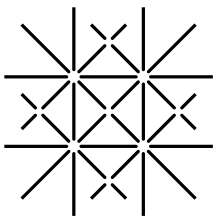
Quantum computing and quantum communication

Niels Loerch

niels.loerch@unibas.ch

December 13, 2017



Overview

- elements of quantum information
  - qubits
  - superposition and entanglement
  - 1- and 2-qubit gates
  - no-cloning theorem
  - Deutsch algorithm
- decoherence and error correction
- **ion trap quantum computer, quantum teleportation, quantum communication**

references:

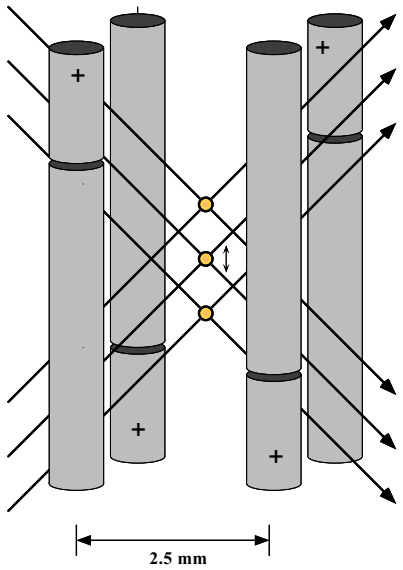
N.D. Mermin, Quantum computer science, Cambridge University Press
M.A. Nielsen and I.L. Chuang, Quantum computation and quantum information, Cambridge University Press
C. Gerry, P. Knight, Introductory Quantum Optics
Lecture notes by C. Bruder and R. Tiwari

www.quantumtheory.unibas.ch/people/loerch/

physical implementations of quantum bits

- Ions in magnetic traps Cirac and Zoller
- Superconducting qubits
- Electron spins in semiconductor quantum dots Loss and DiVincenzo
- ...

Trapped ions: physical setup



- N ions trapped in a harmonic electromagnetic trap
- Each qubit is encoded in two long-lived internal states $|g\rangle, |e\rangle$ of one ion.
- Motion of ions can be described as quantum harmonic oscillator. Common phonon mode is used as a quantum bus.
- Laser beams implement gates.

Trapped ions: Hamiltonian for one ion

- Hamiltonian $H = H_0 + H_I$.
- System Hamiltonian $H_0 = \frac{1}{2}\omega_0\sigma_z + \nu a^\dagger a$
  with frequency gap ω_0 between the ion's internal states
  ν frequency of motional mode, $a = \sum_n \sqrt{n}\,|n\rangle\langle n+1|$,
  $a^\dagger a = \sum_n n\,|n\rangle\langle n|$.
- Interaction Hamiltonian
  $H_I = Ee^{i\omega_L t - k_L\hat{x}} \cdot \mathcal{D}\sigma^- + h.c.$, with
  laser amplitude E, laser frequency ω_L, laser wave vector k_L,
  ion position $\hat{x} = x_{ZPF}(a + a^\dagger)$, dipole moment of the g-e
  transition: $\mathcal{D}$, $\sigma_- = |g\rangle\langle e|$.

Trapped ions: Effective Hamiltonian for one ion

- For small Lamb-Dicke parameter $\eta = k_L x_{ZPF} \ll 1$ we approximate $H_I = \mathcal{D} E e^{i\omega_L t}\sigma_-(1 - i\eta(a + a^\dagger)) + h.c.$
- In the interaction picture where $|\psi'\rangle = U|\psi\rangle$ with $U = \exp(-iH_0 t)$ we obtain $H_I = \mathcal{D} E e^{i(\omega_L - \omega_0)\mathbf{t}}\sigma_-(\mathbf{1} - i\eta(\mathbf{a}e^{i\nu\mathbf{t}} + \mathbf{a}^\dagger e^{-i\nu\mathbf{t}})) + h.c.$
- We can tune the laser detuning $\omega_L - \omega_0 = 0, -\nu, \nu$ to select resonant terms after a rotating wave approximation:
- $H \propto \sigma_- + \sigma_+ \propto \sigma_x$, single qubit gates
- $H \propto a\sigma_- + a^\dagger\sigma_+$, (phonon lasing)
- $H \propto a\sigma_+ + a^\dagger\sigma_-$, excitation swap for multi-qubit gates

Trapped ions: Sideband cooling

- We must initialize the system in the ground state.
- As optical frequencies are sufficiently high, the qubits are in the ground state. ($\bar{n} \approx k_B T / \hbar\omega$)
- The motional mode is in a thermal state, as its frequency is lower.
- However, we can use the swap interaction to cool the motional mode, by swapping its excitations to the ion.

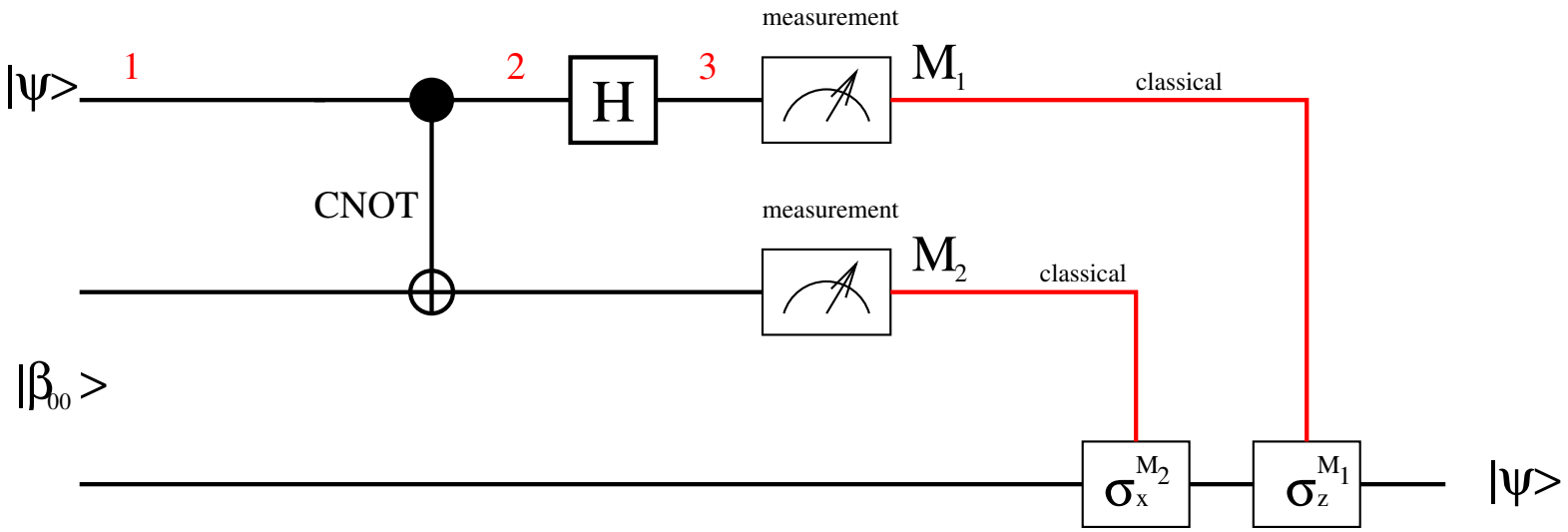
Trapped ions: Cirac-Zoller CNOT-gate

$$
\begin{array}{lcllcllcl}
 & \hat{U}_m^{1,0} & & & \hat{U}_n^{2,1} & & & \hat{U}_m^{1,0} & \\
|g\rangle_m|g\rangle_n|0\rangle & \longrightarrow & |g\rangle_m|g\rangle_n|0\rangle & \longrightarrow & |g\rangle_m|g\rangle_n|0\rangle & \longrightarrow & |g\rangle_m|g\rangle_n|0\rangle\,, \\
|g\rangle_m|e_0\rangle_n|0\rangle & \longrightarrow & |g\rangle_m|e_0\rangle_n|0\rangle & \longrightarrow & |g\rangle_m|e_0\rangle_n|0\rangle & \longrightarrow & |g\rangle_m|e_0\rangle_n|0\rangle\,, \\
|e_0\rangle_m|g\rangle_n|0\rangle & \longrightarrow & -i|g\rangle_m|g\rangle_n|1\rangle & \longrightarrow & i|g\rangle_m|g\rangle_n|1\rangle & \longrightarrow & |e_0\rangle_m|g\rangle_n|0\rangle\,, \\
|e_0\rangle_m|e_0\rangle_n|0\rangle & \longrightarrow & -i|g\rangle_m|e_0\rangle_n|1\rangle & \longrightarrow & -i|g\rangle_m|e_0\rangle_n|1\rangle & \longrightarrow & -|e_0\rangle_m|e_0\rangle_n|0\rangle\,.
\end{array}
$$

- We use the phonon mode as a bus, to make multiple ions interact. For example Cirac-Zoller CNOT gate.
- 0. Initialize phonon mode as $|0\rangle$.
- 1. Swap control qubit with phonon mode.
- 2. Cycle target qubits ground state through phonon mode and alternative excited state. $\Rightarrow$ obtain relative phase.
  (Note that $|g\rangle \to |g\rangle$, $|e\rangle \to -|e\rangle$ is NOT gate in $|\pm\rangle$ basis.)
- 3. Swap phonon mode back to control qubit.

Quantum teleportation

- Cloning a quantum state is impossible (no cloning theorem)
- However, it is possible to teleport it even if only classical signals can be transmitted
- If Alice and Bob have one half each of $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- It is possible for Alice to transmit an unknown state $|\psi\rangle = a|0\rangle + b|1\rangle$ to Bob, using only classical information



- Top two lines represent Alice's system, the last one Bob's
- 1: $|\psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}[a|0\rangle(|00\rangle + |11\rangle) + b|1\rangle(|00\rangle + |11\rangle)]$
- 2: $\frac{1}{\sqrt{2}}[a|0\rangle(|00\rangle + |11\rangle) + b|1\rangle(|10\rangle + |01\rangle)]$
- 3: $\frac{1}{2}[a(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + b(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)]$
- $=\frac{1}{2}[|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) + |10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle)]$
- Depending on Alice's measurement result, Bob applies gate.

Quantum teleportation II

- If Alice measures 00, Bob's system will be in state $|\psi\rangle$
- If she measures something else and tells him (=classical communication), Bob can "fix it" such that his state is equal to $|\psi\rangle$

Classical cryptography

- Alice wants to send a secret message to Bob ... both have exchanged an encryption key beforehand
- 0 1 0 0 1 1 0 0 1 0 0 0 message
- 1 1 0 1 0 1 1 1 0 1 0 0 encryption key
- 1 0 0 1 1 0 1 1 1 1 0 0 sum = encrypted message
- Message transmitted to Bob over public channel
- 1 0 0 1 1 0 1 1 1 1 0 0 encrypted message
- 1 1 0 1 0 1 1 1 0 1 0 0 encryption key
- 0 1 0 0 1 1 0 0 1 0 0 0 difference = message
- Provably secure if the key is as long as the message

Problem: key distribution

- If Eve (eavesdropper) gets hold of the key, she may listen to the encrypted message
- However, quantum mechanics can be used to create and distribute a key, giving no chance to Eve

BB84: protocol

- Alice sends a bit string to Bob.
- She randomly switches between orthogonal encodings: 0,1 $= |0\rangle, |1\rangle$ or 0,1 $= |-\rangle, |+\rangle$. (remember $|\pm\rangle \propto |0\rangle \pm |1\rangle$)
- Bob measures the qubits. He randomly switches between measuring in $|0\rangle, |1\rangle$ basis or in $|-\rangle, |+\rangle$ basis.
- After the whole string is transmitted, Alice and Bob compare their basis choice via a public channel. They keep only those bits where they used the **same basis.**
- From this string, they select a randomly chosen subset of bits and compare their values via a public channel. If all bits agree, they conclude that the channel was safe. The remaining bits can now be used as a key.

BB84: eavesdropping

- Why can they conclude the channel is save?
- An Eavesdropper (Eve) would have to measure the qubits on their way.
- As Eve does not know Alice's randomized basis choice, she has to guess. In $\frac{1}{2}$ of cases she will measure in the wrong basis. For example Alice sends $|0\rangle$, Eve measures $|\pm\rangle$.
- She sends the result $|\pm\rangle$ onwards to Bob. Now Bob, measuring in the correct basis, will get the wrong bit $|1\rangle$ with probability $\frac{1}{2}$.
- Therefore the presence of Eve unavoidably corrupts $\approx \frac{1}{4}$ of bits. Alice and Bob will notice!

Ekert 91 protocol

- Ekert91 protocol: The singlet state $|\psi_s\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ is distributed among Alice and Bob.
- Both make measurements on their half of the pair.
- Using the same basis, the results are random but perfectly anticorrelated
  $\Rightarrow$ generation of a key
- Using different bases, they can verify that the state was entangled. (Bell test) This would prove that Eve could not interfere.
- Alice and Bob randomize their bases to both generate a key and verify security.

Bell Test: check if a two-partite state is entangled

- Many versions of Bell tests exist
- Here: Clauser-Horne-Shimony-Holt (CHSH)
- Scenario: Alice and Bob perform independent measurements on a two-qubit state.
- These measurements are performed in bases A_1, A_2 for Alice, and B_1, B_2 for Bob
- Independent measurements would be possible if the two qubit state is factorizable
- All measurements can have possible outcomes $\{a_1, a_2, b_1, b_2\} \in \{+1, -1\}$
- For example, ± 1 could be encoded as $\{\uparrow, \downarrow\}$ electron spin, or $\{H, V\}$ photon polarization

Bell Test: CHSH inequality $\mathcal{C} \leq 2$

- Measuring spin along $\hat{z}$ (corresponds to $\hat{\sigma}_z$ gives us $\{+1, -1\}$)
- Measuring spin along $\hat{x}$ (corresponds to $\hat{\sigma}_x$ gives us $\{+1, -1\}$)
- Measuring spin along $\hat{y}$ (corresponds to $\hat{\sigma}_y$ gives us $\{+1, -1\}$)
- Try to maximize $\mathcal{C} \equiv a_1 b_1 + a_2 b_1 + a_1 b_2 - a_2 b_2$
- For any non-entangled state $|\mathcal{C}| \leq 2$ (CHSH inequality)
- But for Bell states $|\mathcal{C}| = 2\sqrt{2}$ is possible!

Bell Test: Use Bell state

- Consider Bell State: $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- Spin can be measured along a general direction θ, ϕ.
- Choosing $\phi = 0$ for simplicity we have
  $\hat{\sigma}_\theta = \sin(\theta)\hat{\sigma}_x + \cos(\theta)\hat{\sigma}_z$
- With this choice, all measurements are of the form $\hat{\sigma}_\alpha \otimes \hat{\sigma}_\beta$
- $$\begin{bmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{bmatrix} \otimes \begin{bmatrix} \cos(\beta) & \sin(\beta) \\ \sin(\beta) & -\cos(\beta) \end{bmatrix}$$

Bell Test: Violate $\mathcal{C} \leq 2$

- The measurement correlations are $\langle \beta_{00} | \hat{\sigma}_\alpha \otimes \hat{\sigma}_\beta | \beta_{00} \rangle = \cos(\alpha - \beta)$
- Therefore $|\langle \mathcal{C} \rangle| = |\cos(\alpha_1 - \beta_1) + \cos(\alpha_2 - \beta_1) + \cos(\alpha_1 - \beta_2) - \cos(\alpha_2 - \beta_2)|$
- With optimal choice of angles $\alpha_1 = 0$, $\alpha_2 = \frac{\pi}{2}$, $\beta_1 = \frac{\pi}{4}$, and $\beta_2 = -\frac{\pi}{4}$ we obtain $|\langle \mathcal{C} \rangle| = 2\sqrt{2}$ violates CHSH version of Bell inequality
- Violation of the inequality $|\langle \mathcal{C} \rangle| \leq 2$ demonstrates entanglement