**PHYSICS 150**

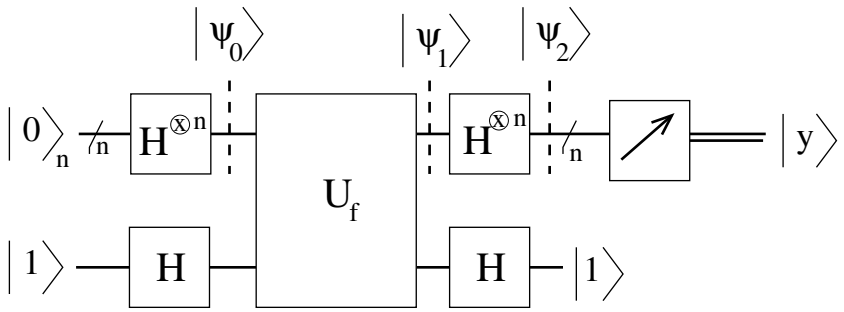
**Homework 4**

To be submitted to Canvas by 11:59 pm, Thursday November 4, 2021

**Midterm:** Recall that the midterm will be in class on Tuesday October 26.
**It will be closed book** but you may use one sheet of notes that you have prepared.
To prepare for the midterm I recommend that, in addition to studying the lecture material, you go over the homework assignments so far (assignments 1–3). For those questions you had difficulty with **study the typed-up worked solutions** available at the class website on Canvas.

1. *The Deutsch-Josza Algorithm*
   This is an extension of the Deutsch algorithm discussed in class. Recall that in Deutsch's algorithm the input is one bit and the output is also one bit. In the Deutsch-Josza algorithm, the output is still one bit but the input has $n$ bits, so there are $2^n$ distinct inputs. We are told that *either* the function is "constant" (in which case the function outputs the same value for all $2^n$ inputs) *or* is "balanced" (in which case an equal number of inputs give the results 1 and 0). Clearly this is a very artificially constructed problem but it will be our first quantum algorithm with more than a one-bit input. Note that it is *precisely* the Deutsch algorithm for $n = 1$.

   The circuit for the Deutsch-Josza is almost identical to that for the Deutsch algorithm except that the upper qubit in the Deutsch algorithm (sometimes called the "input" qubit) is replaced by a $n$-qubit register. The circuit is shown in the figure below.




   The function $U_f$ acts as follows on computational basis states $|x\rangle_n$ and $|z\rangle$:

$$U_f|x\rangle_n|z\rangle = |x\rangle_n|z \oplus f(x)\rangle\,, \tag{1}$$

   where $x$ is an $n$-bit integer, $|x\rangle$ is the state of the n-qubit upper register in the figure, $z$ and $f(x)$ are 1-bit integers, and $|z\rangle$ is the lower qubit in the figure.

   As in the Deutsch algorithm, the lower qubit is initialized to $|1\rangle$. In the Deutsch algorithm, the upper qubit is initialized to $|0\rangle$. Here the single qubit is replaced by an $n$-qubit register which, by analogy, is initialized to $|0\rangle_n$.

   (a) Show that

$$|\psi_0\rangle_n = H^{\otimes n}|0\rangle_n = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle_n\,, \tag{2}$$

   so the input to the function $U_f$ is the uniform superposition of all $2^n$ basis states.

(b) Show that after the action of $U_f$ the state of the upper register is

$$|\psi_1\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle_n. \tag{3}$$

The fact that the value of $f(x)$ only changes the overall sign of the state is called the *phase kickback* trick by Vathsan.

(c) Show that after the action of the second set of Hadamards on the $n$-qubit register, the state of that register is

$$|\psi_2\rangle_n = H^{\otimes n} |\psi_1\rangle_n = \frac{1}{2^n} \sum_{x,y=0}^{2^n-1} (-1)^{[f(x)+x\cdot y]} |y\rangle_n, \tag{4}$$

where $x \cdot y$ is the bitwise inner product of $x$ and $y$ with modulo 2 addition:

$$x \cdot y = x_0 y_0 \oplus x_1 y_1 \oplus \ldots \oplus x_{n-1} y_{n-1} \,. \tag{5}$$

(d) The upper register is then measured, and an $n$-bit integer $y$ is obtained. Show that if the function is a constant then $y = 0$ with probability 1. Show also that if the function is balanced then one must get a non-zero value of $y$. Hence the Deutsch-Josza algorithm succeeds with *just one* function call.

(e) How does this compare with a classical approach? The only thing one can do classically is keep computing $f(x)$ for different values of $x$ and seeing if one gets more than one value for the output. If the function is balanced, one would probably get different outputs quite quickly. If the function is constant one would need to evaluate half the inputs (plus 1), i.e. $2^{n-1}+1$, to be 100% sure that the function is not balanced. This is exponentially (in $n$) worse than the quantum algorithm.

However, this is arguably not fair. We may well be content to establish that the function is constant with some high probability[1], a bit less than one. If the function is constant, how many function calls would you need classically to rule out the possibility that it is balanced with a probability of error of no more than (i) $10^{-3}$ and (ii) $10^{-6}$. *Note:* For simplicity, assume that the number of function calls is much less than $2^{n/2}$, the number of values of $x$ which give the same result if the function is balanced.

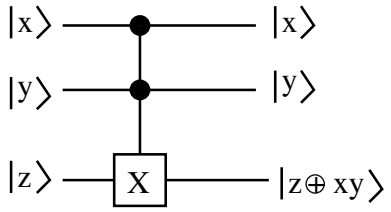
2. Consider the Deutsch-Josza algorithm for $n = 2$, and assume a constant function $f(x) = 0$ for all $x$, i.e. $x = 0, 1, 2, 3$. Compute explicitly the state of the system at each stage and show that you get the state $|y\rangle = |00\rangle$ in the upper register at the end.
*Hint:* Evaluate explicitly Eqs. (2)–(4) for this situation.

3. Consider again the Deutsch-Josza algorithm for $n = 2$ but this time assume that $f(00) = f(01) = 0, f(10) = f(11) = 1$. Show that at least one of the two qubits in the upper register ends up as 1.
*Hint*: See the hint for Qu. 2.

[1]For later quantum algorithms we will only be able to solve the problem with high probability. Since we have to give up 100% certainty in the quantum case, we we should not insist on 100% certainty here from the classical algorithm.

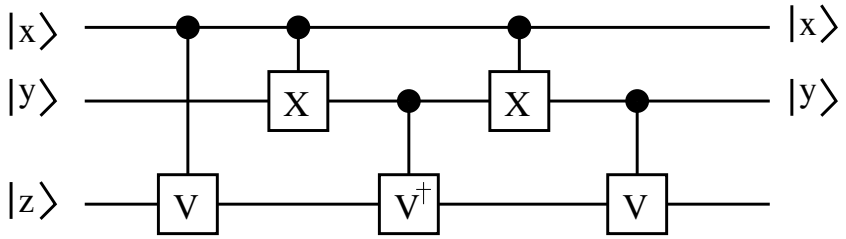
4. *The Toffoli Gate.*
We said in class that that for *classical* reversible computation we need three-bit gates, such as the Toffoli gate, in addition to 1-bit and 2-bit gates, to be able to perform universal computation. However, three qubit gates are, fortunately, not needed in quantum computation because the appropriate three-bit gates can be constructed out of 1-qubit and 2-qubit gates.

Here we consider the quantum Toffoli gate, which is a control-control-NOT (C-C-NOT) gate:




The target qubit $z$ is flipped if both the control qubits, $x$ and $y$, are 1 and is otherwise unchanged.

(a) Consider the following circuit for an arbitrary unitary operator $V$:




Show that it acts with $V^2$ on $|z\rangle$ if both $x$ and $y$ are 1 and otherwise does nothing.
*Hint:* One possible way of approaching this question (though not the only way) is to consider separately what happens for the four possible input values of the control qubits $x$ and $y$, namely 00, 01, 10, and 11.
Another, more elegant, way is to note that the effect of a Ctrl-$V$ gate in which $|z\rangle$ is the target and $|x\rangle$ is the contol is $V\,|x\rangle|z\rangle \longrightarrow |x\rangle V^x|z\rangle$.

(b) Now take $V$ to be the following 1-qubit gate:

$$V = (1-i)\frac{(\mathbb{1} + i\,X)}{2}\,. \tag{6}$$

Show that $V^\dagger V = \mathbb{1}$, and hence $V$ is unitary. Show also that $V^2 = X$ and hence the above circuit is a quantum Toffoli gate.
*Note:* One sometimes says that $V$ is the "square root of $X$".