6.857 Computer and Network Security	November 29, 2001

Lecture Notes 23 : Wrap-up

Lecturer: Ron Rivest — *Scribe: Chen/Kim/Kwon/Medak*

1 Topics

- Wrap-up
- Shor's Factoring Algorithm

2 Wrap-up

- Talks start next week
- Richard Clarke speaks on 12/10 at 6pm in NE43-518
- Follow on courses:
  - 6.875, 6.876 (crypto theory)
  - 6.824 (distributed systems engineering)
  - 6.806 (Ethics and Law on Electronic Frontier)

3 Quantum Computation

We start with a small example, to illustrate how probabilistic computation and quantum computation differ.

Suppose that we have two die–one red and one blue. What is the probability of getting a 3? There are two ways of doing so, 1+2 or 2+1, shown in the two rows of the following table.

Red die	Blue die	Probability	Amplitude	Probability
1	2	$\frac{1}{36}$	$\frac{1}{6}$	$\frac{1}{36}$
2	1	$+\ \frac{1}{36}$	$+\ \frac{-1}{6}$	$\frac{1}{36}$
		$\frac{2}{36}$	0 add first $\rightarrow$	0

In the "probability" column, we show the chance of each possibility as 1/36. In a classical computer these probabilities add, so the final probability is 2/36 of getting a 3.

In the last two columns, we illustrate the notion of destructive interference that can happen in a quantum computer. Here the events have complex amplitudes, and the amplitudes add, not the probabilities. For example, suppose 1+2 has amplitude 1/6 (and thus probability 1/36) and that 2+1 has amplitude -1/6 (and thus probability 1/36 as well). But now the event of "getting a 3" has amplitude 0 (and thus probability zero)! If we only measure the sum of the two die, we could never see a 3, even though if we measure the two individual dies, we would see 1+2 happen with probability 1/36.

Question: How can the probability add to 0?
Answer: You don't add the probability, you add the amplitude first. It's similar to destructive interference with light.

Question: How are you representing the die?
Answer: This is just a pedagogical example to illustrate destructive interference.

Here is another example of computation on qubits, as a warm-up: the square root of NOT!

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

$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \frac{(\alpha+\beta)}{\sqrt{2}} \\ \frac{(\alpha-\beta)}{\sqrt{2}} \end{bmatrix}$

$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$ is like $\sqrt{not}$ because squaring it gives the NOT matrix $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$

4 Factoring

Here is the outline of Shor's algorithm:

Given n which we wish to factor
Pick x at random
Find r s.t. $x^r \equiv 1 (\bmod\ n)$ where r is the order of $x (\bmod\ n)$

with probability $\geq \frac{1}{2}$ r is even $\rightarrow (x^r - 1) = 0 (\bmod\ n)$ *and* $(x^{\frac{r}{2}} - 1)(x^{\frac{r}{2}} + 1) = 0 (\bmod\ n)$

$gcd(x^{\frac{r}{2}} - 1, n) = p \;\; p|n$ with high probability

4.1 Basics

Cloning would take:

$$(\alpha|0> + \beta|1>)\cdot(|0>) = \begin{pmatrix}\alpha\\0\\\beta\\0\end{pmatrix} = \begin{pmatrix}w\\x\\y\\z\end{pmatrix}$$

Clone $\begin{pmatrix}\alpha^2\\\alpha\beta\\\alpha\beta\\\beta^2\end{pmatrix} \leftarrow$ no unitary transform can give this result.

Need reversibility, but "controlled XOR" is OK. $(q_1, q_2) \to (q_1, q_2 \oplus q_1)$
So we can "copy" in a reversible manner.

$$\begin{array}{c} |00> \\ |01> \\ |10> \\ |11> \end{array} \begin{pmatrix} 1 & 0 & & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{array}{c}\text{like one} - \text{round} \\ \text{Feistel} \\ \overset{q_1}{|} \longrightarrow \overset{q_2}{\oplus}\end{array}$$

Can go from $|\underline{x}, \underline{0}>$ to $|\underline{\mathrm{x}}, \underline{\mathrm{f}}(\mathrm{x})>$ for an arbitrary function f, so we are really not limited.
multi-qubit registers
$|x, y>$ to $|\mathrm{x}, \mathrm{y} \oplus \mathrm{f}(\mathrm{x})>$

Theorem 1 *Shor's Factoring algorithm: Find* ***order*** r *of* x*, mod* n $(x^r \equiv 1 \bmod n)$
if r *even (which it is often) then* $(x^{r/2}-1)(x^{r/2}+1) \equiv 0(\mathrm{mod} n)$ *try gcd*$(x^{r/2}-1, n) =?$

1. $\frac{1}{\sqrt{q}} \sum_{k=1}^{q} |k, 0>$ (flip coins) $q \approx n^2$, q smooth e.g. 2^k

2. $\frac{1}{\sqrt{q}} \sum_{k=1}^{q} |k, f(k)>, f(x) = x^k \bmod n$

3. Fourier: $|k- > \mapsto \frac{1}{\sqrt{q}} \sum_{h=1}^{q} e^{\frac{2\pi hki}{q}} |h, ->$
   $\frac{1}{q} \sum_{h=1}^{q} \sum_{k=1}^{q} e^{\frac{2\pi ihk}{q}} |h, f(k)>$
   Classical: probabilities add.
   Quantum: amplitudes add. Prob = $|\mathrm{amp}|^2$.

4. Think of $k = ar + b$
   $$\frac{1}{q} \sum_{h=1}^{1} \sum_{b=1}^{r} \underbrace{\sum_{a=0}^{\frac{(a-b)}{r}} e^{\frac{2\pi ih(ar+b)}{q}}}_{innersum} |h, f(b)>$$
   Innersum is large in absolute value if $\frac{hr}{q}$ near an integer, else small.

5. Observe h: likely that $\frac{hr}{q}$ near an integer $\frac{h}{q} \to \frac{1}{r}$; this gives a way to find r, as desired, and thus factor n.