Lecture 19

Comment: Plan for HW3 to be released today – expect to be short. Plan for guidelines on exam, and some practice questions, released by end of week.

Cost of O_f. Recall the f used in Shor's algorithm

$$f\colon \{0,1,\ldots,M-1\} \to \{0,1\ldots,N-1\}; \quad x \mapsto a^x \mod N \tag{101}$$

Say $M = 512$, $a = 11$ and $N = 21$ and you want to compute $f(91)$. Naive way

$$11^1 \mod 21, \quad 11^2 \mod 21, \quad 11^3 \mod 21, \ldots, 11^M \mod 21 \tag{102}$$

time complexity M but M is chosen to be about N^2 so no good!

Idea: repeated squaring: all equations are mod 21.

$$\begin{aligned}
11^1 =& 11\\
11^2 =& 11^2 = 121 = 16\\
11^4 =& (11^2)^2 = 16^2 = 256 = 4\\
11^8 =& (11^4)^2 = 4^2 = 16\\
11^{16} =& (11^8)^2 = 16^2 = 4\\
11^{32} =& (11^{16})^2 = 16\\
11^{64} =& (11^{32})^2 = 16^2 = 4
\end{aligned}$$

Number of rows: $\log_2(91) \le O(\log(M))$, each row involves squaring a number in $\{0,1,\ldots,N-1\}$ which has $O(\log(N))$ bits, so costs $O(\log^2(N))$. So getting the table costs $O(\log(M)\log^2(N))$.

Finally, assemble from table: $91 = 64+16+8+2+1$ so $11^{91} = 4 \times 4 \times 16 \times 16 \times 11 = 64 \times 11 = 11$. There are $\log_2(91) \le O(\log(M))$ multiplications of $O(\log(N))$-bit numbers, so costs another $O(\log(M)\log^2(N))$.

Overall cost: $O(\log(M)\log^2(N)) = O(\log^3(N))$ since M is about N^2.

Cost of QFT. Recall the QFT used in Shor's algorithm.

Definition 20. Let M be a positive integer. The QFT on $\mathbb{C}^M$ is the unitary defined by

$$\mathrm{QFT}_M |j\rangle = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} \omega_M^{kj} |k\rangle, \quad \text{for all } j \in \{0,1,\ldots,M-1\} \tag{103}$$

where $\omega_M \coloneqq \exp(2\pi i/M)$.

Consider when $M = 2^n$ for some positive integer n. Write $j = x_1 \ldots x_n$ and $k = y_1 \ldots y_n$ in binary.

Then, the amplitude on $|k\rangle$ of $\mathrm{QFT}_M |j\rangle$ is

$$\begin{aligned}
\frac{1}{\sqrt{2^n}}\omega_M^{kj} =& \frac{1}{\sqrt{2^n}}\omega_M^{(2^{n-1}y_1+\cdots+y_n)(2^{n-1}x_1+\cdots+x_n)} && (104)\\
=& \frac{1}{\sqrt{2^n}}\exp(2\pi i(2^{n-1}y_1 + 2^{n-2}y_2 + \cdots + y_n)[0.x_1x_2\ldots x_n]) && (105)\\
=& \frac{1}{\sqrt{2^n}}\exp(2\pi i(2^{n-1}y_1)[0.x_1x_2\ldots x_n]) \cdot \exp(2\pi i(2^{n-2}y_2)[0.x_1x_2\ldots x_n]) \cdots \exp(y_n[0.x_1x_2\ldots x_n]) && (106)\\
=& \frac{1}{\sqrt{2^n}}\exp(2\pi i(2^{n-1}y_1)[0.x_1x_2\ldots x_n]) \cdot \exp(2\pi i(2^{n-2}y_2)[0.x_1x_2\ldots x_n]) \cdots \exp(2\pi i y_n[0.x_1x_2\ldots x_n]) && (107)\\
=& \frac{1}{\sqrt{2}}\exp(2\pi i(y_1)[x_1\ldots x_{n-1}.x_n]) \cdot \frac{1}{\sqrt{2}}\exp(2\pi i(y_2)[x_1\ldots x_{n-2}.x_{n-1}x_n]) \cdots \frac{1}{\sqrt{2}}\exp(2\pi i y_n[0.x_1x_2\ldots x_n]) && (108)\\
=& \frac{1}{\sqrt{2}}\exp(2\pi i y_1[0.x_n]) \cdot \frac{1}{\sqrt{2}}\exp(2\pi i y_2[0.x_{n-1}x_n]) \cdots \frac{1}{\sqrt{2}}\exp(2\pi i y_n[0.x_1x_2\ldots x_n]) && (109)
\end{aligned}$$

Therefore,

$$
\begin{aligned}
&\mathrm{QFT}_M \left|j\right\rangle \\
=& \sum_{y_1,\ldots,y_n \in \{0,1\}} \frac{1}{\sqrt{2}} \exp(2\pi i y_1 [0.x_n]) \cdot \frac{1}{\sqrt{2}} \exp(2\pi i y_2 [0.x_{n-1}x_n]) \cdots \frac{1}{\sqrt{2}} \exp(2\pi i y_n [0.x_1 x_2 \ldots x_n]) \left|y_1 \ldots y_n\right\rangle \\
=& \sum_{y_2\ldots,y_n \in \{0,1\}} \frac{1}{\sqrt{2}} 1 \cdot \frac{1}{\sqrt{2}} \exp(2\pi i (y_2) [0.x_{n-1}x_n]) \cdots \frac{1}{\sqrt{2}} \exp(2\pi i y_n [0.x_1 x_2 \ldots x_n]) \left|0 y_2 \ldots y_n\right\rangle \\
&\quad + \sum_{y_2\ldots,y_n \in \{0,1\}} \frac{1}{\sqrt{2}} \exp(2\pi i [0.x_n]) \cdot \frac{1}{\sqrt{2}} \exp(2\pi i y_2 [0.x_{n-1}x_n]) \cdots \frac{1}{\sqrt{2}} \exp(2\pi i y_n [0.x_1 x_2 \ldots x_n]) \left|1 y_2 \ldots y_n\right\rangle \\
=& \frac{1}{\sqrt{2}} (\left|0\right\rangle + \exp(2\pi i [0.x_n]) \left|1\right\rangle) \otimes \sum_{y_2\ldots,y_n \in \{0,1\}} \frac{1}{\sqrt{2}} \exp(2\pi i y_2 [0.x_{n-1}x_n]) \cdots \frac{1}{\sqrt{2}} \exp(2\pi i y_n [0.x_1 x_2 \ldots x_n]) \left|y_2 \ldots y_n\right\rangle \\
=& \ldots \\
=& \frac{1}{\sqrt{2}} (\left|0\right\rangle + \exp(2\pi i [0.x_n]) \left|1\right\rangle) \otimes \frac{1}{\sqrt{2}} (\left|0\right\rangle + \exp(2\pi i [0.x_{n-1}x_n]) \left|1\right\rangle) \otimes \cdots \otimes \frac{1}{\sqrt{2}} (\left|0\right\rangle + \exp(2\pi i [0.x_1 x_2 \ldots x_n]) \left|1\right\rangle)
\end{aligned}
$$

The above reveals that the QFT can be implemented by the following circuit. Comment: This is up to a final swapping of qubits – at most $n/2$ "SWAP gates" if you care to count – or you could just use the circuit directly with the understanding that the output qubits are ordered in reverse to the usual definition of QFT.

$$
H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{and} \quad R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{i2\pi/2^k} \end{pmatrix}
$$

The circuit is composed of H gates and the controlled version of R_k:

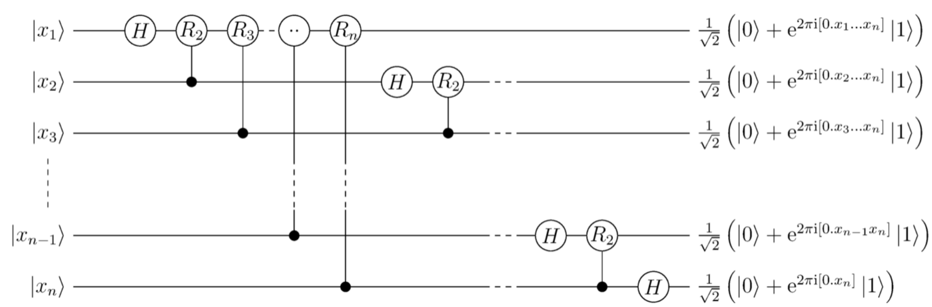

Figure 1: QFT without the final swaps. Note that on the second wire, the last gate is controlled R_{n-1}. On the third wire, the last gate is controlled R_{n-2}. In general, on the ith wire, the last gates is controlled R_{n-i+1} for $i \in \{1, \ldots, n-1\}$.