Quantum Computing: An Applied Approach

Chapter 8 Problems: Building a Quantum Computer

1

The circuit model can be defined as the union of three distinct components: (1) a set of n initialized input qubits, (2) a set of qubit lines consisting of one- or multi-qubit unitary gate operations, and (3) a set of up to n observables to measure that project the qubit states onto the subspace spanned by n classical bits.

The query model, on the other hand, describes some function that maps n input qubits onto n output qubits via the action of some oracle. In this sense, it consists of an input state $\{|x_i\rangle\}_{i=1}^{n}$ and a corresponding collection of classical bits $\{c_i\}_{i=1}^{n}$.

2

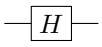
This proof appears relatively elementary. The query complexity involves up to a single oracle call on each of the n input qubits. The circuit, or gate, complexity involves an unbounded number of operations on each of n qubit lines. The query model complexity then represents a lower bound on the circuit complexity, as the circuit complexity involves at least $O(1)$ unitary operations on each qubit.

3

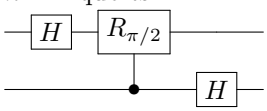
There is a single single-qubit gate per line in the quantum Fourier transform (QFT), so there are n single-qubit gates. The second part of the question clearly means to ask how many double-qubit gates are needed; there are $i-1$ double-qubit gates on the i^{th} line yielding $\sum_{i=1}^{n-1} i = \boxed{\frac{n^2-n}{2}}$ gates overall.

4

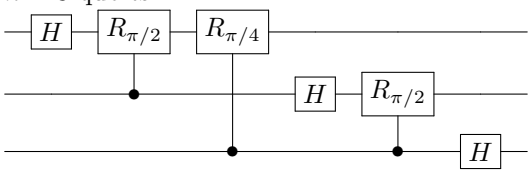
$n = 1$ qubits:



$n = 2$ qubits:



$n = 3$ qubits:



5

The intuition behind this proof is that, when initialized in the zero-state $|0\rangle^{\otimes n}$, all of the controlled-rotation gates reduce to the identity. Consequently, the QFT reduces to a set of one Hadamard operation per line yielding:

$$QFT_n|0\rangle^{\otimes n} = H^{\otimes n}|0\rangle^{\otimes n}$$

as described.

6

6.1

The approach of period finding proposed in this paper by Ekera and Hastad addresses the modular exponentation step and offers several different proposals for reducing the complexity of this step. Overall, especially for low-bit (n) inputs, their approach greatly reduces the number of Toffoli gates required and in doing so, lowers the overall number of qubits required to solve problems such as 2048-bit RSA encryption.

6.2

In terms of the complexity of the modular exponentiation step, Shor's Algorithm involves a Toffoli gate count of $20n_e n^2$, where n_e is the number of modular multiplication operations to perform and n is the number of input bits in the integer to be factored. This step dominates the complexity of Shor's Algorithm as a whole.

6.3

The square-and-multiply approach begins with an initial register qubit x in the state $|1\rangle$. Afterwards, a controlled modular multiplication is run for each exponent qubit e_j, with j iterating from 0 to $n_e - 1$. After this process, including multiple iterations of the modular multiplication subprocess, the initial qubit x stores the exponentiated value $x = g^e$.

6.4

Windowed arithmetic scales down the number of qubits needed for operations in intermediate steps, by replacing subprocesses such as modular multiplication with lookup functions that operate in clusters. In the example shown, a window size of 4 is used to lookup classically known values for the expression $g^{e[4n:4(n+1)]2^{4n}}$, reducing computation time by a factor of 4.

In this paper, this technique is used in both the modular addition and modular multiplication subroutines, modifying the Toffoli gate count from $4n^2 n_e$ to $\frac{2n_e n}{c_{\text{mul}} c_{\text{exp}}}(2n + 2^{c_{\text{mul}}+c_{\text{exp}}})$. A tradeoff takes place, as the scalar decrease in the gate counts with the window sizes c is balanced by the number of Toffoli gates involved in the lookup operation (factor of $2^{c_{\text{mul}}+c_{\text{exp}}}$).

6.5

These implications are explored in Table 1. Although the complexity of the approach studied in this paper is asymptotically greater than the others, for small values of n it reaches a practical baseline for gate complexity in solving 2048-bit RSA decryption around two orders of magnitude lower than the next best.

Specifically, the minimum number of abstract qubits necessary to factor a 2048-bit key has been reduced from 340 in Fowler et al. (2012) to 2.7.

7

Under the approximate QFT, there are at most m two-qubit gates per line, and there are n lines in total. There is also one single-qubit gate per line, yielding a gate complexity of $O(nm + n) = O(nm)$.

In determining the total number of gates exactly, first notice that the number of single-qubit gates remains the same at n. The number of double-qubit gates continues to increase by 1 per line beginning at 0, but stops at m since there are at most m rotations θ_{jk} where $j - k > m$.

There are then $\frac{m(m-1)}{2}$ double-qubit gates in the first m lines, and $(n-m)m$ in the remaining $n - m$. Overall, including the n single-qubit gates this yields

$$\frac{m^2 - m}{2} + \frac{2m(n-m)}{2} = \boxed{\frac{m(2n - m + 1)}{2}}$$

gates.

Since $n > m$ is assumed, this expression has complexity $O(mn)$ as described. It disagrees with the expression listed in the problem set assignment, but matches my own calculations for various values of m and n.

For example, setting $m = 2$ and $n = 5$ for the AQFT yields a quantum circuit with 5 single-qubit gates and 0+1+2+2+2=9 two-qubit gates. Assigning these values into the expression above, this yields $5 + \frac{2(2 \cdot 5 - 2 + 1)}{2} = 5 + 9 = 14$ gates, as expected.