There will be no lecture on June 30. There were lots of errors in the previous handout. I am sorry for that. The corrected version follows.

Let $|0\rangle, \ldots, |N-1\rangle$ be an orthonormal basis of an N-dimensional space. The QFT transforms

$$|j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp(2\pi ijk/N)|k\rangle.$$

The inverse of QFT is given by

$$|k\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{\ell=0}^{N-1} \exp(-2\pi ik\ell/N)|\ell\rangle. \qquad (1)$$

The inverse QFT can also be realized efficiently ($n(n+1)/2$ operations) by reversing the operation of QFT.

Phase estimation 1

Suppose that we have a unitary matrix U and its eigenvector vector $|u\rangle$. Let $\exp(2\pi i\theta)$ be the eigenvalue to which $|u\rangle$ belongs to. We shall show how we can compute θ.

Assumption: We are able to do the controlled-U^{2^j} operation for any $j \geq 0$.

Suppose that we apply the controlled-U^{2^j} to $(|0\rangle + |1\rangle)|u\rangle$, with $|u\rangle$ being the target (we omit the normalizing factor $1/\sqrt{2}$). Then the result is

$$\begin{aligned} & |0\rangle|u\rangle + |1\rangle \otimes U^{2^j}|u\rangle \\ = \; & |0\rangle|u\rangle + |1\rangle \otimes \exp(2\pi i 2^j\theta)|u\rangle \\ = \; & (|0\rangle + \exp(2\pi i 2^j\theta)|1\rangle) \otimes |u\rangle \end{aligned}$$

Assume we have t qubits that are initialized to $(|0\rangle + |1\rangle)/\sqrt{2}$, and apply the controlled-U^{2^j} to the j-th qubit (the rightmost is the zero-th). The result is

$$\begin{aligned} & \frac{1}{2^{t/2}}(|0\rangle + \exp(2\pi i 2^{t-1}\theta)|1\rangle) \otimes \cdots \otimes (|0\rangle + \exp(2\pi i 2^0\theta)|1\rangle) \\ = \; & \frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} \exp(2\pi i k\theta)|k\rangle. \end{aligned} \tag{2}$$

2009-10-2

Applying the IQFT in Eq. (1) to the above state yields

$$\frac{1}{2^t}\sum_{\ell=0}^{2^t-1}\sum_{k=0}^{2^t-1}\exp\left(\frac{-2\pi ik\ell}{2^t}\right)\exp(2\pi ik\theta)|\ell\rangle.$$

Distribution of the measurement outcomes 1

$$\frac{1}{2^t}\sum_{\ell=0}^{2^t-1}\sum_{k=0}^{2^t-1}\exp\left(\frac{-2\pi ik\ell}{2^t}\right)\exp(2\pi ik\theta)|\ell\rangle.$$

We shall compute the probability distribution of the mesurement in the $\{|0\rangle, |1\rangle, |2\rangle, \ldots, |2^t-1\rangle\}$ basis. (The observable is $\sum_{j=0}^{2^t-1}\beta_j|j\rangle\langle j|$.) Recall that $0 \le \theta < 1$, and we can write

$$\theta = 0.b_1b_2\cdots b_tb_{t+1}\cdots.$$

Let $b = b_1b_2\cdots b_t$. We have $0 \le b \le 2^t-1$. Let α_c be the coefficient of $|(b+c) \bmod 2^t\rangle$ in the result of the IQFT. We shall show that if c is large then $|\alpha_c|$ is small. Observe that the coefficient of $|\ell\rangle$ is

$$\begin{aligned}&\frac{1}{2^t}\sum_{k=0}^{2^t-1}\exp\left(\frac{-2\pi ik\ell}{2^t}\right)\exp(2\pi ik\theta)\\ =\ &\frac{1}{2^t}\sum_{k=0}^{2^t-1}\left[\exp\left(2\pi i(\theta-\ell/2^t)\right)\right]^k\end{aligned}$$

Substituting ℓ with $b+c$ we have

$$\alpha_c = \frac{1}{2^t}\sum_{k=0}^{2^t-1}\left[\exp\left(2\pi i(\theta-(b+c)/2^t)\right)\right]^k \qquad (3)$$

This is the sum of a geometric series, so it is equal to

$$\alpha_c = \frac{1}{2^t} \cdot \frac{1 - \exp(2\pi i(2^t\theta - (b+c)))}{1 - \exp(2\pi i(\theta - (b+c)/2^t))}$$

Define $\delta = \theta - b/2^t$, then

$$\alpha_c = \frac{1}{2^t} \cdot \frac{1 - \exp(2\pi i(2^t\delta - c))}{1 - \exp(2\pi i(\delta - c/2^t))}$$

We shall upper bound the probability of getting a measurement outcome m such that $|m - b| > e$. We have

$$p(|m - b| > e) = \sum_{-2^{t-1} < c \leq -e-1, e+1 \leq c < 2^{t-1}} |\alpha_c|^2.$$

Since $|1 - \exp(ix)| \leq 2$,

$$|\alpha_c| \leq \frac{2}{2^t |1 - \exp(2\pi i(\delta - c/2^t))|}.$$

We have $|1 - \exp(ix)| \geq 2|x|/\pi$ for $-\pi \leq x \leq \pi$ and $-\pi \leq 2\pi(\delta - c/2^t) \leq \pi$, it follows

$$|\alpha_c| \leq \frac{1}{2^{t+1} |\delta - c/2^t|}.$$

Therefore we have

$$
\begin{aligned}
& 4p(|m-b|>e) \\
\leq & \sum_{-2^{t-1}<c\leq -e-1} \frac{1}{(2^t\delta - c)^2} + \sum_{e+1\leq c<2^{t-1}} \frac{1}{(2^t\delta - c)^2} \\
\leq & \sum_{-2^{t-1}<c\leq -e-1} \frac{1}{c^2} + \sum_{e+1\leq c<2^{t-1}} \frac{1}{(c-1)^2} \\
\leq & 2 \sum_{e\leq c<2^{t-1}-1} \frac{1}{c^2} \\
\leq & 2\int_{e-1}^{2^{t-1}-1} \frac{dc}{c^2} \\
\leq & 2\int_{e-1}^{\infty} \frac{dc}{c^2} \\
= & \frac{2}{(e-1)} \text{ if } e>1.
\end{aligned}
$$

Suppose that we want an accuracy of 2^{-n}, that is, $|\theta - m/2^t| < 2^{-n}$.

$$
\begin{aligned}
& |\theta - m/2^t| < 2^{-n} \\
\Leftrightarrow & |2^t\theta - m| < 2^{t-n} \\
\Leftarrow & |b-m| < 2^{t-n} - 1.
\end{aligned}
$$

We can see that $e = 2^{t-n} - 1$ ensures the desired accuracy. The probability of the accuracy below 2^{-n}

is $1/2(2^{t-n} - 2)$ In order for $1/2(2^{t-n} - 2) < \epsilon$, we need $t \geq n + \log_2(2 + 1/2\epsilon)$.

Factor $N = pq$

Suppose that we are give $N = pq$, with distinct primes p and q, and asked to compute p and q. We assume that N is odd. In order to break the RSA, we need this kind of computation.

Firstly randomly choose $2 \leq x \leq N-1$, and see if $\gcd(x, N) > 1$. If so, then $x = p$ or $x = q$.

Otherwise, compute the order of x modulo N, that is

$$\mathrm{ord}(x, N) = \min\{i \geq 1 \mid x^i \bmod N = 1\}$$

If $\gcd(x, N) > 1$ then there is no i such that $x^i \bmod N = 1$. So we have to exclude this case first.

Theorem 1 Choose an integer x uniformly at random such that $\gcd(x, N) = 1$ and $1 \leq x \leq N-1$, define $r = \mathrm{ord}(x, N)$. Then the probability of the event that r is even and $x^{r/2} \bmod N \neq N-1$ is $\geq 3/4$.

Proof. Omitted. A copy of proof is proveded.

Assume that r is even and $x^{r/2} \bmod N \neq N-1$. Otherwise choose x again until the above condition is satisfied.

Theorem 2 Let z be an integer such that $2 \leq z \leq N-2$ and $z^2 \bmod N = 1$. Then at least one of $\gcd(z+1, N)$ or $\gcd(z-1, N)$ is greater than 1 and divides N.

2009-10-10

Proof. Omitted. A copy of proof is provided.
Thus, $\gcd(x^{r/2} + 1 \bmod N, N)$ or $\gcd(x^{r/2} - 1 \bmod N, N)$ is equal to p or q.

2009-10-11

Computing the order of x modulo N

There is no known fast algorithm for computing the order of x modulo N. I will introduce a fast quantum algorithm.

Let $2^{L-1} \leq N \leq 2^L - 1$ and $0 \leq y \leq 2^L - 1$, define the unitary operator U such that

$$U|y\rangle = |xy \bmod N\rangle.$$

We define $xy \bmod N = y$ if $N \leq y \leq 2^L - 1$. The order of x modulo N is related to the phase of eigenvalues of U as follows.

Recall $r = \mathrm{ord}(x, N)$. For $0 \leq s \leq r - 1$, define the L-qubit quantum state

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left(\frac{-2\pi isk}{r}\right) |x^k \bmod N\rangle.$$

Then we have

$$\begin{aligned} U|u_s\rangle &= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left(\frac{-2\pi isk}{r}\right) U|x^k \bmod N\rangle \\ &= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left(\frac{-2\pi isk}{r}\right) |x^{k+1} \bmod N\rangle \\ &= \frac{1}{\sqrt{r}} \sum_{k=1}^{r} \exp\left(\frac{-2\pi is(k-1)}{r}\right) |x^k \bmod N\rangle \end{aligned}$$

2009-10-12

$$
\begin{aligned}
&= \exp\left(\frac{2\pi i s}{r}\right) \frac{1}{\sqrt{r}} \sum_{k=1}^{r} \exp\left(\frac{-2\pi i s k}{r}\right) |x^k \bmod N\rangle \\
&= \exp\left(\frac{2\pi i s}{r}\right) \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left(\frac{-2\pi i s k}{r}\right) |x^k \bmod N\rangle \\
&= \exp\left(\frac{2\pi i s}{r}\right) |u_s\rangle
\end{aligned}
$$

If we can estimate the phase of the eigenvalue of $|u_s\rangle$, we know s/r. From which we could know r. The obstacle is that the preparation of $|u_s\rangle$ requires the knowledge of r. Let us see how we can bypass this difficulty.

$$
\begin{aligned}
& \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle \\
= \; & \frac{1}{r} \sum_{k=0}^{r-1} \left(\sum_{s=0}^{r-1} \exp\left(\frac{-2\pi i s k}{r}\right) \right) |x^k \bmod N\rangle
\end{aligned}
$$

We shall show that

$$
\sum_{s=0}^{r-1} \exp\left(\frac{-2\pi i s k}{r}\right) = r\delta_{k0}
$$

Consider the sequence $0k \bmod r$, $k \bmod r$, $2k \bmod r$, ... Define $d = \min\{j \geq 1 \mid jk \bmod r = 0\}$. d

must divide r otherwise $rk \bmod r$ would not be zero. Moreover, $jk \bmod r = (j+d)k \bmod r$. Therefore,

$$\begin{aligned} & \sum_{s=0}^{r-1} \exp\left(\frac{-2\pi isk}{r}\right) \\ = & \frac{r}{d} \sum_{s=0}^{d-1} \exp\left(\frac{-2\pi isk}{r}\right) \end{aligned}$$

On the other hand, if $0 \leq j \neq j' \leq d-1$ then $jk \bmod r \neq j'k \bmod r$, otherwise $(j-j')k \bmod r = 0$, which is a contradiction to the minimality of d. This means that

$$\exp\left(\frac{-2\pi i0k}{r}\right), \exp\left(\frac{-2\pi i1k}{r}\right), \ldots, \exp\left(\frac{-2\pi i(d-1)k}{r}\right)$$

are pairwise distinct roots of $X^d - 1 = 0$.

$$\begin{aligned} X^d - 1 &= \prod_{s=0}^{d-1} (X - \exp\left(\frac{-2\pi isk}{r}\right)) \\ &= X^d + \cdots + \sum_{s=0}^{d-1} \exp\left(\frac{-2\pi isk}{r}\right) X - 1. \end{aligned}$$

This means that

$$\sum_{s=0}^{d-1} \exp\left(\frac{-2\pi isk}{r}\right) = 0.$$

2009-10-14

This means that

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |x^0 \bmod N\rangle = |1\rangle.$$

If we use the phase estimation algorithm with $|1\rangle$, then we get the outcome close s/r with probability $1/r$ for $s = 0, \ldots, r-1$.
The reason is as follows: For $|u_s\rangle$ the probability of outcome far from s/r is almost zero. This means that measurement outcomes of distinct $|u_s\rangle$ and $|u_{s'}\rangle$ do not (almost) overlap.
Let M be an observable with distinct nondegenerate eigenvalues $\lambda_1, \ldots, \lambda_m$ and $\eta_1, \ldots, \eta_n$. Suppose that a state $|\varphi\rangle$ gives measurement outcome λ_i with probability p_i and $|\psi\rangle$ gives η_i with probability q_i. Then $(|\varphi\rangle + |\psi\rangle)/\sqrt{2}$ gives measurement outcomes λ_i with probability $p_i/2$ and η_i with probability $q_i/2$. Observe the similarity between $(|\varphi\rangle + |\psi\rangle)/\sqrt{2}$ and $\sum_{s=0}^{r-1} |u_s\rangle/\sqrt{r}$. The reason is as follows.
Let $|\varphi_i\rangle$ be the eigenvector of λ_i and $|\psi_i\rangle$ be the eigenvector of η_i. Then we have

$$\begin{aligned} |\varphi\rangle &= \alpha_1|\varphi_1\rangle + \cdots + \alpha_m|\varphi_m\rangle, \\ |\psi\rangle &= \beta_1|\psi_1\rangle + \cdots + \beta_n|\psi_n\rangle. \end{aligned}$$

Thus

$$\frac{|\varphi\rangle + |\psi\rangle}{\sqrt{2}} = \sum_{i=1}^{m} \frac{\alpha_i}{\sqrt{2}} |\varphi_i\rangle + \sum_{i=1}^{n} \frac{\beta_i}{\sqrt{2}} |\psi_i\rangle. \qquad (4)$$

The rest of reasoning is your exercise.
In the next lecture, I will show that how to compute r from a binary fractional ditits $0.b_1 b_2 \dots b_t$ that is close to s/r for some unknown $0 \leq s \leq r-1$.

Exercise

Submit your answer to the box in front of Room 311, S3 building, by 17:00 Thursday, if you don't finish by 12:10.

1. Let $N = 3 \times 7$ and $x = 2$. Compute $r = \mathrm{ord}(x, N)$.
2. Tell if $x^{r/2} \neq N - 1 \bmod N$.
3. Tell if $x^{r/2} - 1$ or $x^{r/2} + 1$ is a factor of N.
4. Compute $|u_s\rangle$ with above values and $s = 1$.
5. Let U be as defined in the lecture. With above x and N, what is the eigenvalue of U to which $|u_1\rangle$ belongs?
6. Explain why the state in Eq. (4) gives measurement outcome λ_i with probability $p_i/2$ and η_i with probability $q_i/2$.
7. If your answers to the previous exercises were evaluated as incorrect, please indicate whether or not you agree to that evaluation. Write which part in today's lecture was difficult for your understanding.

2009-10-17