Quantum computing and quantum communication

Rakesh P. Tiwari

rakesh.tiwari@unibas.ch

December 7, 2016

UNI
BASEL

What will we learn ?

- elements of quantum information
  - qubits
  - superposition and entanglement
  - 1- and 2-qubit gates
  - no-cloning theorem
  - Deutsch algorithm
- error correction, encryption, teleportation
- “hardware” for quantum computers

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

Big problem

- Unitary time evolution of a quantum computer has to be phase-coherent
- But a system of 100's or 1000's of qubits is coupled to its environment $\Rightarrow$ phase-breaking processes
- Way out: quantum error correction! (Shor)
- Introduce redundancy $\Rightarrow$ protection from phase-breaking errors.
- Operation of a quantum computer possible if $\frac{\tau_{switch}}{\tau_\phi} \leq 10^{-4}$
- τ_{switch}: time to do a 1-qubit operation
- τ_ϕ: phase-breaking time

Classical error correction I

- Bit flip is the most general classical single-bit error ($0 \leftrightarrow 1$)
- Probability of 1-bit error: p per unit time
- A bit is corrupted after $\mathcal{O}(1/p)$ steps
- To get around add redundancy by the following encoding: $0 \rightarrow 00$ and $1 \rightarrow 11$
- The strings 00 and 11, both have even parity
- If we detect an odd party string, an error has occurred
- How to correct ?

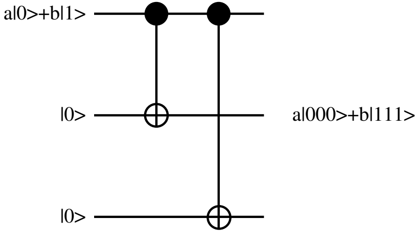
Classical error correction II

- Increase redundancy: $0 \rightarrow 000$ and $1 \rightarrow 111$
- 1-bit errors can be corrected by 'majority voting'
- What if two errors occur ? *error correction works incorrectly*
- What if three errors occur ? *error undetectable*
- Probability of single bit error is 3p with a redundancy of three
- probability of 2-bit and 3-bit error is $3p^2$ and p^3 respectively
- If $3p^2 + p^3 < p$ then error correction is worth doing, choose $p \ll 1$

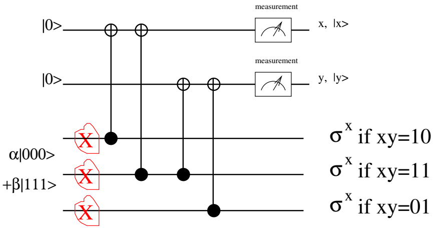
Quantum error correction I

- No cloning theorem $\rightarrow$ cannot increase redundancy
- Finding errors requires measurements destroying quantum information
- Surprisingly, we can still correct errors
- Consider bit flip error
- Corresponds to bit flip gate $\hat{\sigma}_x$
- Embed single qubit state in a state of three qubits, $\alpha|0\rangle + \beta|1\rangle$ is encoded as $|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$
- We have NOT copied $\alpha|0\rangle + \beta|1\rangle$, doesn't violate no cloning theorem

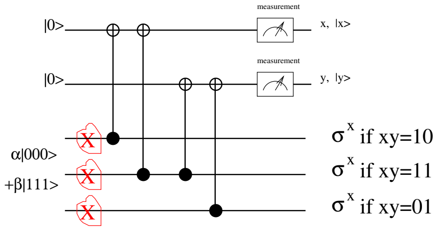
Quantum error correction II



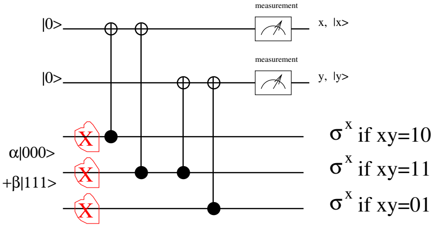
- Using CNOT: $\alpha|0\rangle + \beta|1\rangle \Rightarrow \alpha|000\rangle + \beta|111\rangle$
- Single bit-flip error can result in $\alpha|100\rangle + \beta|011\rangle$ or $\alpha|010\rangle + \beta|101\rangle$ or $\alpha|001\rangle + \beta|110\rangle$
- If we knew the parities of qubits 1 and 2, and qubits 2 and 3, we know which error (if any) has occurred
- How to correct ?



- Alice sends $\alpha|000\rangle + \beta|111\rangle$
- 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 $p(1-p)^2$
- Bob receives $\alpha|110\rangle + \beta|001\rangle$ with probability $p^2(1-p)$
- Bob receives $\alpha|101\rangle + \beta|010\rangle$ with probability $p^2(1-p)$
- Bob receives $\alpha|011\rangle + \beta|100\rangle$ with probability $p^2(1-p)$
- Bob receives $\alpha|111\rangle + \beta|000\rangle$ with probability p^3



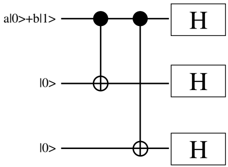
- After Bob's CNOTs
- Bob gets $(\alpha|000\rangle + \beta|111\rangle)|00\rangle$ with probability $(1-p)^3$
- Bob gets $(\alpha|100\rangle + \beta|011\rangle)|10\rangle$ with probability $p(1-p)^2$
- Bob gets $(\alpha|010\rangle + \beta|101\rangle)|11\rangle$ with probability $p(1-p)^2$
- Bob gets $(\alpha|001\rangle + \beta|110\rangle)|01\rangle$ 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



- Bob flips one of the qubits depending on the values of x and y
- $P_{fail} = 3p^2 - 2p^3 \sim \mathcal{O}(p^2)$: add last four
- If nothing is done, $P_{fail} \sim \mathcal{O}(p)$, single bit flip error
- With just three qubits, we reduced the error probability by a factor of $\frac{1}{3p} \sim 300$ for $p = 0.001$
- Suppression is more powerful with more qubits

Phase flip error

- Bit flip error is only one kind of possible error
- Phase flip error: $\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|0\rangle - \beta|1\rangle$
- No classical equivalent
- How to correct phase flip errors ?
- Turn phase flip channel into bit flip channel !
- $|+\rangle \equiv \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $|-\rangle \equiv \frac{|0\rangle-|1\rangle}{\sqrt{2}}$
- In this basis phase flip acts like bit flip
- In $|+\rangle$ and $|-\rangle$ basis the state is $\frac{1}{\sqrt{2}}\left[\begin{array}{c} \alpha+\beta \\ \alpha-\beta \end{array}\right]$



- $\alpha|0\rangle + \beta|1\rangle \Rightarrow \alpha|+++\rangle + \beta|---\rangle$
- Remaining procedure same as before
- Combination of the phase flip and the bit flip code can protect against arbitrary errors: Shor Code

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
- She can do it without Bob's knowledge of the interception of the message
- However, quantum mechanics can be used to distribute or create a key, giving no chance to Eve
- EPR protocol: Alice produces a number of 2-qubit states $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and sends one qubit of the pair to Bob
- Both make measurements on their half of the pair (in the same basis), and the results are random but identical on both sides $\Rightarrow$ generation of a key

Eavesdropping

- If Eve knew the basis she could also get the key
- If Eve secretly tries to read the key during transmission, she will change the qubit state
- Alice and Bob can check this by selecting a random subset of the pairs, and test if they violate Bell's inequality
- Eve cannot get any information from the qubits transmitted from Alice to Bob without disturbing their state
- This is the heart of quantum cryptography