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

- Answers to Exercises III have been posted.

- Midterm will be Thursday, April 28 1pm – 2:50pm
  Open book/handouts/slides (use pdf), et cetera;
  calculators are allowed as well.

- Check out web site for last minute notices.

- Other questions?

Central Question

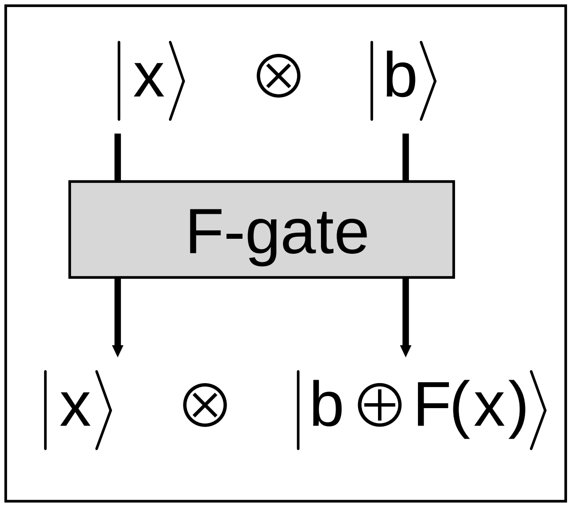
- The crucial question that we try to answer in the theory of quantum algorithms is:

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

  For which F/properties combinations can we use this as a subroutine to solve a natural problem?

Quantum Querying Functions

We assume that we have the network component:



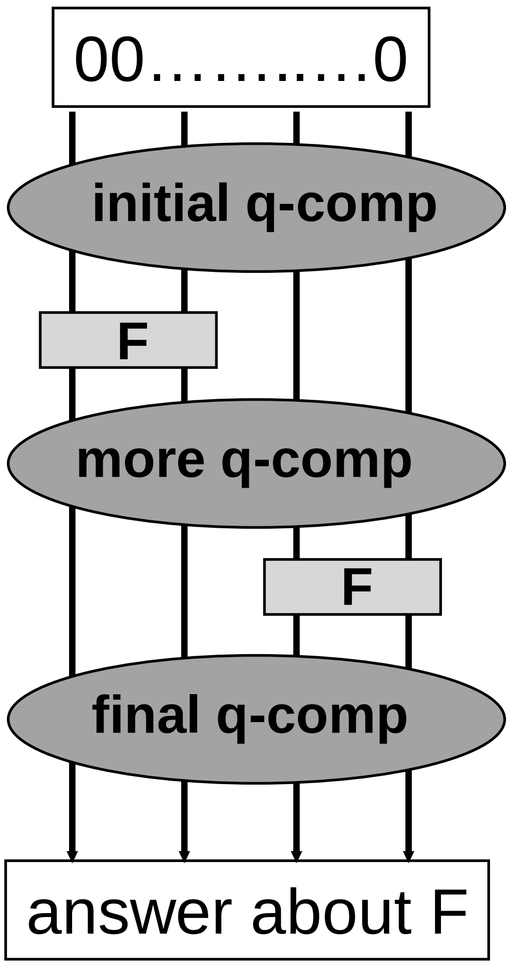
Let $F:\{0,1\}^n \rightarrow S$

There are things about F that
- are hidden,
- we can assume,
- we want to know,
- we are not interested in.

We want to minimize the queries to the F-*box when solving problems.*

Query and Time Complexity

Given the F-gate component, make a network:



Query Complexity:

"How many times do we have to use the F gate?"

Time Complexity:

"How big does the total gate network (including q-comp parts) have to be?"

Two observations:

1. Time complexity is what really counts.
2. Time complexity is lower bounded by query complexity.

Parity & Deutsch/Jozsa

- Let $F:\{1,\ldots,N\} \rightarrow \{0,1\}$ consist of N bits.
- What is the parity $F(1)\oplus F(2)\oplus\ldots\oplus F(N)$ of F?

- **Classically**: requires N queries to F.
  With <N queries your guess will be completely random.

- **Quantumly**: Deutsch/Jozsa allows us to compute $F(i)\oplus F(j)$ with one query for arbitrary i,j.
  By calculating $F(1)\oplus F(2)$, $F(3)\oplus F(4)$,…., $F(N-1)\oplus F(N)$ we can determine the parity in N/2 F-queries.

Quantum Searching

- Let $F:\{1,\ldots,N\} \rightarrow \{0,1\}$ with $F(j)=0$ for almost all j, and $F(t)=1$ for a unique unknown *target* element $1 \leq t \leq N$.
- Task: determine this t.

- **Classically**:
  Deterministically you need $N-1$ queries to F.
  Probabilistically you need $\Theta(N)$ queries to F.

- **Quantum Computing**:
  Exercises III showed that for $N=4$ we need one query.
  In general, we need $\Theta(\sqrt{N})$ quantum queries to F.

Uppers and Downers

- [Grover] showed that searching a database of size N can be done with $O(\sqrt{N})$ quantum queries.
- [Bennett, Bernstein, Brassard & Vazirani] showed (earlier) that $\Omega(\sqrt{N})$ queries are required.

- Note that a result of O(log N) quantum queries would show that we can solve all NP problems in quantum-polynomial time. BBBV shows that life is not that easy.

- This is typical: Quantum computing is no snake oil.

- To get real good results we need to understand the **Quantum Fourier Transformation**.