Grover's Search Algorithm: A quantum algorithm to search through the inputs of function $f(x)$ to check whether the function $f(x)$ returns true for that input x.

Quantum Oracle O: On a quantum computer, we can transform the function into a set of quantum gates contributing for a quantum oracle O, and use Grover's search algorithm to find a correct input with $\sqrt{2^n}$ iterations.

e.g. We need the quantum oracle O to pick out string 10. Then the function that O represents should be:

$$f(x) = \begin{cases} 1, x = 10 \\ 0, x \neq 10 \end{cases}$$

In order to reprent this, we can design the quantum oracle O by:

$$O|x\rangle = (-1)^{f(x)}|x\rangle$$

which will flips the amplitude of the quantum state if x=10, and it can be expressed by the quantum matrix:

$$O = \begin{array}{c c} & \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \begin{array}{c} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} & \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

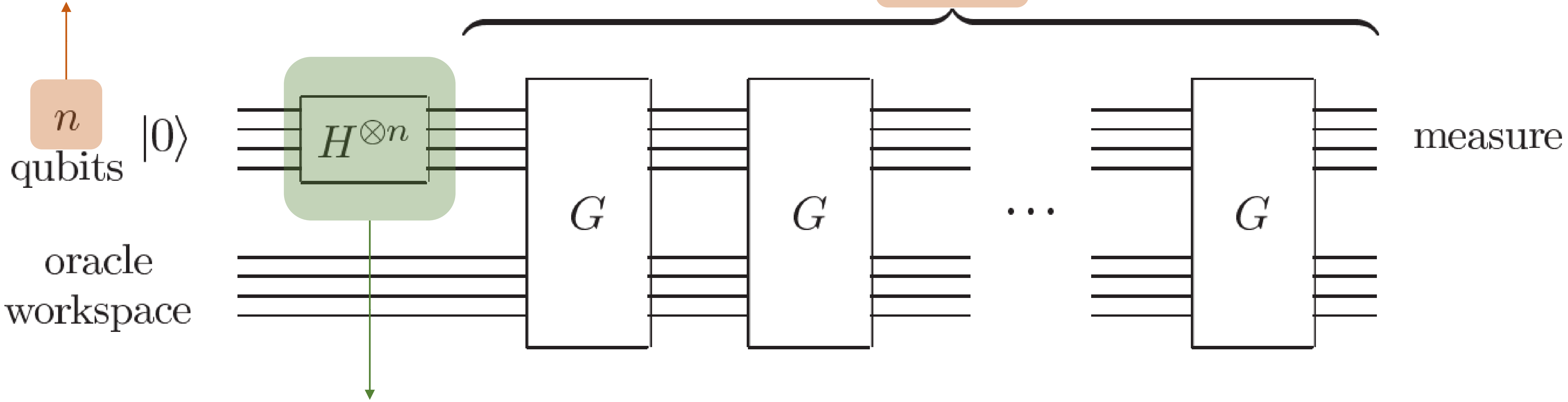
Thus, O is a black-box quantum oracle that is already given to the algorithm.

Procedures of Grover’s Search Algorithm – Step 1. Create input

Number of iterations

$O(\sqrt{N})$

$N = 2^n$ is the number of elements that we search from, which means that the index of those elements are from 0 to N-1.

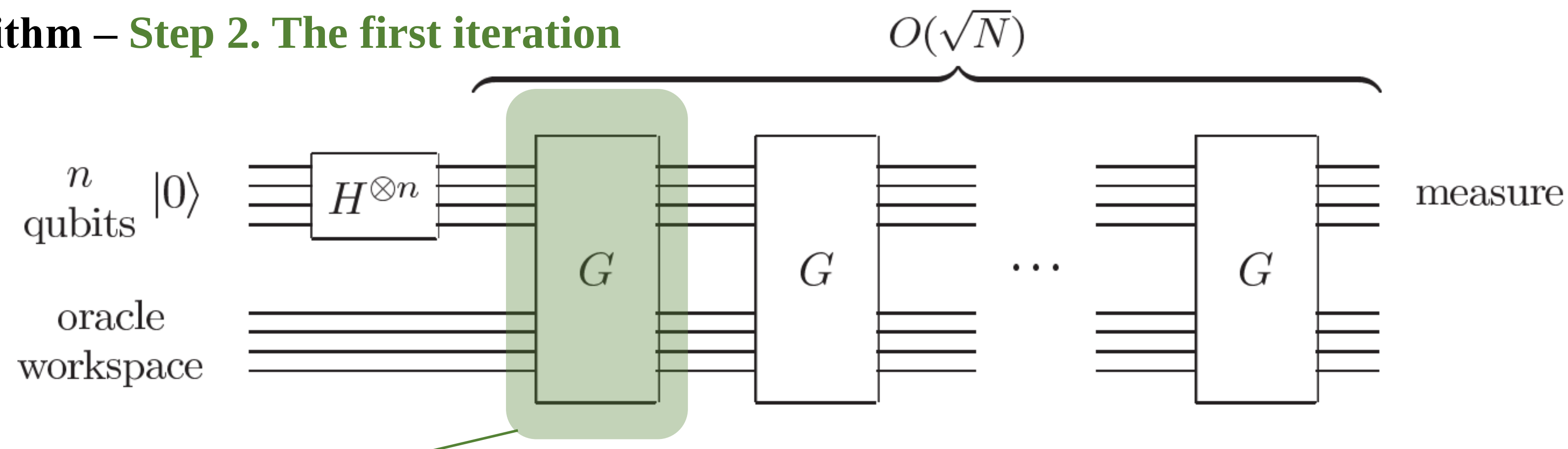


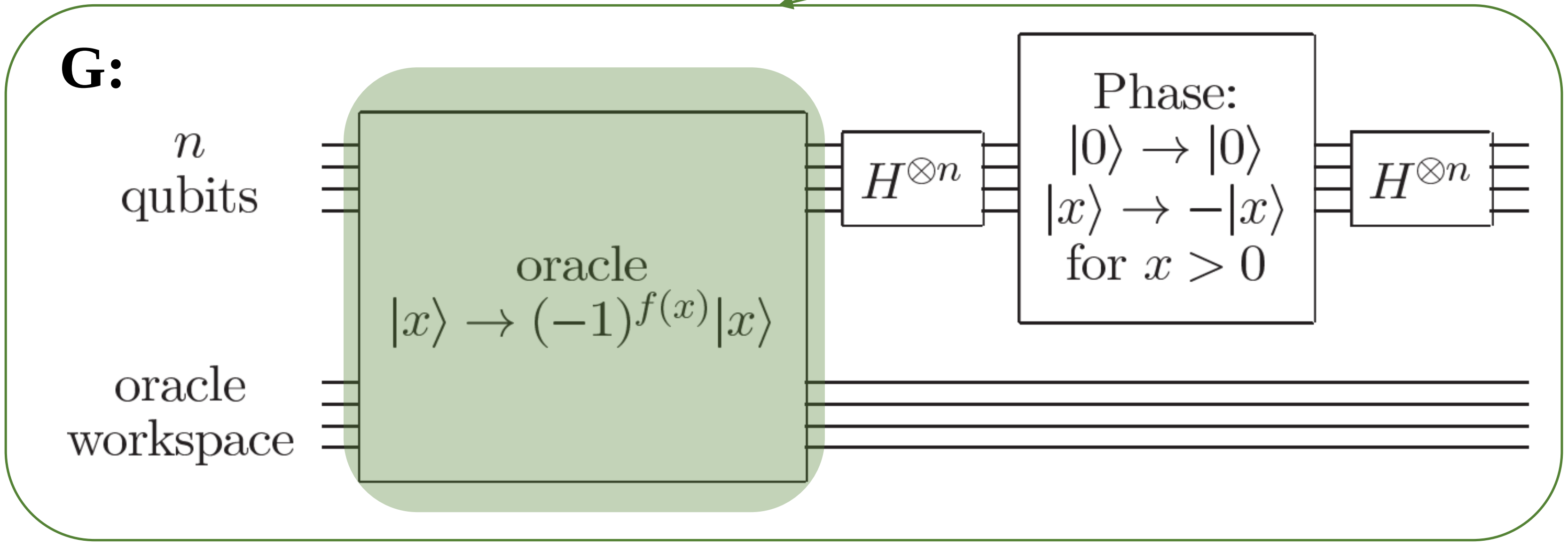
Step 1. Apply the Hadamard transforms, which is to create the possible inputs with equally weighted superposition, $|\psi\rangle = \frac{1}{\sqrt{n}} \sum_{x=0}^{n=1} |x\rangle$.

(e.g. When n=2, the input should be $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$.

Reference & picture: Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

Procedures of Grover's Search Algorithm – **Step 2. The first iteration**

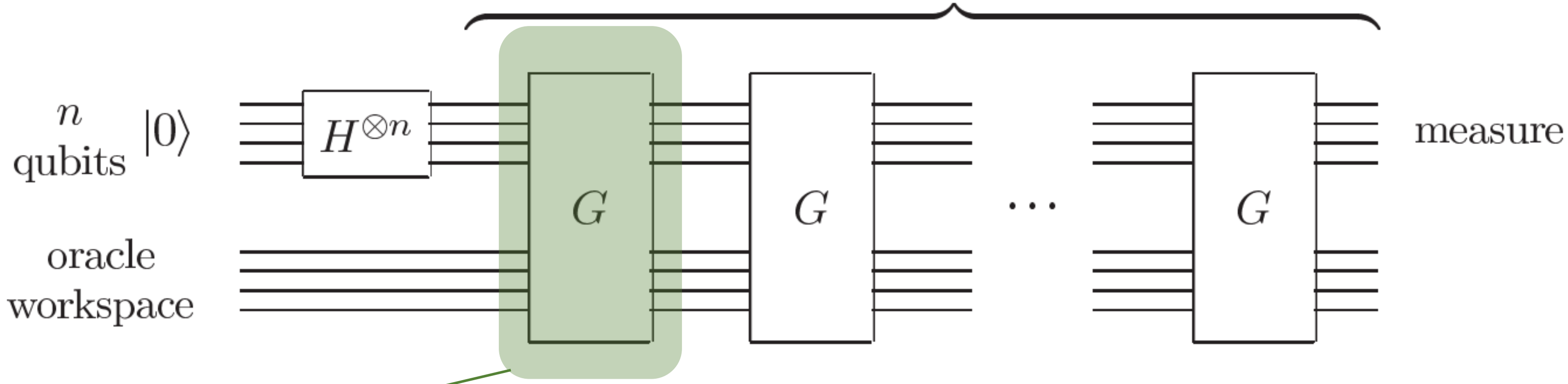


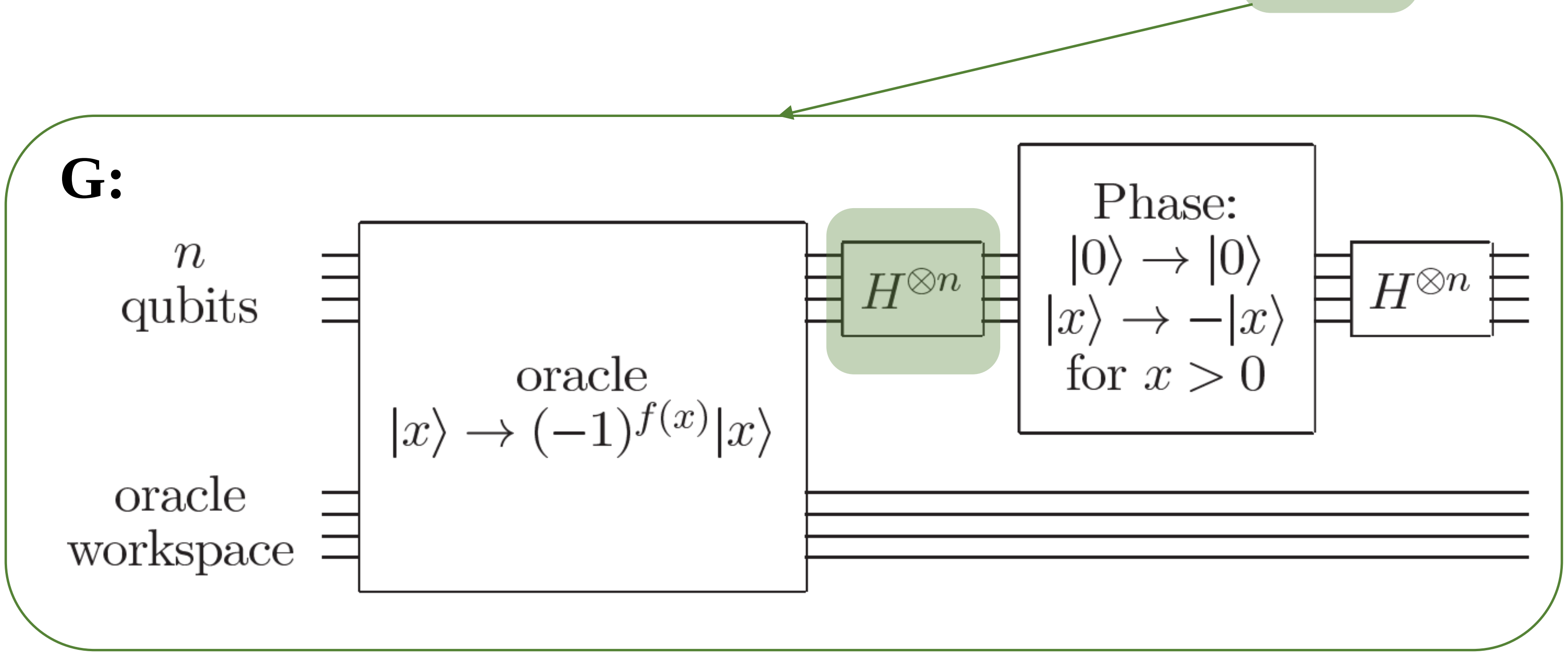


Step 2.1 Apply the quantum oracle O gate to mark the state that satisfies $f(x)$=1. This procedure is detailly decribed in the first slide.

Reference & picture: Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

Procedures of Grover's Search Algorithm – **Step 2. The first iteration**

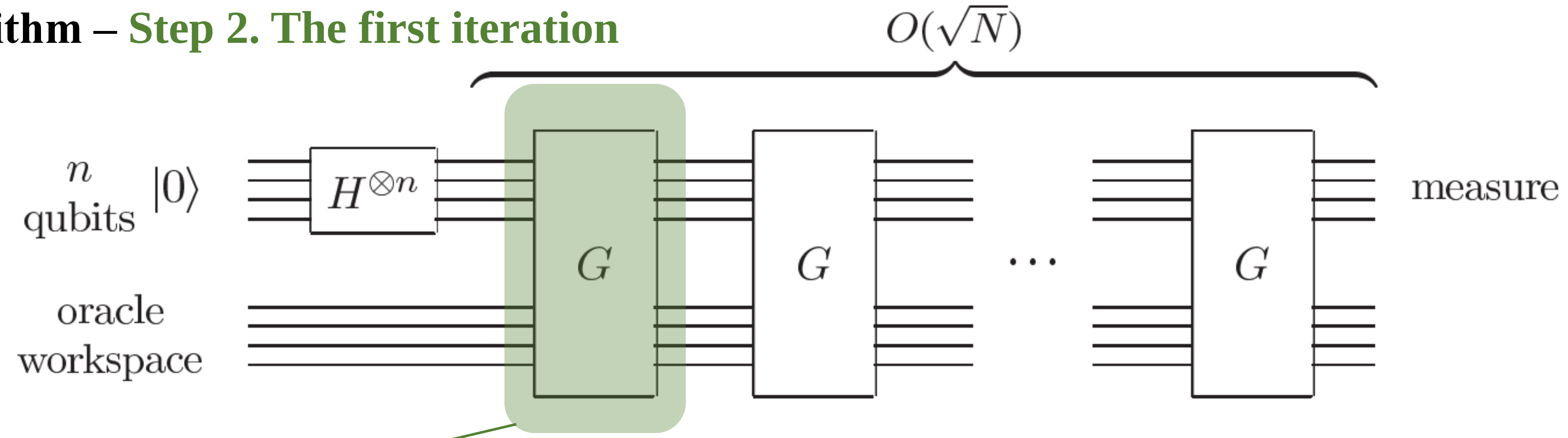


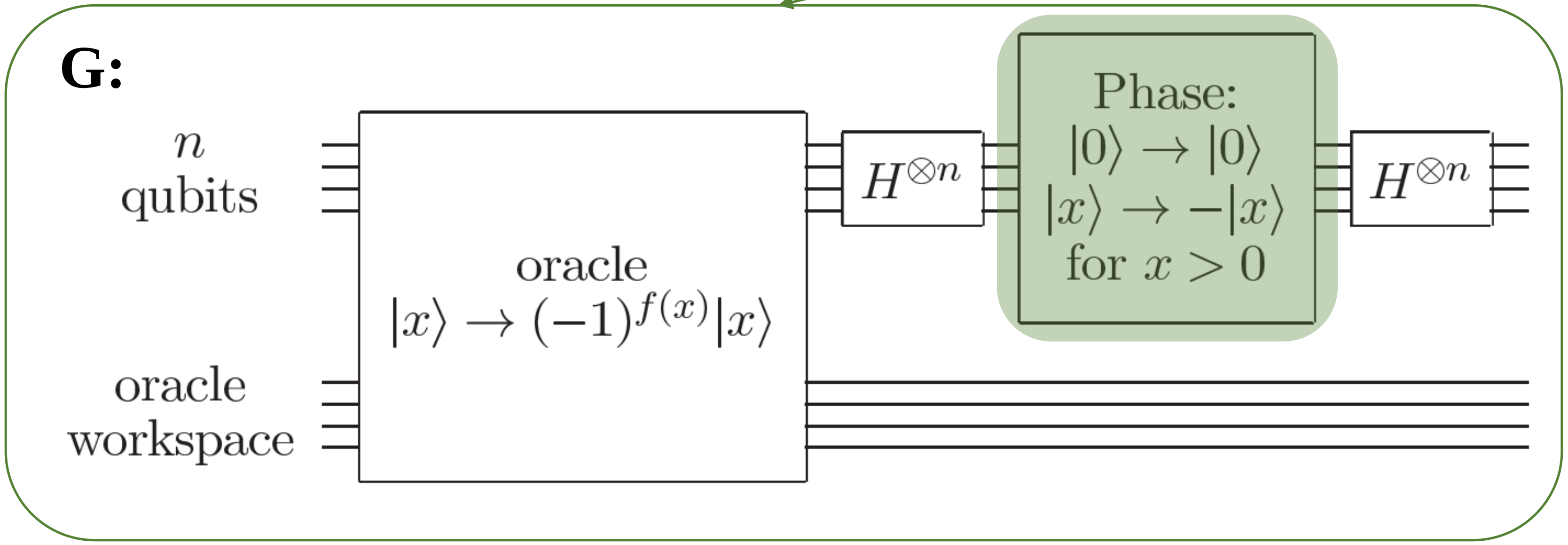


Step 2.2 Again apply the Hadamard transforms to the n qubits.

Reference & picture: Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

Procedures of Grover's Search Algorithm – **Step 2. The first iteration**

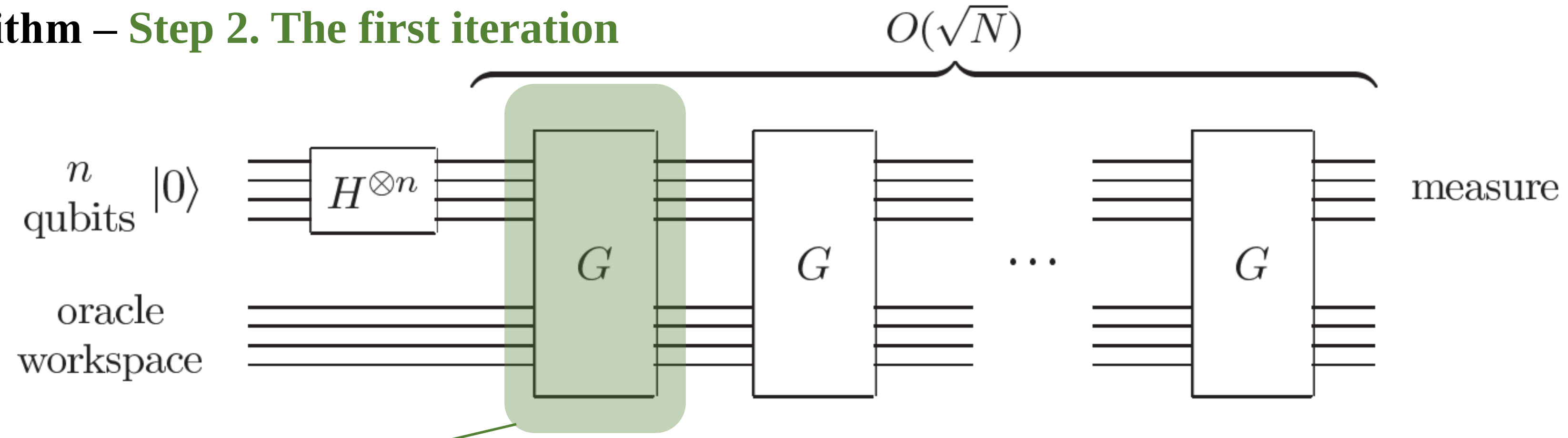


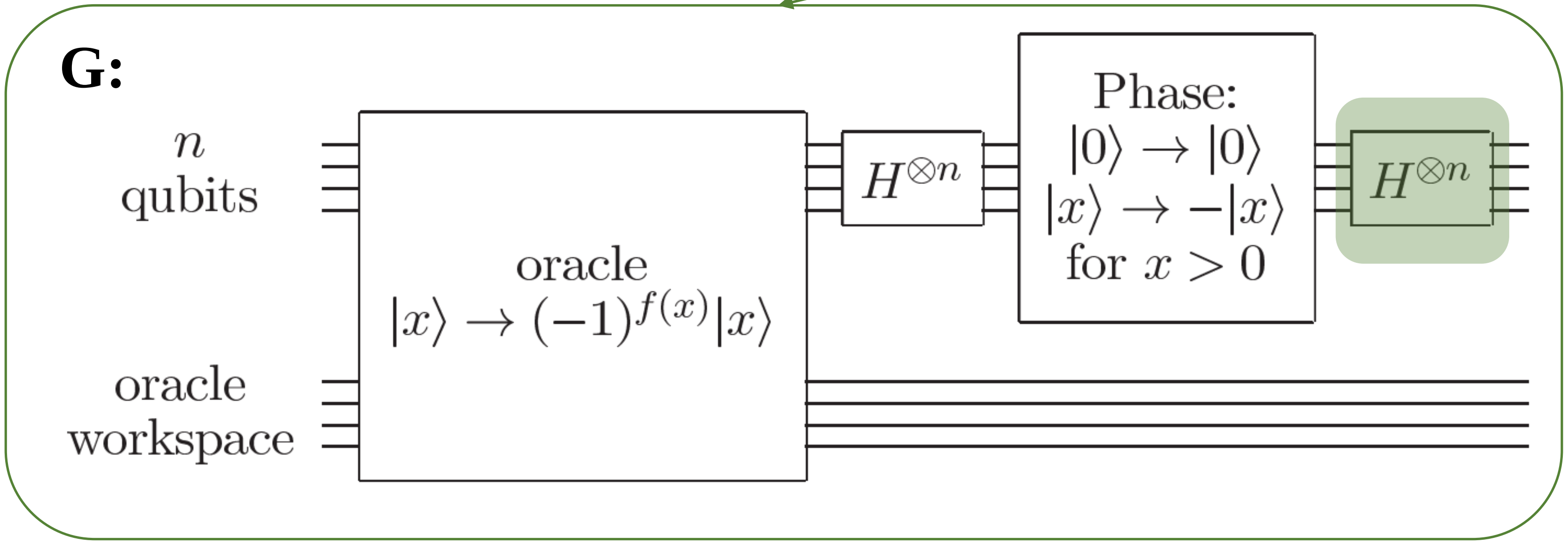


Step 2.3 Inverse all the states other than $|x\rangle$.

Reference & picture: Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

Procedures of Grover's Search Algorithm – Step 2. The first iteration

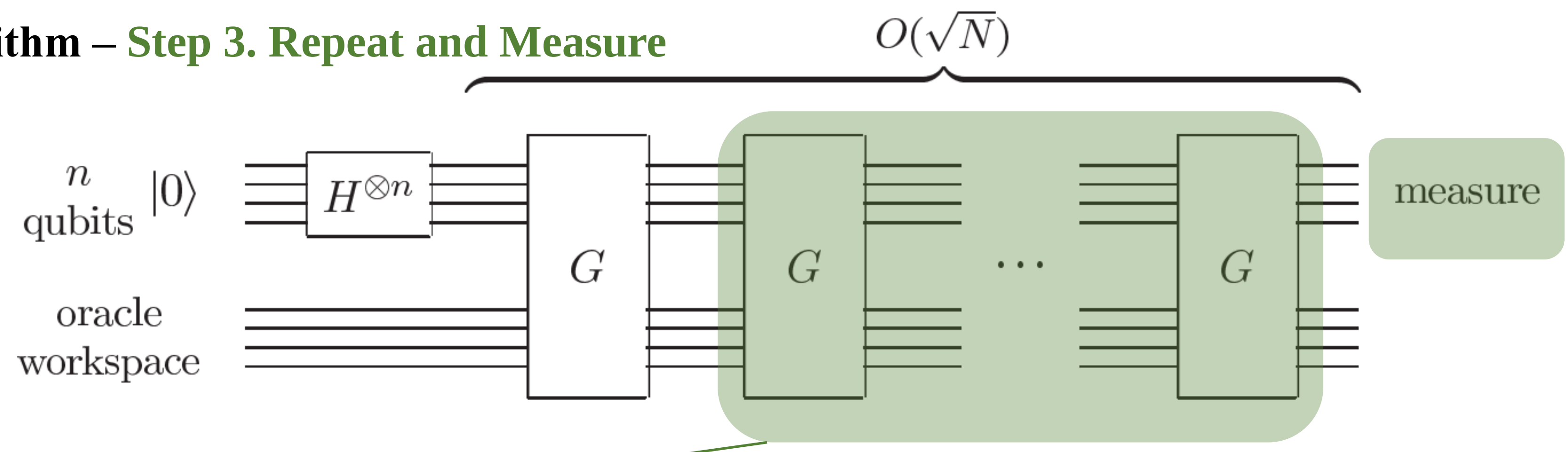


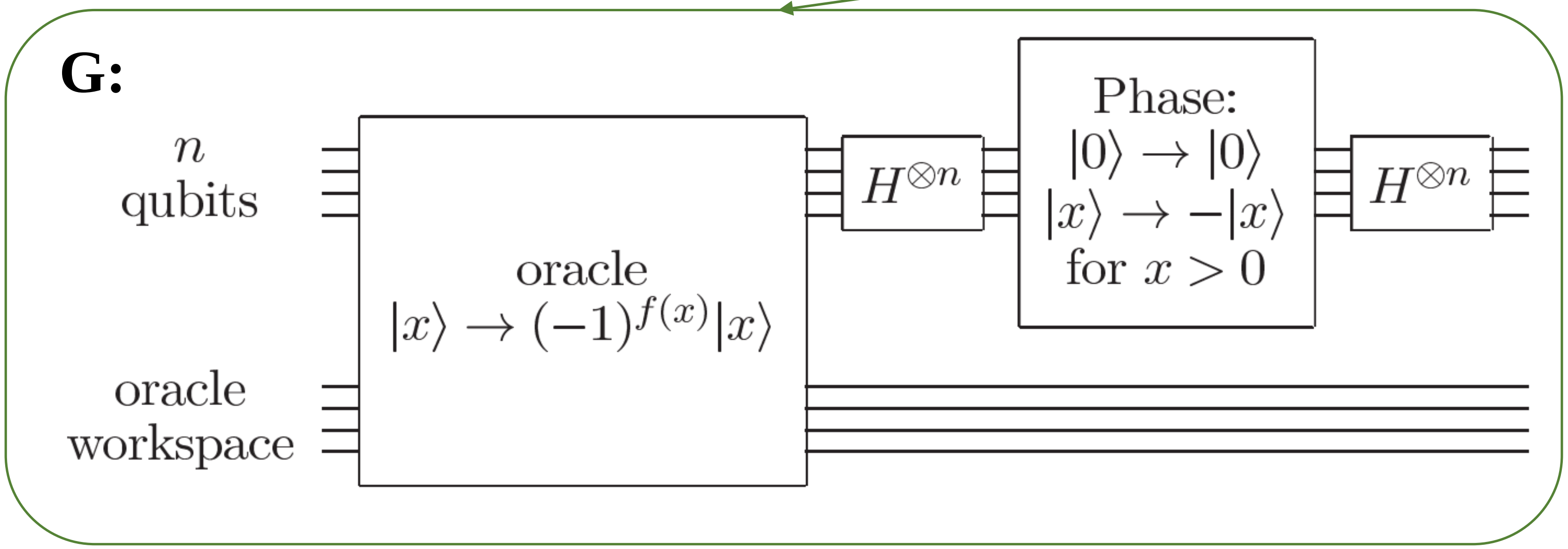


Step 2.4 Again apply the Hadamard transforms to the n qubits.
Thus steps 2.1 to 2.4 can be expressed by:
$H^{\otimes n}(2|0\rangle\langle 0| - I)\, H^{\otimes n} = 2|\psi\rangle\langle\psi| - I.$
Thus the G operator is:
$G = (2|\psi\rangle\langle\psi| - I)O.$

Reference & picture: Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

Procedures of Grover's Search Algorithm – **Step 3. Repeat and Measure**





Step 3. Repeat the operation G for $O(\sqrt{N})$ times. Then measure the n qubits, to get the x with high probability.

Reference & picture: Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.