# 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

- Do the exercises.
- Answers will be posted at the end of the week.
- Midterm examination will be Thursday, April 28
  Open book, open everything.
- Bookstore will start returning books on April 25.
- Other questions?

# Things that have come up

- Know how to take tensor products of vectors.
- Mind the ordering of qubits for quantum gates:
  Example: CNOT between two bits
- In both cases: mind the ordering of the dimensions in the vector/matrix notation.

# This Week

Wrap-up of the quantum circuit model of efficient quantum computation.

Effect of partial measurements on superpositions.

Small quantum algorithms.

# Clean Reversible Computation

- With CCNot gates, we can implement NOT and AND.
- If we keep old memory around, any classical circuit function F can be implemented efficiently as $U_F$:$|x,0,0\rangle \mapsto |x,g_x,F(x)\rangle$ (which is a classical transform).

- By copying the output F(x) and running the circuit $U_F$ in reverse, we can erase the garbage bits $g_x$: $|x,g_x,F(x),0\rangle \mapsto |x,g_x,F(x),F(x)\rangle \mapsto |x,0,0,F(x)\rangle$.
- In sum: $|x,0,0\rangle \mapsto |x,F(x),0\rangle$ can be implemented efficiently as long as we have clean 0-qubits around.

- Also in superposition: $\Sigma_x|x,0,0\rangle \mapsto \Sigma_x|x,F(x),0\rangle$.

# Last Week's Question

- Why can we copy the F(x) bit and run the circuit $U_F$ in reverse to clean up the work space?

- Reason: $U_F$:$|x,0,0\rangle \mapsto |x,g_x,F(x)\rangle$ implements a classical transformation that does not create superpositions.

- If we have $U_F$ as a circuit, we can also apply it to a superposition of states. General clean computation:

$$\boxed{\sum_{x\in\{0,1\}^n} \alpha_x |x,0\rangle \mapsto \sum_{x\in\{0,1\}^n} \alpha_x |x,F(x)\rangle}$$

# Power of Reversible Computation

- We showed that the requirement of reversibility does not change (significantly) the efficiency of our computations: **Reversible Computation = General Computation.**

- But what about the efficiency of implementing general quantum transformations?

- We have to look at what it means to efficiently implement a computation that uses quantum superpositions.

# Closeness of States

- We know that unitary transformations are inner product preserving. Hence the angle between two states |ψ〉 and |ψ’〉 is the same as the angle between C|ψ〉 and C|ψ’〉 after we applied the circuit C to them.
- “If states are close, they remain close.”
- Measure of closeness: **Fidelity** $\boxed{\mathrm{F}(|\psi\rangle,|\varphi\rangle) = |\langle\psi|\varphi\rangle|}$
- If F(|ψ〉,|ψ’〉) ≈ 1, then the states are close.
- If F(|ψ〉,|ψ’〉) ≈ 0, then the states are ‘far away’.

- Close states lead to near identical probability distributions when measured.

# How Close?

Take two states $|\psi\rangle$ and $|\varphi\rangle$ with fidelity F.
Measuring the states in the computation basis $\{0,1\}^n$ gives two probability distributions p and q respectively.

If the states are close (F≈1), then p and q have to be close as well. How close?

$$\boxed{1-F \le \tfrac{1}{2} \sum_{s\in\{0,1\}^n} |p_s - q_s| \le \sqrt{1-F^2}}$$

**“Quantum states that are close in terms of their fidelity behave in all respects almost the same.”**

# Approximate Q-Computing

If F(ψ,ψ’)≈1, then having |ψ’〉 instead of |ψ〉 is equally good when performing computations.

If our ideal quantum circuit produces the outcome state ψ, then an approximate circuit that produces ψ’ also solves the computational problem. (If in doubt, run the computation several times and take the majority of the outcomes.)

Just as states can be close, so can gates and circuits.
For the task of quantum computation it is sufficient to implement the wanted unitary transformation approximately.

# Universal Q-Computing

- If we use a small set of standard gates {CCNOT, H, $R_z$} then we can implement (approximately) any possible unitary transformation $U \in \mathbb{C}^{D \times D}$.

- Moreover, if a circuit is build using a different set of gates {$G_1$,…,$G_r$}, then we can approximate this circuit efficiently using the {CCNOT, H, $R_z$} set. (You do this by finding the proper replacement circuits for $G_1$,…,$G_r$.)

- Other sets of gates are also possible.

- **“It does not really matter which gates you use to study quantum circuit complexity”.**

# Modern Church-Turing Thesis

- “Whatever we can build in the lab, we will be able to simulate it efficiently using our quantum circuit model.”

- By studying quantum circuit complexity we are studying the intrinsic computation complexity of problems in the quantum mechanical world as-we-know it.

- Note that complexity theory does depend on the fact that Nature is not classical (factoring, discrete log,…).

# General Set Up

- Input size n
  Consider a function $F:\{0,1\}^n \rightarrow \{0,1\}^m$
  We want to know some properties of F
  F is easy to compute, but $|\{0,1\}^n|$ is too big.

- **Quantum Approach:** Create a superposition of F(x) values by calculating F once on a superposition:

$$\boxed{\sum_{x\in\{0,1\}^n} \alpha_x \left|x,0\right\rangle \;\mapsto\; \sum_{x\in\{0,1\}^n} \alpha_x \left|x,F(x)\right\rangle}$$

- Then, do something quantum smart with this state.

# Partial Measurements

- What happens to $\sum_x \alpha_x |x,F(x)\rangle$ if we measure the F(x) part of the register, but not the x-part?

- Compare the two cases:

$$\boxed{\tfrac{1}{2}(|0\rangle+|1\rangle)\otimes(|0\rangle+|1\rangle) \mapsto \begin{cases} \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes|0\rangle & \text{outcome "0"} \\ \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes|1\rangle & \text{outcome "1"} \end{cases}}$$

$$\boxed{\tfrac{1}{\sqrt{2}}(|0,0\rangle+|1,1\rangle) \mapsto \begin{cases} |0,0\rangle & \text{outcome "0"} \\ |1,1\rangle & \text{outcome "1"} \end{cases}}$$

Informal: The state collapses according to the measurement outcome, but not more than that.

# Partial Measurements II

- **More formal description of Measurements**
- Consider a Boolean measurement on a superposition:

$$\boxed{\sum_{x \in \{0,1\}^n} \alpha_x \left| x, F(x) \right\rangle}$$

- Rewrite the state according to the Boolean values.

$$\boxed{\sum_{F(x)=0} \alpha_x \left| x, 0 \right\rangle \quad + \quad \sum_{F(x)=1} \alpha_x \left| x, 1 \right\rangle}$$

- Depending on the outcome, the state collapses to one of the two outcomes, with probability $\Sigma_x|\alpha_x|^2$ (sum over approriate x values F(x)=0 or F(x)=1).

# Partial Measurements III

- **Even more Formal Description of Measurement**
- Let M be the set of measurement outcomes, each quantum state φ can be written as

$$\boxed{|\varphi\rangle = \sum_{m\in M} \beta_m |\psi_m, m\rangle}$$

- When measuring the M quantity:
  - We observe $m \in M$ with probability $|\beta_m|^2$
  - State collapses as $|\varphi\rangle \mapsto |\psi_m, m\rangle$

- Note that this $\psi_m$ can still be a superposition.
- The state $|\psi_m, m\rangle$ is again properly normalized.

# Common Computational Setting

- We create a superposition of F:{0,1}$^n$ values, where the amplitudes are uniform over all x∈{0,1}$^n$. After that we measure an F(x)=y value, such that

$$\boxed{\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} \left|x, F(x)\right\rangle \mapsto \frac{1}{\sqrt{S_y}} \sum_{F(x)=y} \left|x, y\right\rangle}$$

- For each y∈M this happens randomly with probability $S_y/2^n$, where $S_y = |\{x : F(x)=y\}|$.

- *You can not use this to fast search* F(0),F(1),…

# 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

- Remember: Midterm is next Thursday, April 28
  Open book, open notes.

- New handout has been posted (on measurements).

- Do the exercises.

- New exercises and answers to old ones will be posted tomorrow (Friday).

- Tuesday: Q&A session of Midterm material.

# General Set Up

- Input size n
  Consider a function F:{0,1}$^n \rightarrow$ {0,1}$^m$
  We want to know some properties of F
  F is easy to compute, but |{0,1}$^n$| is too big.

- **Quantum Approach:** Create a superposition of F(x) values by calculating F once on a superposition:

$$\boxed{\sum_{x\in\{0,1\}^n} \alpha_x |x,0\rangle \mapsto \sum_{x\in\{0,1\}^n} \alpha_x |x,F(x)\rangle}$$

- Then, do something quantum smart with this state.

# A First Example (1)

- Consider a Boolean function: $F:\{0,1\}\rightarrow\{0,1\}$, Implemented by the unitary evolution $|x,b\rangle \mapsto |x,b\oplus F(x)\rangle$ for all x,b.

- <u>Question</u>: “F(0)=F(1)”?

- <u>Single Call</u> <u>Quantum</u> <u>Solution</u>: After calculating F only once in superposition we can answer the question perfectly.

# A First Example (2)

- Single Call Quantum Solution:

1. Apply Hadamard,Hadamard to 0,1 state
2. Apply F to superposition

Thus from $|0,1\rangle$ we get:

$$H \otimes H \mapsto \tfrac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle)$$

$$= \tfrac{1}{2}|0\rangle \otimes (|0\rangle - |1\rangle) + \tfrac{1}{2}|1\rangle \otimes (|0\rangle - |1\rangle)$$

$$F \mapsto \tfrac{1}{2}(-1)^{F(0)}|0\rangle \otimes (|0\rangle - |1\rangle) + \tfrac{1}{2}(-1)^{F(1)}|1\rangle \otimes (|0\rangle - |1\rangle)$$

$$= \tfrac{1}{2}\left[(-1)^{F(0)}|0\rangle + (-1)^{F(1)}|1\rangle\right] \otimes (|0\rangle - |1\rangle)$$

**Phase-Flip Trick**

# A First Example (3)

- Look at the left bit:

$$\text{If } F(0) = F(1) \text{ we have: } \quad \tfrac{1}{2}(-1)^{F(0)}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle)$$

$$\text{If } F(0) \neq F(1) \text{ we have: } \quad \tfrac{1}{2}(-1)^{F(0)}(|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle)$$

- $(|0\rangle+|1\rangle)/\sqrt{2}$ and $(|0\rangle-|1\rangle)/\sqrt{2}$ are orthogonal states

- Using a Hadamard on the first bit we can reliably distinguish between these two cases.

# A Simple Example (4)

- **Summary:**
  Using two qubits, a few Hadamards, a **single** application of the function F:|x,b⟩↦|x,b⊕F(x)⟩ and a final measurement we can determine if “F(0)=F(1)” or not.
- Classically you would need two evaluations of F to decide this problem.
- If evaluating F is very expensive, then this might be a useful speed-up to solve the problem.

- Crucial ingredient: Phase-Flip Trick:

$$F : |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \mapsto (-1)^{F(x)} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

# Deutsch-Jozsa Algorithm

- Generalization of the previous algorithm.
- Let F:{0,1}$^n$ → {0,1} with either:
  F is “constant”: F(0…0) = … = F(1…1), or
  F is “balanced”: 50% cases F(x)=0 and 50% F(x)=1
- Deutsch-Jozsa Algorithm decides this distinction with only one quantum-query F:$|x,b\rangle \mapsto |x,b\oplus F(x)\rangle$.

- First create superposition of x values and apply Phase-Flip Trick with F(x) values to the appended qubit state $(|0\rangle-|1\rangle)/\sqrt{2} = |-\rangle$, yielding:

$$\boxed{\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \otimes |-\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{F(x)} |x\rangle \otimes |-\rangle}$$

# Deutsch-Jozsa Algorithm 2

- Depending on whether F is constant or balanced, the (±1)-phases in the superposition are very different.
- Generalization of previous small example: apply n Hadamard gates to the n qubits.
- This gives

$$\boxed{\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{F(x)}\left|x\right\rangle \mapsto \begin{cases} (-1)^{F(0)}\left|0,\ldots,0\right\rangle & \text{if F constant} \\ \text{anything but } \left|0,\ldots,0\right\rangle & \text{if F balanced} \end{cases}}$$

- If we measure these bits then for the outcomes: “0…0” proves that F = constant; otherwise, F = balanced. Classically this requires $2^n/2 + 1$ queries.

# Central Question

- The crucial question that we try to answer in the theory of quantum algorithms is:

  **For which functions F can we determine which properties much faster than classically?**

  **For which F/properties combinations can we use this into a quantum algorithm that solves a relevant problem?**

# Quantum Query Results for Function F:{1,…,N} → {0,1}

- Searching "∃x:F(x)=1" ?
  - –Grover's search: $\boxed{\Theta(\sqrt{N})}$ versus classical $\Omega(N)$

- Parity "F(1) + … + F(N) mod2" ?
  - –Classical: N; Quantum: $\boxed{\frac{1}{2}\cdot N}$

- Interrogation "F(1),…,F(N)" ?
  - –(probabilistic) quantum: $\boxed{\frac{1}{2}N+\sqrt{N}}$ instead of N.