Quantum Computing Exercise Sheet 1

August 2, 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

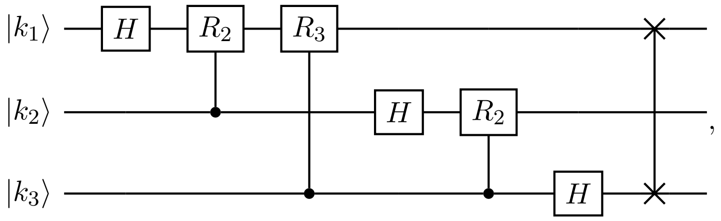
$$(\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

(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.) 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 $N, \dots, x^{2^{n-1}}$ mod N, using $O(n^2 \log(n) \log\log(n))$ steps.

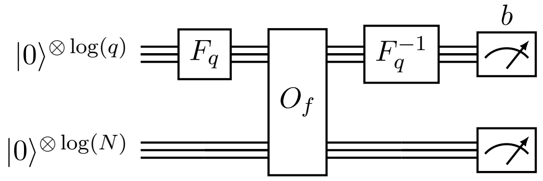
(b) Suppose n-bit number a can be written as $a = a_{n-1} \dots a_1 a_0$ in binary. Express x^a mod N as a product of the numbers computed in part (a).

(c) Show that you can compute $f(a) = x^a$ mod N in $O(n^2 \log(n) \log\log(n))$ 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 $q = 128$ 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 $b = cq/r$ with c coprime to r.

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 8: You may invoke here (without proof) the Schönhage-Strassen algorithm for fast multiplication [SS71, Knu97]. This allows you to multiply two n-bit integers mod N using $O(n \log(n) \log\log(n))$ steps (where $n = \lceil \log_2 N \rceil$).[*]

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, 2019. arXiv: `1907.09415`

[*] Shor used Schönhage-Strassen in his original paper. We could also invoke the more recent improvement of Harvey and van der Hoeven [HvdH21], who remove the $\log\log n$ factor.