CO 781/QIC 823/CS 867 Assignment 1

Your completed assignment should include an acknowledgment of any sources (research papers, textbooks, etc) consulted. The assignment must be submitted by Thursday, June 15 at 9pm.

Problem 1 (Errors in the output distribution)**.** Suppose we are given an n-qubit quantum circuit U which is a product of m gates each acting non-trivially on at most 2 qubits. Consider the quantum computation in which U is applied to the all-zeros initial state and then the first w qubits are measured. The output is a bit-string $x \in \{0,1\}^w$ sampled according to the distribution

$$p(x) = \langle 0^n | U^\dagger \left(|x\rangle\langle x| \otimes I_{n-w} \right) U |0^n\rangle.$$

Suppose we approximate the given circuit using a different gate set, via the Solovay-Kitaev theorem. Let $\tilde{p}$ be the corresponding output probability distribution and suppose we aim to guarantee that the total variation distance between p and $\tilde{p}$ is at most ϵ, i.e., $(1/2)\sum_x |p(x) - \tilde{p}(x)| \leq \epsilon$. Establish an asympotic upper bound on the number of elementary gates in the new circuit that is independent of w.

Problem 2 (Small angle rotations in the Quantum Fourier Transform)**.** Provide a solution to Exercise 5.6 from Nielsen and Chuang (you may replace $\Theta(\cdot)$ with $O(\cdot)$ in the statement of the problem)

Problem 3 (Hybrid lower bound for search)**.** Read Section 9.3 of the KLM textbook [4].

(i) Fill in the details of the proof of Theorem 9.3.2. That is, provide a complete proof that: given oracle access to a function $f : \{0,1\}^n \to \{0,1\}$, a quantum computer needs at least $\Omega(2^{n/2})$ queries to f in order to decide between the following two cases (a) $f(x) = 0$ for all x or (b) there is a unique bit string x such that $f(x) = 1$.

(ii) Suppose we are given oracle access to a function $f : \{0,1\}^n \to \{0,1\}$ and we are promised that there is a unique bit string x such that $f(x) = 1$. Show that a quantum algorithm that outputs x with high probability must use at least $\Omega(2^{n/2})$ queries to f.

Problem 4 (Lower bound for phase estimation)**.** Let U be a unitary and ϕ be a quantum state such that $U|\phi\rangle = e^{2\pi i\theta}|\phi\rangle$ for some phase $\theta \in (0, 1)$. Suppose we are given a black-box which performs a controlled-U operation

$$CU = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$$

where the first register is a single qubit.

(i) Explain how the quantum phase estimation algorithm provides an approximation to the phase with n bits of precision (and some small constant failure probability) using $O(2^n)$ uses of CU.

(ii) Establish a matching lower bound $\Omega(2^n)$ on the number of uses of CU. Hint: you may use the lower bound established in the previous problem.

Problem 5 (Linear combinations of unitaries)**.** A quantum computer natively performs quantum circuits, which are expressed as products of elementary unitary gates. However—with some additional cost— it is also possible to perform sums or linear combinations of unitaries and this functionality has been exploited in some recent algorithmic advances (see for example Refs. [3, 1, 2]). In this problem you will see how this works. Suppose $V_1, \ldots, V_m$ are n-qubit unitaries and we have quantum circuits that implement each of them.

(i) Consider an n-qubit register and a $\lceil \log(m) \rceil$-qubit register, with computational basis states labeled as

$$\{|z\rangle|j\rangle : z \in \{0, 1\}^n, j = 1, 2, \ldots, m\}.$$

Define a unitary

$$SV = \sum_{j=1}^{m} V_j \otimes |j\rangle\langle j|.$$

Describe how to implement SV using the quantum circuits which implement $V_1, V_2, \ldots, V_m$.

(ii) Describe a subroutine that prepares the state $\frac{1}{\sqrt{m}} \sum_j V_j|0^n\rangle|j\rangle$.

(iii) Describe an algorithm which uses the subroutine $O(m/\| \sum_j V_j|0^n\rangle\|)$ times and outputs a state proportional to

$$\sum_j V_j|0^n\rangle.$$

(iv) Describe a generalization of the above algorithm which prepares a state $\sum_j \beta_j V_j |0^n\rangle$ for some given complex coefficients β_j and give an upper bound on the number of uses of SV required.

Problem 6 (Meaning of the HSP)**.** In what sense does the literature on the Hidden Subgroup Problem provide evidence that quantum computers are more powerful than classical ones? Provide a summary consisting of at least one paragraph and at most 1/2 page.

Problem 7 (Hidden shift problem)**.** Suppose $f : \{0,1\}^n \to \{0,1\}$ is a known function (in the following setting where we are counting queries to g, this means we can compute it at zero cost) and we are given oracle access to another function $g : \{0,1\}^n \to \{0,1\}$ with the promise that there exists a secret string $s \in \{0,1\}^n$ such that $f(x) = g(x \oplus s)$ for all $x \in \{0,1\}^n$.

(i) Establish a lower bound on the number of queries to g that are needed for a quantum computer to output s (with high probability, say)?

(ii) Consider the very special case where f is a *bent function* [5]. That is, the Fourier transform of f (over $\mathbb{Z}_2^n$) is also a boolean function:

$$\frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} (-1)^{x \cdot z + f(z)} \in \{+1, -1\} \qquad \text{for all } x \in \{0,1\}^n$$

Describe a quantum algorithm that outputs s deterministically using only one query to g.

References

[1] Dominic W Berry, Andrew M Childs, Richard Cleve, Robin Kothari, and Rolando D Somma. Simulating hamiltonian dynamics with a truncated taylor series. *Physical review letters*, 114(9):090502, 2015.

[2] Andrew M Childs, Robin Kothari, and Rolando D Somma. Quantum algorithm for systems of linear equations with exponentially improved dependence on precision. *SIAM Journal on Computing*, 46(6):1920–1950, 2017.

[3] Andrew M Childs and Nathan Wiebe. Hamiltonian simulation using linear combinations of unitary operations. *arXiv preprint arXiv:1202.5822*, 2012.

[4] Phillip Kaye, Raymond Laflamme, Michele Mosca, et al. *An introduction to quantum computing*. Oxford University Press, 2007.

[5] Martin Rötteler. Quantum algorithms for highly non-linear boolean functions. In *Proceedings of the twenty-first annual ACM-SIAM symposium on Discrete algorithms*, pages 448–457. SIAM, 2010.