psi_{\mathrm{encoded}}\rangle = \alpha|000\rangle + \beta|111\rangle$$

- we have not copied $|\psi_{\mathrm{logical}}\rangle$, no violation of no-cloning theorem! (instead we created a three-qubit entangled state)

Quantum error correction; encoding circuit

- Use CNOT: $\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle$

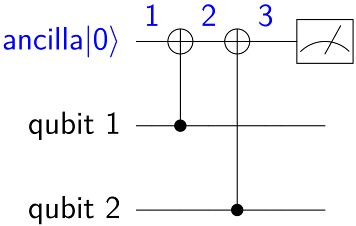


- Single bit-flip error can result in (i.e., applying σ_x)

$$\alpha|100\rangle + \beta|011\rangle \text{ or}$$
$$\alpha|010\rangle + \beta|101\rangle \text{ or}$$
$$\alpha|001\rangle + \beta|110\rangle$$

- If we know the parities of qubits 1 and 2, and qubits 2 and 3, we know which error (if any) has occurred

Measuring the parity of two qubits



1: $(\alpha|01\rangle + \beta|10\rangle) \otimes |0\rangle$

2: $\alpha|01\rangle \otimes |0\rangle + \beta|10\rangle \otimes |1\rangle$

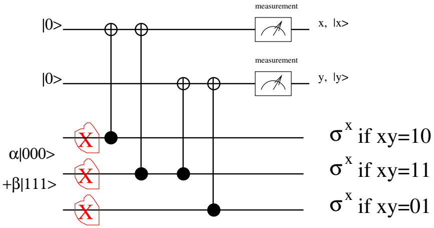
3: $\alpha|01\rangle \otimes |1\rangle + \beta|10\rangle \otimes |1\rangle$

$= (\alpha|01\rangle + \beta|10\rangle) \otimes |1\rangle$

- state of the ancilla qubit after step 3 is $|0\rangle$ if the parity of qubits 1 and 2 is even, and $|1\rangle$ if it is odd
- measurement of the ancilla qubit does not provide any information on α and β

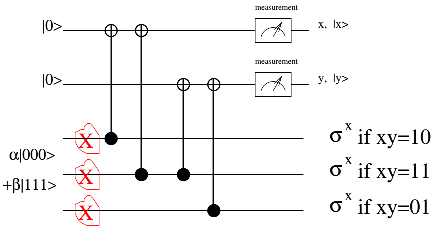
  $\Rightarrow$ superposition will not be destroyed

Correction circuit



- Alice sends $\alpha|000\rangle + \beta|111\rangle$
- with probability p, a bit-flip error $(\hat{\sigma}_x)$ occurs on a qubit
- Bob receives $\alpha|000\rangle + \beta|111\rangle$ with probability $(1-p)^3$
- Bob receives $\alpha|100\rangle + \beta|011\rangle$ with probability $p(1-p)^2$
- Bob receives $\alpha|010\rangle + \beta|101\rangle$ with probability $p(1-p)^2$
- Bob receives $\alpha|001\rangle + \beta|110\rangle$ with probability $p(1-p)^2$
- ...

Correction circuit



- Bob determines the parities
- Bob gets $(\alpha|000\rangle + \beta|111\rangle)|00\rangle$ with probability $(1-p)^3$
- Bob gets $(\alpha|100\rangle + \beta|011\rangle)|10\rangle$ with probability $p(1-p)^2$
- Bob gets $(\alpha|010\rangle + \beta|101\rangle)|11\rangle$ with probability $p(1-p)^2$
- Bob gets $(\alpha|001\rangle + \beta|110\rangle)|01\rangle$ with probability $p(1-p)^2$
- ...
- Bob flips one qubit depending on the values x and y

Does error correction work?

- Bob gets $(\alpha|000\rangle + \beta|111\rangle)|00\rangle$ with probability $(1-p)^3$
- Bob gets $(\alpha|100\rangle + \beta|011\rangle)|10\rangle$ with probability $p(1-p)^2$
- Bob gets $(\alpha|010\rangle + \beta|101\rangle)|11\rangle$ with probability $p(1-p)^2$
- Bob gets $(\alpha|001\rangle + \beta|110\rangle)|01\rangle$ with probability $p(1-p)^2$
- Bob gets $(\alpha|110\rangle + \beta|001\rangle)|01\rangle$ with probability $p^2(1-p)$
- Bob gets $(\alpha|101\rangle + \beta|010\rangle)|11\rangle$ with probability $p^2(1-p)$
- Bob gets $(\alpha|011\rangle + \beta|100\rangle)|10\rangle$ with probability $p^2(1-p)$
- Bob gets $(\alpha|111\rangle + \beta|000\rangle)|00\rangle$ with probability p^3
- failure probability with error correction is $3p^2 - 2p^3 \approx \mathcal{O}(p^2)$
- failure probability without error correction is $\mathcal{O}(p)$
- suppression is more powerful with more qubits

- bit-flip error is only one kind of possible single-qubit error
- phase-flip error: $\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|0\rangle - \beta|1\rangle$
- corresponds to $\hat{\sigma}_z$ gate
- no classical equivalent

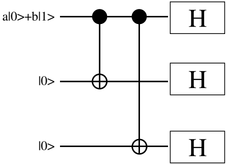
How to correct phase flip errors?

- turn phase-flip channel into bit-flip channel:
  i.e., phase flips become bit flips in the basis $\{|+\rangle, |-\rangle\}$

$$|+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|-\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Phase-flip error

- encode $\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|+++\rangle + \beta|---\rangle$:



- remaining detection and correction procedure stays the same, use $\hat{H}$ gates to switch between $|+\rangle, |-\rangle$ and $|0\rangle, |1\rangle$ basis
- combination of the bit-flip and the phase-flip code can protect against arbitrary errors: Shor's 9-qubit code

- Cloning a quantum state is impossible (no-cloning theorem)
- However, it is possible to teleport a quantum state:
- Alice and Bob have one half each of the Bell state

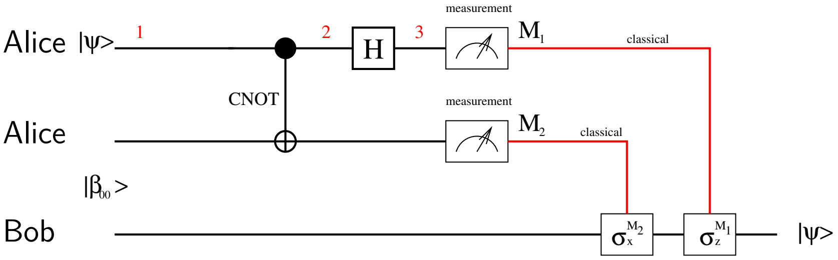
$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

- Alice can transmit an unknown state

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

to Bob using only classical information

Quantum teleportation



1: $|\psi\rangle \otimes |\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle\left(|00\rangle + |11\rangle\right) + \beta|1\rangle\left(|00\rangle + |11\rangle\right)\right]$

2: $\frac{1}{\sqrt{2}}\left[\alpha|0\rangle\left(|00\rangle + |11\rangle\right) + \beta|1\rangle\left(|10\rangle + |01\rangle\right)\right]$

3: $\frac{1}{2}\left[\alpha(|0\rangle + |1\rangle)\left(|00\rangle + |11\rangle\right) + \beta(|0\rangle - |1\rangle)\left(|10\rangle + |01\rangle\right)\right]$

$$= \frac{1}{2}\Big[\ |00\rangle\left(\alpha|0\rangle + \beta|1\rangle\right) + |01\rangle\left(\alpha|1\rangle + \beta|0\rangle\right)$$

$$+|10\rangle\left(\alpha|0\rangle - \beta|1\rangle\right) + |11\rangle\left(\alpha|1\rangle - \beta|0\rangle\right)\Big]$$

- the final state is

$$\frac{1}{2}\Big[\quad |00\rangle\,(\alpha|0\rangle+\beta|1\rangle) \\ +|01\rangle\,(\alpha|1\rangle+\beta|0\rangle) \\ +|10\rangle\,(\alpha|0\rangle-\beta|1\rangle) \\ +|11\rangle\,(\alpha|1\rangle-\beta|0\rangle)\Big]$$

- if Alice measures $|00\rangle$, Bob's system will be in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- if Alice measures something else and tells Bob (via classical communication), Bob can modify his state to be equal to $|\psi\rangle$

Main take-home messages of Lecture 2

- Any realistic quantum computer will be *noisy* due to uncontrolled interaction with environment.
- When information is transmitted we have to face two types of the errors: bit flips and phase flips
- Correction schemes are based on redundancy; to encode one *logical qubit* we need more *physical qubits*
- A quantum state cannot be simply copied from Alice to Bob (no-cloning theorem) but can be teleported provided that Alice and Bob share an auxiliary entangled state.