

Quantum information and computing

Lecture 1

Jani-Petri Martikainen

`Jani-Petri.Martikainen@helsinki.fi`

`http://www.helsinki.fi/~jamartik`

Department of Physical Sciences

University of Helsinki

Lecturer

- Lecturer: Jani Martikainen
- Email: Jani-Petri.Martikainen@helsinki.fi
- Phone and office: 191 50677 office: C325
- Reception (preferably) Fri 12-13.

Course info

- Course web page:
<http://theory.physics.helsinki.fi/~quantumgas/>
- 3sw or 5sp
- Exercises (roughly) every second week and they give 1/3 of the grade.
- No special exercise session, I will go over the exercises during the lectures.
- Return the exercises before 17 : 15 on Monday before the lecture on Wednesday (leave the solutions to my mailbox in the 3rd floor...)
- Exam Tuesday 08.05.07 13-17 at D101

Suggested material (for example)...

- Book “Quantum computation and Quantum information”
- John Preskill lecture notes in the web
<http://www.theory.caltech.edu/7Epreskill/ph219/index.html#lecture>
- course lecture notes from the course homepage...most likely quite compressed
- web, look for reviews (xxx.lanl.gov)
- Some handwritten notes might appear in the lecture notes shelf on the 2nd floor..DIAGRAMS etc...

Contents of this course...continues

1. Introduction and overview
2. Essential quantum mechanics: states, postulates, measurement, qubits, density operators...
3. brief sketch of computer science
4. Quantum circuits
5. Quantum FFT and its applications
6. Quantum search

Contents of this course

1. Physical realization of a quantum computer
2. Quantum noise: how the noise changes things
3. Error correction: how to quantum compute in the real world
4. Entropy and information
5. Quantum information
6. Quantum cryptography: fool-proof secure communication

Some background

- One of the goals has been to develop tools which makes quantum mechanics more intuitive
- For example, can you use quantum mechanics to communicate faster than light? (You should not be able to do that!)
- Hinges on the question that is it possible to **clone** an unknown quantum state. If the answer is yes, then it would be possible to signal faster than light.
- No-cloning theorem...:BLACKBOARD

Some background

- 1970s: obtain a complete control over single quantum system.
- usually we have a huge number of atoms etc. in the system and we can only access few aspects of the underlying quantum mechanical nature.
- from 1970s onwards manipulating single quantum systems has become more and more feasible and commonplace...
- Perhaps there are surprises waiting for us in new regimes of nature?
- Technological progress: miniaturization starts to approach regime where quantum effects start to come into play...

Some background

- Perhaps we need a new paradigm for computing if we wish to see Moore's law obeyed in the coming decades. (Computing power doubles for constant cost roughly every two years)
- Computer science: If computing is done quantum mechanically, do we have to modify some concepts of computer science (are some set of problems hard for a classical computer and quantum computer?)
- Answer appears to be that some tasks can be done efficiently on a quantum computer, but only inefficiently on a classical computer.

Some background

- Information science: how do we define the concept of information in a quantum world?
- How much information can be carried over a (noisy) channel working according to the rules of quantum mechanics
- I.e. how to extend the classical Shannon's contributions to information science to take the possibilities of quantum mechanics into account?
- Cryptography: how to distribute secret keys in a fool proof way? (use quantum mechanics)
- How to break current cyptosystems (RSA)? (use a quantum computer)

Physics of information

- Information physical: encoded in the state of the physical system
- Computation is carried out by a physical device
- Engineering perspective: mastering the underlying physics is essential in developing state of the art computing hardware.
- Physics constraints: Obey the laws of physics, because they are the LAW!
- Landauer 1961: Erasure of information is necessarily dissipative (example)

Reversible computation?

- Reversible computation: is it possible?
- typically one uses irreversible logic gates such as NAND $((a, b) \rightarrow \neg(a \wedge b))$
- note: \wedge means AND and \neg means NOT or NEGATION
- NAND has two inputs and a single output, we cannot recover a unique input from a given output
- Since NAND erases information, it is dissipative and requires at least $W = k_B T \ln 2$ of energy for each operation.
- This fundamental limit might become important when the electronics shrinks further.

Reversible computation

- Bennett 1973: Reversible computation IS possible.
- use, for example, a reversible version of NAND.
- Toffoli gate: $(a, b, c) \rightarrow (a, b, c \oplus a \wedge b)$, where \oplus is a bitwise sum... $1 + 0 = 0 + 1 = 1$, but $1 + 1 = 0$
- i.e. flip the third bit if $a \wedge b = 1$ (that is if both are one)
- If $c = 1$ we have the normal NAND logic gate
- Creates extra junk: did you just postpone the energy cost?
- Answer: No, since you can compute to the end print out the result and then reverse your steps and return to the initial state.

Maxwell's demon

- Maxwell thought of a gas in a box, divided into two parts A and B by a partition
- Demon operates a shutter in the partition...allowing fast molecules to pass from A to B and slow ones from B to A
- A cools while B heats up, with a negligible expenditure of work... heat flows from cold to hot place and 2nd law of thermodynamics is violated!

Maxwell's demon

- However, Demon must collect and store information about the molecules. If he has a finite memory eventually the information must be erased...Pay the power bill for the cooling!
- These insights were anticipated by Leo Szilard in 1929 who associated the entropy $\Delta S = k \ln 2$ with the acquisition of one bit.
- He also invented the concept of a **bit** of information (not the name however)

Quantum information

- The universe is quantum mechanical: what changes?
- The very act of acquiring information disturbs the system
- True randomness in the measurement outcomes
- quantum information cannot be copied perfectly (copying normal “classical” information is very easy)
- Quantum information is typically encoded in **non-local** correlations
- Field started in 80’s and blossomed in the 90’s

What is the point of quantum computing?

- quantum computer is computer which computes according to the rules of quantum mechanics (quantum states, unitary time evolution, measurement...)
- Is it possible for the quantum computer to solve efficiently problems which cannot be solved efficiently with a classical computer?
- attack on the Church-Turing thesis: any algorithmic process can be efficiently simulated using a Turing machine.
- Answer: (Probably) Yes, since in 1994 Shor showed that finding prime factors of some number can be efficiently solved on a quantum computer, but it is believed that no such feat is possible with a classical computer

Complexity and efficient computation

- Classical complexity theory is a study of which problems are hard and which ones are easy.
- Usually which is “hard” and “easy” are defined in terms of how much time and/or memory are needed.
- Shouldn't we specify the hardware? Something might be hard for a PC, but easy for some other type of computer.
- Meaningful distinction between “hard” and “easy” should be universal and should not depend on which machine we are using
- Often focus on whether the algorithm is “polynomial time” (easy) or “exponential time ” (hard) (...exponential could also mean just super-polynomial)

Complexity and efficient computation

- One universal classical computer can simulate another with at worst “polynomial overhead”
- i.e. if something is hard/easy on one universal classical computer it will be so in all the others as well.
- If you can simulate a quantum computer with a classical one and have just polynomial overhead, quantum computer would not be of great interest to the complexity theory
- However, Shor’s result suggest that no polynomial time simulation of a quantum computer is possible! **Some things which are hard for a classical computer might not be hard for a quantum computer.**

Factoring

- The difficulty of factoring is the key to the security of the widely used public key cryptography (RSA)
- The best classical algorithm for factoring, the number field sieve takes the time ($c \approx 1.9$)

$$\tau \sim \exp[c(\ln n)^{1/3}(\ln \ln n)^{2/3}], \quad (1)$$

- With a quantum computer $\tau \sim (\ln n)^3$
- Assume that a 65 digit factors of a 130 digit number can be found in a month....factoring a 400 digit number takes 10^{10} years
- If we have quantum computer which factors 130 digit number in one month... factoring a 400 digit number takes 3 years

Bit and Qubit...

- The indivisible unit of classical information is the bit: an object which is either 0 or 1
- The corresponding unit of quantum information is the qubit
- Qubit is a vector in a two-dimensional complex vector space with inner product.
- We call the elements of an orthonormal basis in this space $|0\rangle$ and $|1\rangle$. Then the normalized vector can be represented as

$$|\psi\rangle = a|0\rangle + b|1\rangle, \quad (2)$$

where $|a|^2 + |b|^2 = 1$ and $a, b \in \mathcal{C}$

Simulating quantum systems

- Feynman 1982: Simulating a quantum system on a classical computer is hard...use quantum mechanics to build a computer to simulate quantum mechanics.
- Classical simulation is hard since for a N -qubit (qubit is a single two level quantum system) system the quantum state lives in 2^N dimensional Hilbert space. So you need 2^N complex numbers to store the quantum state on a computer
- $N = 50 \rightarrow 10^{15}$ complex numbers. Store the numbers to 128 bit precision... 32 bytes for each amplitude... 32000 Tbytes!
- 90 qubits at the same level requires 32×10^{27} bytes...implement on a single atom level...kilograms of matter.

Simulating quantum systems

- Unitary evolution amounts to a rotation of the state vector in the Hilbert space. This is even less feasible than storing the general N -qubit state.
- Quantum computer could just work with N -qubits directly.
- However, could we design a probabilistic classical computer, in which the various outcomes arise with the probability distribution which coincides with that generated by a quantum computation?
- Bell: There is no local probabilistic algorithm which reproduces the conclusions of quantum mechanics.
- Therefore, it seems very likely that simulating a quantum system (or emulating a quantum computer) is a very hard problem for any classical computer.

Other curious things...

- Distributed quantum computers: Distribute computing resources to different places. How much communication is required between the computers to complete the computation?
- It has been shown that quantum computers can require exponentially less communication than classical computers.
- Again, the key is that quantum information is typically encoded non-locally.

Other curious things...

- Take a system of $3N$ -cubits and split it in three part, one part in Helsinki, one in Stockholm, and one in Berlin
- entropy in each subsystem $S \simeq N - 2^{-(N+1)}$
- If entropy is N there is no accessible information... so each subsystem has only exponentially small amount of accessible information.
- To find the information you must see how the measurement outcomes in Helsinki, Stockholm and Berlin are correlated! **Perform a collective measurement**

Other curious things...

- Private key cryptography: Use the key to decrypt the message. How to distribute the keys securely?
- Use quantum key distribution! It is based on the fact that possible eavesdropper will disturb the quantum state and then her presence can be observed from comparing the measurement outcomes at each end of the quantum channel.
- Public key cryptography: Alice uses Bobs public key to encode her message to Bob.
- To decrypt easily one needs Bobs private key as well, but Bob has it!
- Hard for anyone else because finding prime factors of large numbers is hard...Use quantum computer to eavesdrop!

Quantum parallelism

- Following Deutch, imagine a black box which computes a single bit function $f(x)$ from the single bit input x . Each computation takes 24 hours.
- We want to know if $f(x)$ is constant $f(1) = f(0)$...need two evaluations and 48 hours.
- But suppose we have a quantum computer...quantum computer is invertible so we need to take two qubits to two

$$U_f : |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle \quad (3)$$

- Because we have a quantum computer, we can choose a superposition input state for the second qubit
 $1/\sqrt{2}(|0\rangle - |1\rangle)$

Quantum parallelism

$$\begin{aligned} U_f : |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) &\rightarrow |x\rangle \frac{1}{\sqrt{2}}(|f(x)\rangle - |1 \oplus f(x)\rangle) \\ &= |x\rangle (-1)^{f(x)} / \sqrt{2} (|0\rangle - |1\rangle) \end{aligned} \quad (4)$$

- Now suppose that we prepare the first qubit as $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$$\begin{aligned} U_f : \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) &\rightarrow \\ \frac{1}{\sqrt{2}} \left[(-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle \right] \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) & \end{aligned}$$

Quantum parallelism

- finally perform a measurement that projects the first qubit onto the basis

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle) \quad (5)$$

- If the function is constant, we will always obtain $|+\rangle$ for the first qubit.
- Suppose we are interested in the global properties of a function which acts on N bits with 2^N possible arguments...hard for a classical computer since the number of evaluations is so high
- But with quantum computer that acts according to

$$U_f : |x\rangle|0\rangle \rightarrow |x\rangle|f(x)\rangle \quad (6)$$

Quantum parallelism

- we can choose the input register to be

$$\left[\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right]^N = \frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} |x\rangle \quad (7)$$

- Single computation creates a state

$$\frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} |x\rangle |f(x)\rangle \quad (8)$$

- we can extract global properties of $f(x)$ if we can only think of an efficient way to do this...**massive quantum parallelism**

Quantum parallelism

- The information is now in the correlations between the input and the output. This nonlocal information is not easy to decipher
- If I measure $|x\rangle$, I would obtain a result $|x_0\rangle$ where x_0 is chosen at random among 2^N alternatives. The state would be projected into $|x_0\rangle|f(x_0)\rangle$
- Now we just have access to a single function evaluation.
- You have to be more clever in exploiting the correlations
In Eq. (8) if quantum computer is to be useful.

Quantum search

- Quantum search algorithms: basic ideas due to Grover
- Given a search space of size N and no prior knowledge about the structure of the information, we want to find an element of the search space which satisfies some given property.
- Classically we need about N operations to solve this.
- Quantum search algorithm allows it to be solved using only \sqrt{N} operations. (only quadratic speed up)

Few words about hardware

1. Storage: need to store qubits for a long time..enough to complete the computation
2. Isolation: The qubits must be well isolated from the environment, to minimize decoherence errors
3. Readout: We'll need to measure the qubits efficiently and reliably
4. Gates: Need to manipulate the quantum states of individual qubits, so that we can perform quantum gates...two qubits should also be able to interact.
5. Precision: Need high precision in implementation for reliability

Candidate systems: Ion traps

- Ion traps: use a linear Paul trap. Quantum state of each ion is a linear combination of the ground state $|g\rangle$ and a long-lived metastable excited state $|e\rangle$.
- Coulomb repulsion keeps ions apart so each ion can be addressed individually with a laser.
- Hardest thing is to make two qubits interact with each other. In an ion trap interactions arise because mutual Coulomb repulsion implies a spectrum of coupled normal modes of vibration for the trapped ions.
- When ion absorbs a photon, the center of mass of the ion recoils. But if the laser is properly tuned, then when a single ion absorbs or emits, a normal mode involving many ions will recoil coherently (Mössbauer effect)

Candidate systems: Ion traps

- The lowest vibrational mode is the center of mass (cm) mode, in which ions oscillate in-phase in the harmonic well of the trap
- A laser pulse of appropriate frequency and time will rotate the state $|e\rangle_n$ state of the n :th ion into $|g\rangle_n$ while the cm oscillator makes a transition from $|0\rangle_{cm}$ to $|1\rangle_{cm}$ (a single phonon). However, the state $|g\rangle_n|0\rangle_{cm}$ is off-resonance and is not influenced...so we have

$$|g\rangle_n|0\rangle_{cm} \rightarrow |g\rangle_n|0\rangle_{cm} \quad (9)$$

$$|e\rangle_n|0\rangle_{cm} \rightarrow -i|g\rangle_n|1\rangle_{cm} \quad (10)$$

Candidate systems: Ion traps

- The bit originally stored in the internal state of the n :th atom is now stored in the collective state of motion of all ions.
- The state of motion of m :th ion has been influenced by the internal state of the n th ion... induced an interaction between ions.
- We should still transfer the quantum information from the cm phonon back to the internal state of one of the ions. Also, cm mode should return back to its ground state $|0\rangle_{cm}$
- quantum XOR (controlled not gate): $|x, y\rangle \rightarrow |x, y \oplus x\rangle$ can be implemented with 5 laser pulses.
- Problem: vibrational state splitting is small, so you need long laser pulses... intrinsically slow

Candidate systems: cavity QED

- Trap neutral atoms in a high finesse optical cavity.
- Store information in the internal state of the atoms
- Atoms interact because they are coupled to the normal modes of the electromagnetic field inside the cavity.
- Laser pulses...transition in one atom conditioned on the internal state of another atom

Candidate systems: cavity QED

- Or, store the qubit in the polarization of the photon.
- Trapped atom can then be used as the intermediary that causes one photon to interact with another.

Candidate systems: NMR

- Nuclear magnetic resonance: qubits are carried by certain nuclear spins in a particular molecule.
- Each spin is either aligned $|0\rangle$ or anti-aligned $|1\rangle$ with the applied magnetic field
- spins take a long time to relax or decohere (good thing)
- Pulsed rotating magnetic field can induce Rabi oscillations of the spin...single qubit operations can be done
- Dipole-dipole coupling between spins can be used to perform a gate

Candidate systems: NMR

- The splitting between $|0\rangle$ and $|1\rangle$ for one spin depends on the state of the neighboring spins. So whether or not the magnetic field is on-resonance to tip the spin is conditioned on another spin.
- Not obvious that NMR systems should work: they are HOT, typically room temperature is million times larger than the splitting between $|0\rangle$ and $|1\rangle$
- Quantum state is very noisy due to the thermal fluctuations.

Candidate systems: NMR

- We do not actually perform our processing on a single molecule, but on a macroscopic sample containing $\sim 10^{23}$ “computers”...signal is the average over these
- Average over the ensemble is not equivalent to running the computation on a single device; averaging may obscure the results.
- Can overcome these difficulties: arrange things so that fluctuating properties average out when the signal is detected.
- Also, in some quantum algorithms averaging over many computations will not spoil the result, since large fraction of the computers give the same answer