Quantum Computing Exercise Sheet

August 2 & 4, 2022

Most exercises come from Ronald de Wolf's lecture notes [dW19, Chapters 1, 4&5]. Feel free to skip exercises that you find too easy or hard. On the last page you can find some hints where indicated by (**H**).

Exercises

1.) Compute and write down in both Dirac (bra-ket) and vector notation the following:

(a) $(H|0\rangle) \otimes (H|1\rangle)$

(b) $H \otimes H$

(c) $(H \otimes H)|01\rangle$

2.) Show that surrounding a CNOT gate with Hadamard gates switches the role of the control-bit and target-bit of the CNOT: $(H \otimes H)\text{CNOT}(H \otimes H)$ is the 2-qubit gate where the second bit controls whether the first bit is negated (i.e., flipped).

3.) Prove that an EPR-pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is an *entangled* state, i.e., it cannot be written as the tensor product of two separate qubits.

4.) (**H**) Prove the *quantum no-cloning theorem*: there does not exist a 2-qubit unitary U that maps

$$|\phi\rangle|0\rangle \mapsto |\phi\rangle|\phi\rangle$$

for every qubit $|\phi\rangle$.

5.) (Quantum teleportation [BBC$^+$93] – [dW19, Chapter 1.5]) Suppose there are two parties, Alice and Bob. Alice has a qubit $\alpha_0|0\rangle + \alpha_1|1\rangle$ that she wants to send to Bob via a *classical* channel. Suppose Alice also shares an EPR-pair

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

with Bob (say Alice holds the first qubit and Bob the second). Initially, their joint state is

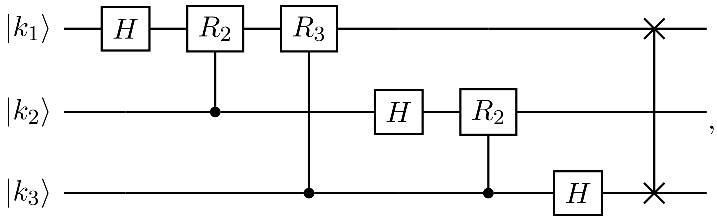
$$(\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

(a) What is their joint state if Alice performs a CNOT on her two qubits and then a Hadamard transform on her first qubit.

(b) Suppose Alice measures her qubits and sends the results to Bob. Show that Bob can reconstruct the original state of Alice using these two bits of information by applying an X and / or Z gate on his qubit depending on the bit values.

6.) For $\omega = e^{2\pi i/3}$ and $F_3 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$, calculate $F_3\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ and $F_3\begin{pmatrix} 1 \\ \omega^2 \\ \omega \end{pmatrix}$

7.) (**H**) Show that the following circuit implements the quantum Fourier transform F_8:



, where $R_s = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^s} \end{pmatrix}$. Can you generalize the construction to F_{2^n}?

8.) This exercise is about efficient classical implementation of modular exponentiation.

(a) (**H**) Given n-bit numbers x and N, compute the whole sequence x^0 mod N, x^1 mod N, x^2 mod N, x^4 mod N, x^8 mod N, x^{16} mod $N, \ldots, x^{2^{n-1}}$ mod N, using $O(n^2 \log(n))$ steps.

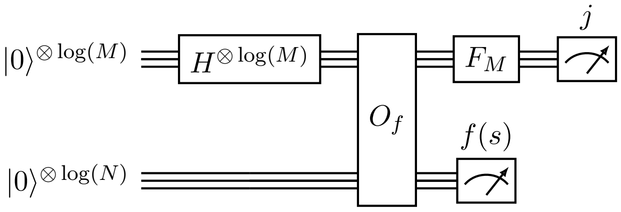
(b) Suppose n-bit number a can be written as $a = a_{n-1} \ldots a_1 a_0$ in binary. Express x^a mod N as a product of the numbers computed in part (a).

(c) Show that you can compute $f(a) = x^a$ mod N in $O(n^2 \log(n))$ steps.

9.) Consider the function $f(a) = 7^a$ mod 10.

(a) What is the period r of f?

(b) Show how Shor's algorithm finds the period of f, using a Fourier transform over $M = 128$ elements.



Write down all intermediate superpositions of the algorithm for this case (don't just copy the general expressions, but instantiate them with actual numbers as much as possible, incl. with the value of the period found in (a)). You may assume you're lucky, meaning the first run of the algorithm already gives a measurement outcome $j = cM/r$ with c coprime to r.

10.) (**H**) Show that computing the discrete logarithm over a cyclic group $C = \{\gamma^n \colon n \in [N]\}$ of size N can be reduced to the Hidden Subgroup Problem. That is, for any $A \in C$ give an efficiently computable function f from some group G such that the subgroup $H \leq G$ on whose cosets f is constant reveals the value $n \in [N]$ such that $\gamma^n = A$.

11.) Show that if the number of solutions is $t = N/4$, then Grover's algorithm always finds a solution with certainty after just one Grover step. How many queries would a classical algorithm need to find a solution with certainty if $t = N/4$? And if we allow the classical algorithm error probability say $1/3$?

12.) Suppose we have a database with $N = 2^n$ binary slots, containing t ones (solutions) and $N - t$ zeroes. You may assume you know the number t.

(a) Show that we can use Grover's algorithm to find the positions of *all* t ones, using an expected number of $O(t\sqrt{N})$ queries to the database. You can argue on a high level, no need to draw actual quantum circuits.

(b) (**H**) Show that this can be improved to an expected number of $O(\sqrt{tN})$ queries.

13.) (Marriott-Watrous rewinding) Suppose you can perform binary projective measurements according to the projectors $(\Pi, I - \Pi)$ and $(|\psi\rangle\langle\psi|, I - |\psi\rangle\langle\psi|)$. Suppose that initially you hold $|\psi\rangle$.

(a) If you first measure $(\Pi, I - \Pi)$, what are the possible post-measurement states?

(b) Then, if you measure $(|\psi\rangle\langle\psi|, I - |\psi\rangle\langle\psi|)$, what are the possible post-measurement states?

(c) If you once again measure $(\Pi, I - \Pi)$, what are the possible post-measurement states?

(d) Suppose that you continue alternating the measurements until you get back to the original state $|\psi\rangle$. What is the expected number of measurements that you need to perform?

(e) (**H**) Show that a similar result holds when we replace the binary measurement $(|\psi\rangle\langle\psi|, I - |\psi\rangle\langle\psi|)$ by $(\widetilde{\Pi}, I - \widetilde{\Pi})$ such that $\widetilde{\Pi}|\psi\rangle = |\psi\rangle$, and we only ask that we get back to a state $|\phi\rangle$ such that $\widetilde{\Pi}|\phi\rangle = |\phi\rangle$.

Hints

Exercise 4: Consider what U has to do when $|\phi\rangle = |0\rangle$, when $|\phi\rangle = |1\rangle$, and when $|\phi\rangle$ is a superposition of these two.

Exercise 7: Observe that the quantum Fourier transformation maps computational basis states to product states:

$$\begin{aligned} F_8 \colon |k_1k_2k_3\rangle \mapsto & \frac{1}{\sqrt{8}}\sum_{j=0}^{7} e^{2\pi i \frac{j\cdot k}{8}}|j\rangle \\ & = \frac{1}{\sqrt{2}}\Big(|0\rangle + e^{2\pi i\cdot 0.k_3}|1\rangle\Big) \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle + e^{2\pi i\cdot 0.k_2k_3}|1\rangle\Big) \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle + e^{2\pi i\cdot 0.k_1k_2k_3}|1\rangle\Big) \end{aligned}$$

Exercise 8: You may invoke here (without proof) the algorithm of Harvey and van der Hoeven for fast multiplication [HvdH21], allowing the multiplication of two n-bit integers mod N using $O(n\log(n))$ steps (where $n = \lceil \log_2 N \rceil$). This is a relatively recent improvement over the better known Schönhage-Strassen algorithm [SS71, Knu97] which uses $O(n\log(n)\log\log(n))$ steps.

Exercise 10: Take $G := \mathbb{Z}_N \times \mathbb{Z}_N$ and define $f(x,y) := \gamma^x A^{-y}$.

Exercise 12: Recall that if there are i solutions, then one variant of Grover's algorithm finds a solution using an expected number of $O(\sqrt{N/i})$ queries.

Exercise 13: Consider the singular value decomposition of $\Pi\cdot\widetilde{\Pi}$, and show that the decomposition corresponds to a set of mutually orthogonal two (or one) dimensional invariant subspaces that are invariant under both reflections. (This result is known as Jordan's lemma.) Then decompose $|\psi\rangle$ according to the right singular vectors.

References

[BBC$^+$93] C. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70:1895–1899, 1993.

[HvdH21] David Harvey and Joris van der Hoeven. Integer multiplication in time $O(n\log n)$. *Annals of Mathematics*, 193(2):563 – 617, 2021.

[Knu97] Donald E. Knuth. *The Art of Computer Programming, Volume 2 (3rd Ed.): Seminumerical Algorithms.* Addison-Wesley Longman Publishing Co., Inc., 1997.

[SS71] A. Schönhage and V. Strassen. Schnelle multiplikation großer zahlen. *Computing*, 7:281–292, 1971.

[dW19] Ronald de Wolf. Quantum computing: Lecture notes (version 4), 2019. arXiv: `1907.09415v4`