MASSACHUSETTS INSTITUTE OF TECHNOLOGY

2.111J/18.435J/ESD.79
Quantum Computation

Problem 1. Find a circuit with $cn\log n$ gates that gives a good approximation to QFT on n qubits. (c is a constant.)

Solution:

The circuit in Fig. 5.1 consists of $n(n+1)/2$ gates. In order to find a circuit with $cn\log n$ gates, we approximate the operators $R_j = |0\rangle\langle 0| + \exp(2\pi i/2^j)|1\rangle\langle 1|$ by the identity operator for $j > k = c\lceil \log_2 n \rceil$. Then, clearly the number of gates on each line of Fig. 5.1 is less than or equal to $c\log n$, and therefore, the total number of gates is on the order of $n\log n$. Now, we find the error due to this approximation. If we denote the operation by the ideal QFT circuit by U and our approximation by V, for any basis vector $|j\rangle$, from (5.9) and (5.18), we have

$$U|j\rangle = \frac{1}{2^{n/2}}\bigotimes_{l=1}^{n}\left(|0\rangle + e^{2\pi i j 2^{-l}}|1\rangle\right)$$

$$= \frac{1}{2^{n/2}}\bigotimes_{l=1}^{k}\left(|0\rangle + e^{2\pi i j 2^{-l}}|1\rangle\right)\otimes\left(|0\rangle + e^{2\pi i 0.j_{n-k}\cdots j_{n-1}j_n}|1\rangle\right)\otimes\cdots\otimes\left(|0\rangle + e^{2\pi i 0.j_1\cdots j_n}|1\rangle\right)$$

$$= \frac{1}{2^{k/2}}\bigotimes_{l=1}^{k}\left(|0\rangle + e^{2\pi i j 2^{-l}}|1\rangle\right)\otimes|\phi_k\rangle\otimes\cdots\otimes|\phi_{n-1}\rangle$$

where

$$|\phi_m\rangle = \left(|0\rangle + e^{2\pi i 0.j_{n-m}\cdots j_{n-1}j_n}|1\rangle\right)/\sqrt{2}$$

Also, using (5.13)–(5.18), it can be seen that our approximation acts as a truncating operator with the following action

$$V|j\rangle = \frac{1}{2^{n/2}}\bigotimes_{l=1}^{k}\left(|0\rangle + e^{2\pi i j 2^{-l}}|1\rangle\right)\otimes\left(|0\rangle + e^{2\pi i 0.j_{n-k}\cdots j_{n-1}}|1\rangle\right)\otimes\cdots\otimes\left(|0\rangle + e^{2\pi i 0.j_1\cdots j_k}|1\rangle\right)$$

$$= \frac{1}{2^{k/2}}\bigotimes_{l=1}^{k}\left(|0\rangle + e^{2\pi i j 2^{-l}}|1\rangle\right)\otimes|\nu_k\rangle\otimes\cdots\otimes|\nu_{n-1}\rangle$$

where

$$|\nu_m\rangle = \left(|0\rangle + e^{2\pi i 0.j_{n-m}\cdots j_{n-m+k-1}}|1\rangle\right)/\sqrt{2}$$

Therefore, defining the error vector

$$|\psi_j\rangle = (U - V)|j\rangle$$

we have

$$\begin{aligned}\|(U-V)|j\rangle\|^2 &= \langle\psi_j|\psi_j\rangle \\ &= \prod_{m=k}^{n-1}\langle\phi_m|\phi_m\rangle + \prod_{m=k}^{n-1}\langle\nu_m|\nu_m\rangle - 2\,\mathrm{Re}\prod_{m=k}^{n-1}\langle\nu_m|\phi_m\rangle\end{aligned}$$

but

$$\langle\nu_m|\phi_m\rangle = (1+\exp(2\pi i 0.00\cdots 0 j_{n-m+k}\cdots j_n))/2$$

where there are k zeros in the above exponent. This term has a very small phase for large n, and therefore

$$\begin{aligned}\mathrm{Re}\langle\nu_m|\phi_m\rangle &\geq \mathrm{Re}(1+\exp(2\pi i/n^c))/2 \\ &\approx \left|1+e^{2\pi i/n^c}\right|/2 \quad \text{for } n \text{ large} \\ &= \cos(\pi/n^c) \\ &\simeq (1-\pi^2/n^{2c})\end{aligned}$$

For the product term, the phase of each argument is on the order of π/n^c, therefore for $c \geq 2$, the phase of the product $\prod_{m=k}^{n-1}\langle\nu_m|\phi_m\rangle$ is less than π/n, and we can again approximate the real part by its magnitude to obtain:

$$\begin{aligned}\|(U-V)|j\rangle\|^2 &\approx 2-2(1-\pi^2/n^{2c})^{n-k} \\ &\approx 2[1-(1-(n-k)\pi^2/n^{2c}] \\ &\approx 2\pi^2/n^{2c-1}\end{aligned}$$

which means that the error decreases inversely proportional to $n^{c-1/2}$.

Problem 2. Problem 5.6 in Nielsen and Chuang. Show how to do addition using Fourier transform and phase shift.

Solution:

From Problem Set 5, Problem 3, for $N = 2^n$, we have

$$U_N^\dagger R_N U_N = T_N$$

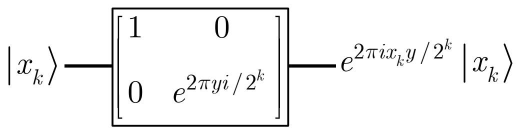
where

$$T_N = \sum_{x=0}^{N-1}|x+1 \bmod N\rangle\langle x|$$

is the addition operator for $y = 1$, and therefore

$$(T_N)^y = U_N^\dagger R_N U_N U_N^\dagger R_N U_N \cdots U_N^\dagger R_N U_N = U_N^\dagger (R_N)^y U_N$$

is the addition operator for any y. U_N performs the quantum Fourier transform on *n* qubits, and $(R_N)^y = \sum_{x=0}^{N-1} \exp(2\pi xyi/N)|x\rangle\langle x|$ can be constructed using *n* single-qubit phase shifts, one for each input qubit. The circuit for the *k*th qubit is as follows:



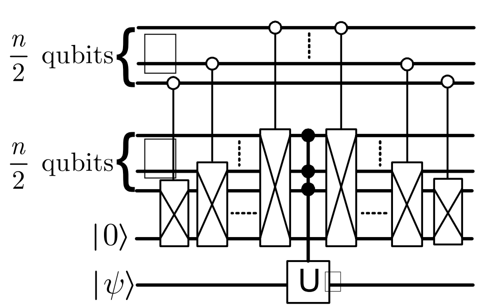
which takes $|x\rangle = |x_1\rangle \cdots |x_n\rangle$, for $x = x_1 2^{n-1} + x_2 2^{n-2} + \cdots + x_n 2^0$, to $\exp(2\pi xyi/N)|x\rangle$ as desired. So in order to construct $(T_N)^y = U_N^\dagger (R_N)^y U_N$, we need $2(n^2/2 + 2n)$ operations for QFT and its inverse, and *n* operations for the phase shift, which results in $n^2 + 5n$ operations.

Problem 3. In the Grover's algorithm, what is the probability of success after only one iteration if we are using two qubits (there are 4 possibilities) and there is only one right answer to the search problem. For the two-qubit system, the Grover's algorithm starts with $|\psi\rangle = |+\rangle \otimes |+\rangle$, and, in each iteration, we perform $(2|\psi\rangle\langle\psi| - I)O$, where O is the oracle operator that takes the right answer $|y\rangle$ to $-|y\rangle$ and leaves other states unchanged. The final measurement is in the computational basis.

Solution:

Each iteration of the Grover's algorithm rotates $|\psi\rangle$ by 2θ, where $\theta = \sin^{-1}(\sqrt{M/N}) = \sin^{-1}(\sqrt{1/4}) = \pi/6$, in the subspace spanned by the right answer vector and the superposition of wrong answer vectors. Because the initial phase of $|\psi\rangle$ in this plane is given by θ, after one iteration this angle becomes $\theta + 2\theta = \pi/2$, which is exactly what the right answer represents. Hence, we get the right answer with probability one.

Problem 4. For $n = 2^k$, we can use the following circuit, recursively, to build an *n*-qubit-controlled *U* gate using only single-qubit-controlled *U* gates and Fredkin gates with reverse polarity. Explain how this circuit works, and find how many gates and work bits will be needed to construct the controlled *U* gate.



where the Fredkin gate with reverse polarity swaps the two input states if the control qubit is $|0\rangle$ and does nothing if it is $|1\rangle$.

Solution:

Let's refer to the first n/2 input qubits by the first register, and use the second register for the second half. Then, in order to prove that the above circuit acts the same as an n-qubit-controlled gate, we need to show that the above circuit does nothing unless all input qubits are $|1\rangle$. We consider the following cases:

1- If any of the qubits in the first register is $|0\rangle$, then one of the Fredkin gates becomes active and swaps the work bit $|0\rangle$ and one of the input qubits in the second register. Therefore, one of the control qubits of the n/2-qubit-controlled gate will be $|0\rangle$, and the whole circuit does nothing.
2- If all of all the qubits in the first register are $|1\rangle$, then none of the Fredkin gates is active, and therefore, if any of the qubits in the second register is $|0\rangle$, the n/2-qubit-controlled gate does nothing, and so does the whole circuit.
3- If all input qubits are $|1\rangle$, then none of the Fredkin gates is active, and we have all $|1\rangle$ at the input of the n/2-qubit-controlled gate. Hence, the whole circuit behaves as an n-qubit-controlled gate.

Now that we know the given circuit is an n-qubit-controlled gate, we can use it again to construct the n/2-qubit-controlled gate using a single n/4-qubit-controlled gate, n/2 Fredkin gates, and one work qubit. We can continue this procedure until we get to a circuit with only one single-qubit-controlled gate. This circuit consists of $n + n/2 + \cdots + 2 = 2n - 2$ Fredkin gates, one single-qubit-controlled gate, and $k = \log n$ work qubits.