Exercises

10.1. $|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ is one of the famous "Bell states," a highly entangled state of its two qubits. In this question we examine some of its strange properties.

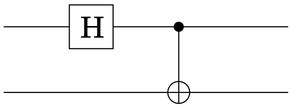
(a) Suppose this Bell state could be decomposed as the (tensor) product of two qubits (recall the box on page 314), the first in state $\alpha_0|0\rangle + \alpha_1|1\rangle$ and the second in state $\beta_0|0\rangle + \beta_1|1\rangle$. Write four equations that the amplitudes α_0, α_1, β_0, and β_1 must satisfy. Conclude that the Bell state cannot be so decomposed.

(b) What is the result of measuring the first qubit of $|\psi\rangle$?

(c) What is the result of measuring the second qubit after measuring the first qubit?

(d) If the two qubits in state $|\psi\rangle$ are very far from each other, can you see why the answer to (c) is surprising?

10.2. Show that the following quantum circuit prepares the Bell state $|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ on input $|00\rangle$: apply a Hadamard gate to the first qubit followed by a CNOT with the first qubit as the control and the second qubit as the target.



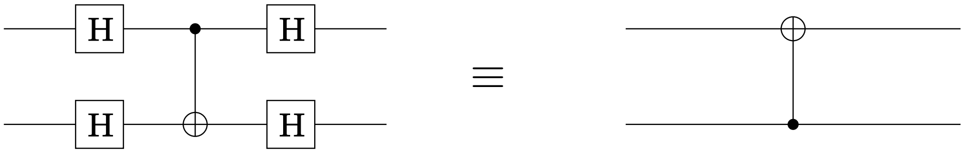
What does the circuit output on input 10, 01, and 11? These are the rest of the Bell basis states.

10.3. What is the quantum Fourier transform modulo M of the uniform superposition $\frac{1}{\sqrt{M}}\sum_{j=0}^{M-1}|j\rangle$?

10.4. What is the QFT modulo M of $|j\rangle$?

10.5. *Convolution-Multiplication.* Suppose we shift a superposition $|\alpha\rangle = \sum_j \alpha_j|j\rangle$ by l to get the superposition $|\alpha'\rangle = \sum_j \alpha_j|j+l\rangle$. If the QFT of $|\alpha\rangle$ is $|\beta\rangle$, show that the QFT of α' is β', where $\beta'_j = \beta_j\omega^{lj}$. Conclude that if $|\alpha'\rangle = \sum_{j=0}^{M/k-1}\sqrt{\frac{k}{M}}\,|jk+l\rangle$, then $|\beta'\rangle = \frac{1}{\sqrt{k}}\sum_{j=0}^{k-1}\omega^{ljM/k}|jM/k\rangle$.

10.6. Show that if you apply the Hadamard gate to the inputs and outputs of a CNOT gate, the result is a CNOT gate with control and target qubits switched:



10.7. The CONTROLLED SWAP (C-SWAP) gate takes as input 3 qubits and swaps the second and third if and only if the first qubit is a 1.

(a) Show that each of the NOT, CNOT, and C-SWAP gates are their own inverses.

(b) Show how to implement an AND gate using a C-SWAP gate, i.e., what inputs a, b, c would you give to a C-SWAP gate so that one of the outputs is $a \wedge b$?

(c) How would you achieve fanout using just these three gates? That is, on input a and 0, output a and a.

(d) Conclude therefore that for any classical circuit C there is an equivalent quantum circuit Q using just NOT and C-SWAP gates in the following sense: if C outputs y on input x, then Q outputs $|x, y, z\rangle$ on input $|x, 0, 0\rangle$. (Here z is some set of junk bits that are generated during this computation).

(e) Now show that that there is a quantum circuit Q^{-1} that outputs $|x, 0, 0\rangle$ on input $|x, y, z\rangle$.

(f) Show that there is a quantum circuit Q' made up of NOT, CNOT, and C-SWAP gates that outputs $|x, y, 0\rangle$ on input $|x, 0, 0\rangle$.

10.8. In this problem we will show that if $N = pq$ is the product of two odd primes, and if x is chosen uniformly at random between 0 and $N - 1$, such that $\gcd(x, N) = 1$, then with probability at least $3/8$, the order r of $x \bmod N$ is even, and moreover $x^{r/2}$ is a nontrivial square root of $1 \bmod N$.

(a) Let p be an odd prime and let x be a uniformly random number modulo p. Show that the order of $x \bmod p$ is even with probability at least $1/2$. (*Hint:* Use Fermat's little theorem (Section 1.3).)

(b) Use the Chinese remainder theorem (Exercise 1.37) to show that with probability at least $3/4$, the order r of $x \bmod N$ is even.

(c) If r is even, prove that the probability that $x^{r/2} \equiv \pm 1$ is at most $1/2$.