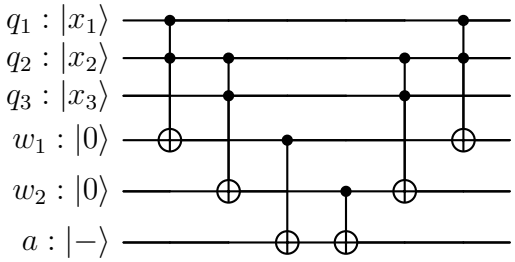
Example problem

Grover's algorithm searches for certain bit strings using a phase oracle

$$O_f\,|x\rangle = (-1)^{f(x)}\,|x\rangle, \tag{1}$$

where $f(x)$ is a Boolean function with $f(x) = 1$ for solution strings and $f(x) = 0$ for all other bit strings. Here we let $x = x_1\,x_2\,x_3$ be a three-bit string. Consider the following implementation of a Grover phase oracle on three query qubits, two work qubits, and one ancilla qubit:

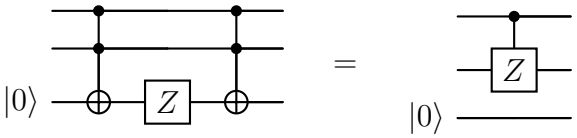


(2)

(a) Determine the Boolean function $f(x_1, x_2, x_3)$ implemented by this oracle, and list the computational-basis states that are solutions. Why is the ancilla qubit initialized in $|-\rangle$ rather than in $|0\rangle$ when this circuit is used as a Grover oracle?

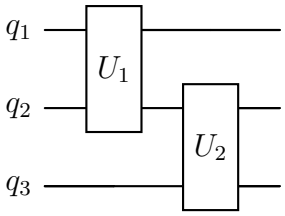
(b) Grover's algorithm proceeds iteratively, where one Grover iteration consists of applying the oracle and a diffusion operator. Describe qualitatively how the probability of measuring a solution state behaves as the number of Grover iterations increases, and explain what this implies for choosing the number of iterations before measuring.

(c) Show that the following circuit identity holds when the bottom qubit is initialized to $|0\rangle$ and the first two qubits are arbitrary:



(3)

(d) Simplify the oracle circuit (2) to a circuit of the form:



(4)

Determine U_1 and U_2. To do this, first analyze how a CNOT acts when its target is $|-\rangle$, and replace each such CNOT by a one-qubit gate on its control. Then use (3) and gate commuting.

(e) Why is the final oracle circuit (4) preferable for real hardware compared with the original circuit (2)? Give at least two reasons.