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

- This Thursday: Talk by M. Steffen on “Nuclear Magnetic Resonance” (NMR) quantum computing.
- Handout on Fourier transform and new Exercises are posted on web site.
- Comprehensive exams will be *closed* book.
- Questions?

Last Week

- We can use the quantum Fourier transformation to find the unknown period of a proper periodic function F.

- By using functions like $F = x^t \bmod N$, we can factorize N and calculate the discrete logarithm mod N.

- Some nontrivial number theory was involved,
  as well as some (hand waving) arguments that an approximation of the function F (where the period does not divide the size of the domain) works as well.

Quantum Fourier Transform

Consider the mod N numbers {0,1,2,…,N–1}.
The "Quantum Fourier Transform over $\mathbb{Z}_N$" is defined for each $x \in \{0,1,\ldots,N-1\}$ by

$$\boxed{|x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i \cdot xy/N} |y\rangle}$$

Hence for each superposition over mod N:

$$\boxed{\sum_{x=0}^{N-1} \alpha_x |x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \sum_{x=0}^{N-1} \alpha_x \cdot e^{2\pi i \cdot xy/N} |y\rangle}$$

Important fact: The QFT can be efficiently implemented in circuit size poly(log(N)) for each N.

Quantum Searching

Consider function $F:\{0,\ldots,N-1\} \to \{0,1\}$,
where for one $0 \le t < N$ we have $F(t)=1$.
<u>Task</u>: Find t with a minimum of F queries.
<u>Solution</u>: Lov Grover's quantum search algorithm requires only $O(\sqrt{N})$ queries (and is optimal).
This algorithm consists of a repeated sequence of Fourier transforms over $\mathbb{Z}_N$, phase flip operations

$$\boxed{U_F : |j\rangle \mapsto (-1)^{F(j)}|j\rangle}$$

and

$$\boxed{U_0 : |j\rangle \mapsto \begin{cases} |0\rangle & \text{if } j = 0 \\ -|j\rangle & \text{otherwise} \end{cases}}$$

Grover Iteration

- The 'Grover Iteration' is defined by

$$\boxed{G_F = Four_N \cdot U_0 \cdot Four_N \cdot U_F}$$

Note that U_F be implemented with one call to the black-box function F in combination with the phase-flip trick:
If $F:|j,b\rangle \mapsto |j,b \oplus F(j)\rangle$, then $F:|j\rangle \otimes |-\rangle \mapsto (-1)^{F(j)}|j\rangle \otimes |-\rangle$.

Instead of the Fourier transformation over $\mathbb{Z}_N$,
we can also use other 'mixing operations'.
For example, if $N=2^n$ then $H \otimes \ldots \otimes H$ works as well.

The Grover iteration 'amplifies' the amplitude of the correct state $|t\rangle$ with $F(t)=1$, at the expense of the others.

Grover's Algorithm

Given a black box function $F:\{0,\ldots,N-1\} \rightarrow \{0,1\}$.

1. Create the uniform superposition (using Four_N):

$$\boxed{\left|\psi_0\right\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}\left|j\right\rangle}$$

2. Apply the Grover iteration T times to $|\psi\rangle$.

3. Measure the register for answer t'.
4. (Check that t' indeed gives F(t')=1.)

Analyzing Grover's Algorithm

A proper analysis of the previous algorithm shows that after the k-th iteration, the amplitude of the target state "t" is: $\langle t|\psi_k\rangle = \sin(\theta(2k+1)/2)$ with $\sin(\theta)=2\sqrt{(N-1)}/N$.
For large enough N, this gives $\theta \approx 2/\sqrt{N}$, such that $\langle t|\psi_k\rangle \approx \sin((2k+1)/\sqrt{N})$, which shows that $k \approx \frac{1}{4}\pi\sqrt{N}$ works.

[Nielsen&Chuang "QC&QI", Sections 6–6.1.4] gives a more detailed analysis that also shows that with M solutions (instead of 1), you only need $\approx \frac{1}{4}\pi\sqrt{(N/M)}$ queries to the black box function.
(If N/M = 4, then only one call is required.)