CS290A, Spring 2005:

Quantum Information & Quantum Computation

Wim van Dam

Engineering 1, Room 5109
vandam@cs

http://www.cs.ucsb.edu/~vandam/teaching/CS290/

Administrivia

- Final exam will be *open* book.

- Material will be everything discussed in class (slides, Handouts, Exercises).
- References to specific sections in Nielsen and Chuang’s “Quantum Computation and Quantum Information” will be posted on the web site.

This Week

- Bell’s proof of the nonlocality of quantum physics
- Quantum Communication Complexity

- **The future and feasibility of quantum computing:**

- Quantum Error Correcting Codes
- Future quantum algorithms
- Experimental implementations

Hidden Variables

In a hidden variable theory, the particles have determined beforehand what the measurement outcomes will be.

Several kinds of measurements are possible so each particle has a list of answers that obeys the quantum predictions.

Hence for EPR pair $(|00\rangle+|11\rangle)/\sqrt{2}$:
If we measure A and B in the basis 0/1 then both answers have to be the same.
Idem for +/– basis. For example:
A=[$M_{0/1}$=“0”, $M_{+/–}$=“–”] and
B=[$M_{0/1}$=“0”, $M_{+/–}$=“–”] gives the table

A^B	0	1	+	–
0	Y			Y
1				
+				
–	Y			Y

Hidden Variable Theory

We can completely “explain” the statistics of an EPR pair and measurements in the 0/1 or +/– basis by assuming that the particles implement the one of the following four tables at random (Prob. ¼ each).

A^B	0	1	+	−
0	Y			Y
1				
+				
−	Y			Y

A^B	0	1	+	−
0	Y		Y	
1				
+	Y		Y	
−				

A^B	0	1	+	−
0				
1		Y		Y
+				
−		Y		Y

A^B	0	1	+	−
0				
1		Y	Y	
+		Y	Y	
−				

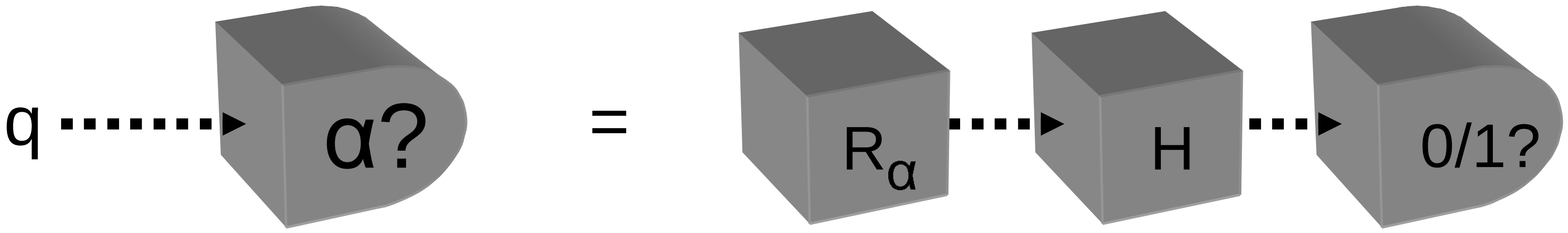
Note: The particles are allowed to coordinate their answers, but they have to do that before the measurements are performed (when the particles are far away).

Bell’s Theorem

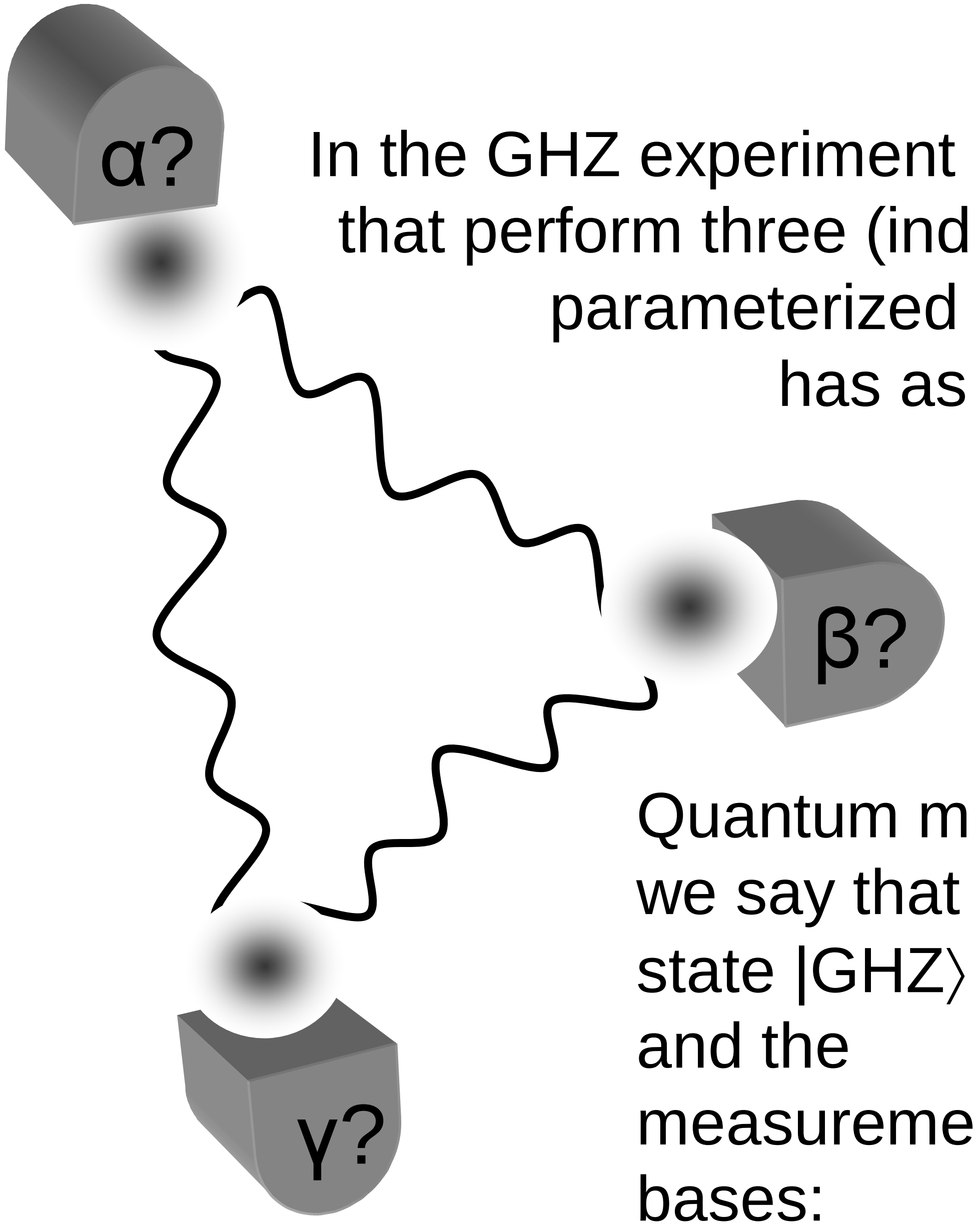
Although there is a ‘classical theory’ for EPR qubits and measurements in the 0/1 or +/– basis, this does not hold in general.

Bell’s Theorem: There are settings with separated entangled qubits and measurements where it is not possible to explain the statistics of quantum physics in a classical way.

Here we will discuss a 3 qubit proof for the state $|\mathrm{GHZ}\rangle = (|000\rangle+|111\rangle)/\sqrt{2}$ and simple measurements:



GHZ Experiment



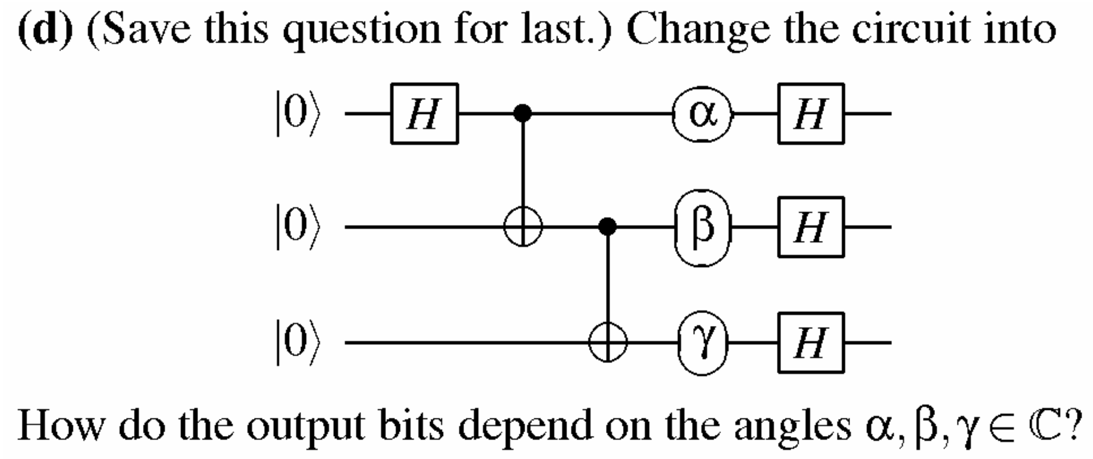
In the GHZ experiment we have 3 parties (A,B,C) that perform three (independent) measurements parameterized by angles (α,β,γ) and that has as outcome three bits $\{0,1\}^3$.

Quantum mechanically speaking we say that we have the 3-qubit state $|\mathrm{GHZ}\rangle = (|000\rangle+|111\rangle)/\sqrt{2}$ and the measurement bases:

$$\left|\text{"}0_\alpha\text{"}\right\rangle = \tfrac{1}{\sqrt{2}}\left(\left|0\right\rangle + e^{-i\alpha}\left|1\right\rangle\right)$$

$$\left|\text{"}1_\alpha\text{"}\right\rangle = \tfrac{1}{\sqrt{2}}\left(\left|0\right\rangle - e^{-i\alpha}\left|1\right\rangle\right)$$

Midterm Flashback



(d) (Save this question for last.) Change the circuit into

$|0\rangle$
$|0\rangle$
$|0\rangle$
H
α
β
γ
H
H
H

How do the output bits depend on the angles $\alpha, \beta, \gamma \in \mathbb{C}$?

How the outcomes are determined by the angles α,β,γ was the last question on the Midterm.

- The three rotations have the global effect

$$|\mathrm{GHZ}\rangle \mapsto \tfrac{1}{\sqrt{2}}(|000\rangle + e^{i(\alpha+\beta+\gamma)}|111\rangle)$$

- After the three Hadamard gates this become

$$\mapsto \quad \tfrac{1}{4}(1+e^{i(\alpha+\beta+\gamma)})(|000\rangle+|011\rangle+|101\rangle+|110\rangle)$$
$$+\tfrac{1}{4}(1-e^{i(\alpha+\beta+\gamma)})(|001\rangle+|010\rangle+|100\rangle+|111\rangle)$$

- If the sum α+β+γ = 0 mod 2π then the parity of the outcome bits will be even. If α+β+γ = π mod 2π, then the parity of the three bits will be odd.

Hidden Variables?

GHZ focuses on the cases where $\alpha,\beta,\gamma\in\{0,\frac{1}{2}\pi\}$.
If we want to explain this with a local, hidden variable theory, then each particle must have a predetermined outcome for the 2 measurements.
Denote these values: $M_0^A, M_{\frac{1}{2}\pi}^A, M_0^B, M_{\frac{1}{2}\pi}^B, M_0^C, M_{\frac{1}{2}\pi}^C$
Such that for example $M_{\frac{1}{2}\pi}^B = 1$ means that if B's particle gets measured at the ½π angle, then the outcome is "1".

All M have bit values $\in\{0,1\}$. GHZ's version of Bell's theorem shows that it is impossible to have M values that are in accordance with the prediction of quantum mechanics that says: $M^A \oplus M^B \oplus M^C = (\alpha+\beta+\gamma \bmod 2\pi)/\pi$.

How?…

No Hidden Variables

Take 3 cases where α+β+γ = π such that $M^A \oplus M^B \oplus M^C = 1$.

$$M_0^A \oplus M_{\frac{1}{2}\pi}^B \oplus M_{\frac{1}{2}\pi}^C = 1$$

$$M_{\frac{1}{2}\pi}^A \oplus M_0^B \oplus M_{\frac{1}{2}\pi}^C = 1$$

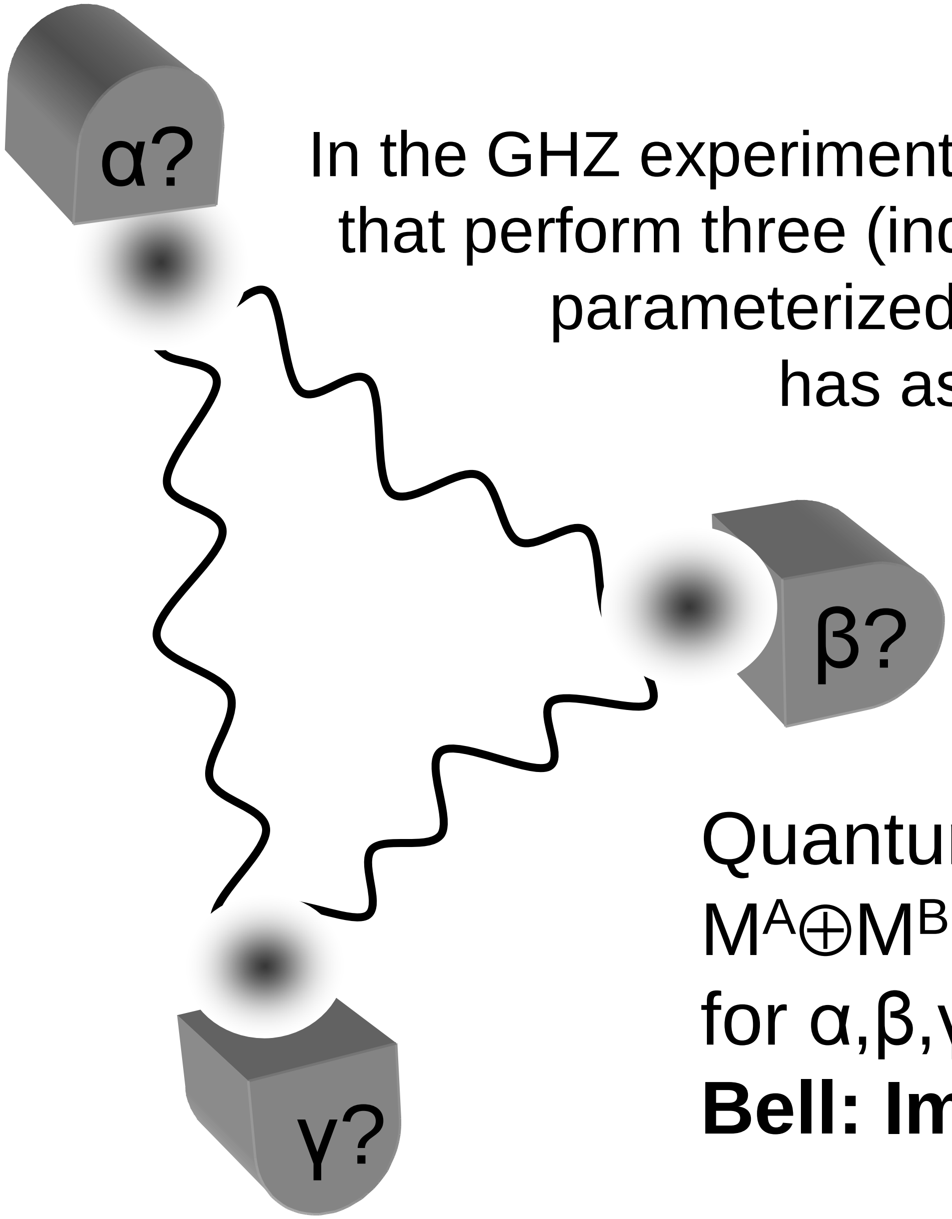
$$M_{\frac{1}{2}\pi}^A \oplus M_{\frac{1}{2}\pi}^B \oplus M_0^C = 1$$

Adding these three equations (modulo 2) gives:

$$M_0^A \oplus M_0^B \oplus M_0^C = 1$$

But this contradicts the requirement for α+β+γ = 0 such that the 3 output bits must have even parity: $M_0^A \oplus M_0^B \oplus M_0^C = 0$

GHZ Experiment



In the GHZ experiment we have 3 parties (A,B,C) that perform three (independent) measurements parameterized by angles (α,β,γ) and that has as outcome three bits $\{0,1\}^3$.

Quantum mechanics says:
$M^A \oplus M^B \oplus M^C = (\alpha+\beta+\gamma \bmod 2\pi)/\pi$
for $\alpha,\beta,\gamma \in \{0,\tfrac{1}{2}\pi\}$.
Bell: Impossible Classically.

Local Realism

The assumptions of a hidden variable theory for GHZ that led to the contradiction are those of **local realism.**

Locality: The assumption that the actions of remote parties does not effect the outcome of local experiments. For example: A’s outcome does not depend on the measurement settings of B and C, and so on.

Realism: The assumption that the outcomes are somehow predetermined for all experiments. Example: We listed the measurement outcomes M_0 and $M_{\pi/2}$ for particle on A’s side, and so on.

GHZ Continued

For angles $\alpha,\beta,\gamma \in \{0,½\pi,\pi,1½\pi\}$, we want to create remote bits M such that $M_A \oplus M_B \oplus M_C = \alpha+\beta+\gamma \bmod 2\pi$ under the promise that $\alpha+\beta+\gamma = 0 \bmod \pi$.

Quantum mechanically we can do this with 100% success. Classically, the maximum success rate is 75%.

Experimentally, these better-than-classical bounds have been broken: “nonlocality experiments”.

Besides proving profound facts about Nature, quantum nonlocality can also be use for distributed computing tasks if we want to minimize (classical) communication.

Communication Complexity

Take parties A and B, each with input x and y (of length n bits). They want to calculate a distributed function $F:\{0,1\}^n \times \{0,1\}^n \rightarrow S$, with a minimum of communication.

Quantum communication complexity looks at how much communication is required if we are allowed to use prior entanglement.

Just as with quantum algorithms, it turns out that for specific situations, entanglement can save communication: $QCC(F) < CC(F) \leq n$.

Some Examples

- Equality function: f(x,y) = EQ(x,y) = “x=y”?
  deterministic complexity is maximum: CC(EQ)=n

- “x+y even or odd?” has one bit complexity for integer x,y.

- If you allow a small error ε, things can change:
  $CC_{\varepsilon}(EQ) = O(\log n)$

Communication Complexity is studied for to understand better the efficiency of distributed computation

Example: Three Party Even/Odd Problem

- Consider three parties A, B and C, which have three real numbers x, y and z
  - Promise: x+y+z is a natural number
  - Question: is x+y+z even or odd?

- Using entanglement, this can be solved with only two qubits of communication using the GHZ trick.

General CC of Even/Odd

- In general for k parties: QCC(E/O) = k–1,

- Classical, deterministic three party complexity is 4 bits and for k parties CC(E/O) = Θ(k log k)

Entanglement saves us a factor of log k bits.

Admittedly, this problem does not seem all that relevant…

Appointment Problem

- Two diaries with n days: $x_1 \ldots x_n$ and $y_1 \ldots y_n$
- Is there a day j such that $x_j = y_j =$ “free”?
- Using Grover’s search algorithm one can show that

$$QCC_{\varepsilon}(APP_n) = O(\log n \cdot \sqrt{n})$$

- While classically:

$$CC_{\varepsilon}(APP_n) = \Theta(n)$$

Other Results

- Certain functions do not allow a quantum reduction in communication complexity
  Example: $IP(x,y) = x_1y_1\oplus\ldots\oplus x_ny_n$ has complexity $\Theta(n)$.

- There exist distributed tasks with an exponential gap between classical and quantum complexity.

- The theory of quantum communication complexity is "applied philosophy": What started as a theoretical debate on the locality of Nature, evolved into a set of algorithms that saves communication.

CS290A, Spring 2005:

Quantum Information & Quantum Computation

Wim van Dam

Engineering 1, Room 5109
vandam@cs

http://www.cs.ucsb.edu/~vandam/teaching/CS290/

Q&A

The emphasis of the final examination will be on quantum algorithms (Week 1–7).

“Mathematics of Quantum Computation IV” (on the quantum Fourier transform) will be updated.

Don’t forget to return the course evaluation.

Current (Theoretical) Work

What do people work on in theoretical quantum computation/information theory?

- Developing new quantum algorithms that are exponentially faster than classical ones.
- Finding new applications for small quantum devices.
- Designing quantum error correcting codes.

Quantum Algorithms

- Polynomial speedup: Parity, Searching

- Exponential speedup: Factoring, Discrete Logarithms

What more can we do more efficiently?

Polynomial speedup for other general black-box functions: Determining F, Collision problem, Counting, et cetera.

Exponential speedups?...

More Quantum Algorithms

- Pell’s equation: “What are the integer solutions (x,y) to the equation: $x^2–dy^2=1$, with $d>0$ a non-square?” (also “Principal Ideal Problem” in Number theory).
  This breaks the Buchmann-Williams crypto system.

- Simulating quantum mechanical systems.
  Could be relevant for calculations in Biochemistry.

- Several other problems in number theory:
  - Counting solution $F(x,y)=0$ over finite fields $x,y \in \mathbb{F}_q$.
  - Estimating Gauß sums.

Adiabatic Computation

- Adiabatic quantum computation is a heuristic quantum approach to combinatorial optimizations problems.
- Just like the classical simulated annealing approach, it tries to find an optimum by ‘quantum walking’ through the large space of possible answers in a smart way.
- The problem of getting stuck in a local minimum occurs also for adiabatic algorithms, but the quantum algorithm is (sometimes) better at getting out of it.
- Ultimate complexity is unknown and hard to determine.

Where to Look for New Problems?

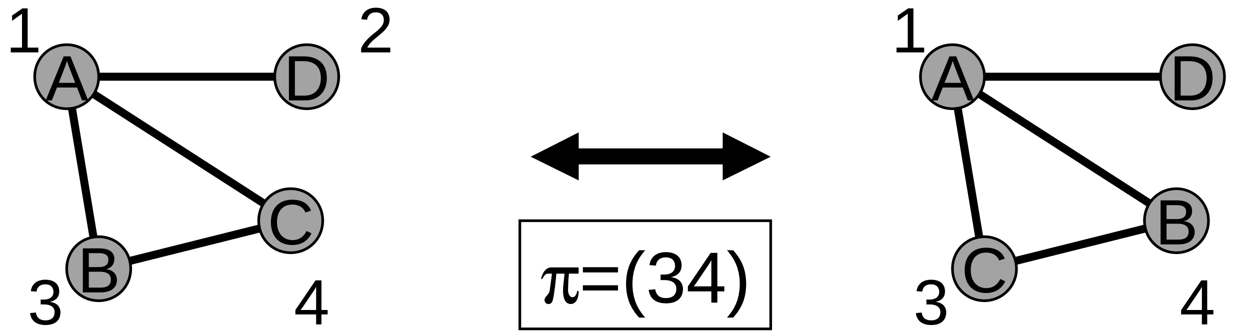
- The consensus is that we have to look for problems that are not in **P**, but that are not **NP**-complete either. (A somewhat forgotten category.)

- Two very interesting candidates:
  - Graph automorphism/automorphism problem
  - Shortest vector problem

- Both have not been solved yet.

Graph Automorphism

- Graph G, is its automorphism group trivial?
- <u>Example</u>:



π=(34)

- <u>Mathematically</u>: “$\pi \in S_n$, $\pi(G)=G$ if and only if $\pi=()$”?

Not known to be in **NP-complete** or in **P**

Shortest Vector

Consider a d-dimensional basis $B=[B_1,\ldots,B_d]$, with $B_j \in \mathbb{Z}^d$ for all $1 \leq j \leq d$. The *lattice* of B is defined by $L(D) = \{ \beta_1 B_1 + \ldots + \beta_d B_d : \beta_j \in \mathbb{Z} \}$ (this is not a vector space).

The shortest/closest vector problem asks for a vector $W \in \mathbb{Z}^d$ if there is a point in L(D) that is ‘close’ to W.

Variants of this problem are between **P** and **NP-complete** and are used in cryptographic protocols.

Experimental Work

- Implementations of quantum communication protocols using photon polarization.
- Implementations of small quantum algorithms (“proof of principle”) using NMR, trapped ions,…
- Towards a scalable quantum computer using ion traps, solid state NMR, superconducting qubits,…
- Will it work for imperfect devices?

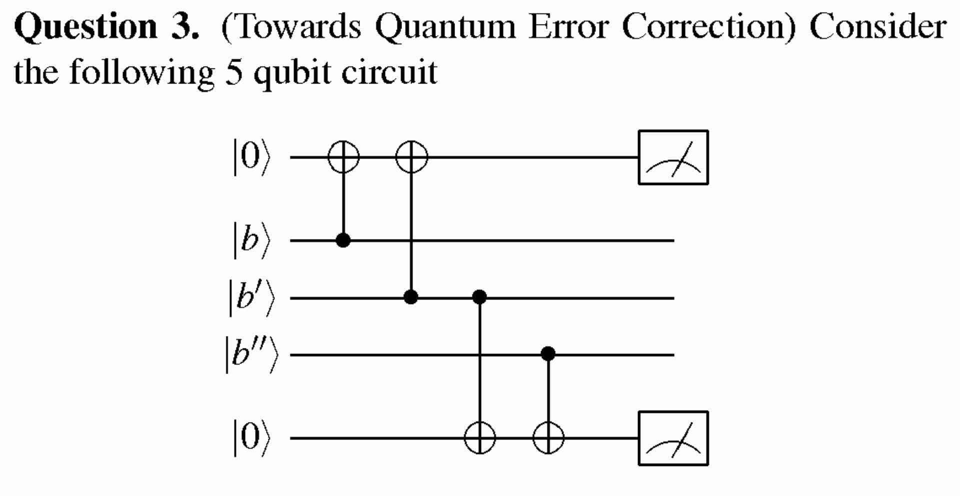
Problems with Quantum Error Correcting Codes

- We cannot copy a state to protect against errors.
- We cannot just measure the state to inspect the error that might have occurred.
- Many ways one can disturb one qubit $\alpha|0\rangle+\beta|1\rangle$.
- What error model do we assume?
- How to use the encoded states in a computation?

Quantum Error Correction

- Consider quantum bit wires that sometimes flip bits. This changes qubit values: $\alpha|0\rangle+\beta|1\rangle \mapsto \beta|0\rangle+\alpha|1\rangle$.
- How to protect oneself against this?

- Exercises 6, Question 3:
- If we use the encoding $\alpha|0_L\rangle+\beta|1_L\rangle = \alpha|000\rangle+\beta|111\rangle$ then we are protected against single bit flips.

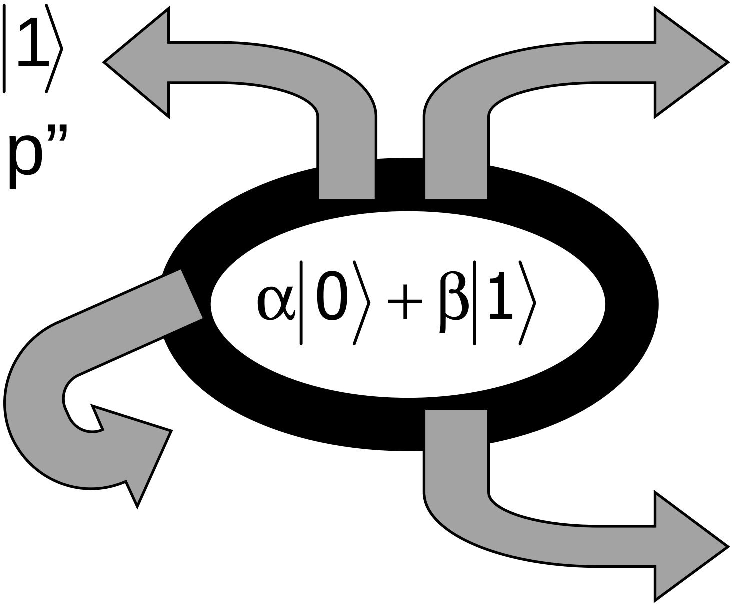


Question 3. (Towards Quantum Error Correction) Consider the following 5 qubit circuit

$|0\rangle$
$|b\rangle$
$|b'\rangle$
$|b''\rangle$
$|0\rangle$

- What about general qubit errors?

The 4 Qubit Errors:



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

“Bit flip”

$\alpha|0\rangle - \beta|1\rangle$

“Phase flip”

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

“Identity”

$\beta|0\rangle - \alpha|1\rangle$

“Bit & Phase flip”

<u>Happy Fact:</u>
If we can correct for these 4 errors,
then we can correct any qubit error.

(Classical error correction deals with bit-flips only.)

A [9,1] Quantum Error Code

Logical qubit: $\boxed{\alpha|0_L\rangle+\beta|1_L\rangle}$

Bit-flip code:

$$\alpha|000\rangle+\beta|111\rangle$$

Phase-flip code:

Combined, this gives
the 9 qubit ‘Shor code’:

$$\boxed{\begin{array}{l}\alpha\cdot\frac{1}{\sqrt{8}}\left(|000\rangle+|111\rangle\right)\otimes\left(|000\rangle+|111\rangle\right)\otimes\left(|000\rangle+|111\rangle\right)\\+\\\beta\cdot\frac{1}{\sqrt{8}}\left(|000\rangle-|111\rangle\right)\otimes\left(|000\rangle-|111\rangle\right)\otimes\left(|000\rangle-|111\rangle\right)\end{array}}$$

This code protects against an arbitrary bit error.

Quantum Error Correction

- Using the results of classical error correction, many quantum codes can be devised.
- Fault-tolerant *computation* is also possible.
- Combined, they give rise to several “thresholds for reliable quantum computation” results.

An error rate of ~0.0001 is sufficient to have a working quantum computer.

Will It Work?

- Nobody knows for sure.
- Regardless, quantum computing forces us to rethink our assumptions about computation and information.
- For physicists it has come as a big surprise that quantum mechanics can be so useful, and that you can think about q.m. in a CS kind-of-way.
- “The border between classical and quantum phenomena is just a question of money”, [A–Z]

One Last Issue

- If we believe that the whole world is quantum mechanical, what does it mean to measure?

- One can argue that if one observes a qubit, what happens is unitary as well:

$$\boxed{\begin{aligned}(\alpha|0\rangle+\beta|1\rangle)\otimes|\text{You}\rangle \mapsto\ & \alpha|0\rangle\otimes|\text{You saw a "zero"}\rangle \\ & +\beta|1\rangle\otimes|\text{You saw a "one"}\rangle\end{aligned}}$$

Many-Worlds Interpretation of QM.

Relevant Sections in QC&QI

These are the relevant sections for the final of Nielsen and Chuang’s “Quantum Computation and Quantum Information”. (This is a significant overestimation.)

- Sections 1–1.4.5
- Sections 2–2.1.4, 2.1.6–2.1.7, 2.2–2.2.5, 2.2.7–2.3, 2.6
- Sections 3–3.3
- Sections 4–4.5, 4.5.5–4.6
- Sections 5–5.1, 5.3–5.4.2
- Sections 6–6.1.4, 6.4–6.5
- Sections 12.6–12.6.1, 12.6.3
- Appendix 4–4.3