Quantum Search Algorithm

Ming Xu

Shanghai Key Lab of Trustworthy Computing
East China Normal University

December 21, 2022

Motivation

An unsorted database contains N records, of which just one satisfies a particular property. The problem is to identity that one record.

- Classical algorithm: search all records and check them one by one. It takes $\mathcal{O}(N)$ operations in the worst case, and takes $\mathcal{O}(N/2)$ operations in the average case. Both are in $\mathcal{O}(N)$.
- Could we speed up this procedure? Grover (1996) gave a positive answer that takes only $\mathcal{O}(\sqrt{N})$ operation using quantum computing.

Oracle

The efficiency of Grover algorithm is owing to an **oracle (query)**, i.e., one can recognize the solutions.

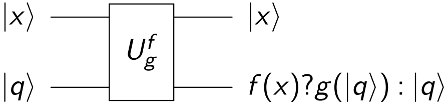
An oracle is a black box of operations, which we do not necessarily know the technical details, but achieves a particular goal.

Recognizing the solutions is usually simpler than finding the solutions. A lots of examples could be mentioned to illustrate this point here.

For example, in RSA public key cryptosystem, it is easy to check if an integer q is a factor of a large integer m. However, finding the factors q of m is very hard.

Oracle-controlled Operation

Equipped with this oracle, we can implement the oracle-controlled operation



$$|x\rangle\,|q\rangle \xrightarrow{U_g^f} |x\rangle\,(f(x)?g(|q\rangle):|q\rangle)$$

where

- $|x\rangle$ is the control qubit, and
- $|q\rangle$ is the target qubit that is changed by g iff $f(x) = 1$, the oracle is checked to be true.

Example

Sometimes, we need the oracle of recognizing an appointed value x_0 by adding a phase shift of -1 to the control qubit $|x\rangle$, where $x \in \{0, 1\}$ is the control bit. How can we achieve it?

Recalling the Deutsch–Jozsa algorithm, the operation

$$|x\rangle|-\rangle \xrightarrow{CNOT} (-1)^x |x\rangle|-\rangle$$

adds a phase shift of -1 to $|x\rangle$ whenever $x = 1$.

Example

Generalizing it, we can achieve

$$|x\rangle\,|q\rangle \xrightarrow{U_g^f} (-1)^{f(x)}\,|x\rangle\,|q\rangle$$

where the oracle $f(x)$ is 1 iff $x = x_0$, by

$$\begin{aligned}|x\rangle\,|q\rangle &\xrightarrow{(|f(x)\rangle\langle x|+\left|\bar{f(x)}\right\rangle\left\langle\bar{x}\right|)\otimes(|-\rangle\langle q|+|+\rangle\langle\bar{q}|)} |f(x)\rangle\,|-\rangle\\ &\xrightarrow{CNOT} (-1)^{f(x)}\,|f(x)\rangle\,|-\rangle\\ &\xrightarrow{(|x\rangle\langle f(x)|+\left|\bar{x}\right\rangle\left\langle\bar{f(x)}\right|)\otimes(|q\rangle\langle -|+|\bar{q}\rangle\langle +|)} (-1)^{f(x)}\,|x\rangle\,|q\rangle\,.\end{aligned}$$

We can view the above operation as $|x\rangle \xrightarrow{U_g^f} (-1)^{f(x)}\,|x\rangle$ in the support of an extra work qubit.

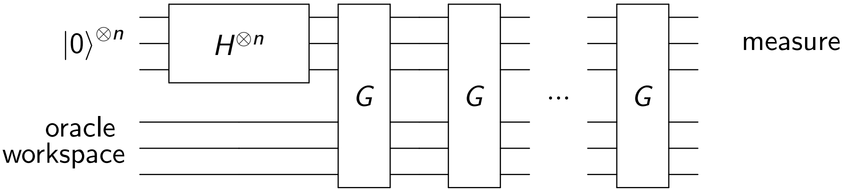
More generally, it could be any abstract function, which induces ...

Query Complexity

The complexity are specified in terms of different scale:

- bit operations: bit AND '&' and OR '|' operations cost one unit of consumption
- arithmetic operations: addition '$+$' and multiplication '$\times$' of two numbers cost one unit of consumption
- algebraic operations: addition, subtraction, multiplication, division, and taking roots of a polynomial cost one unit of consumption
- oracle/query: abstract functions cost one unit of consumption

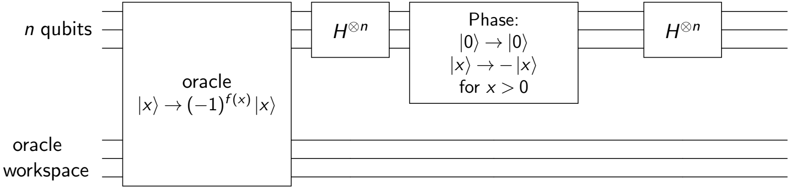
Outline



G is the *Grover iteration* to be described below.

Our goal: find a solution to the search problem using the least possible number of invoking the oracle.

Grover Iteration



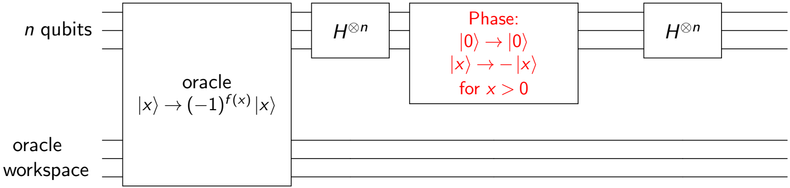
Grover iteration has four steps:

1. apply the oracle O;
2. apply the Hadamard transform $H^{\otimes n}$;
3. perform a conditional phase shift on the computer, with every computational basis state except $|0\rangle$ receiving a phase shift of -1;

$$\begin{cases} |x\rangle \to |x\rangle, & x = 0^{\otimes n} \\ |x\rangle \to -|x\rangle, & x \neq 0^{\otimes n} \end{cases}$$

4. apply with the Hadamard transform $H^{\otimes n}$.

Grover Iteration



- The unitary operator of the phase shift is $2|0\rangle\langle 0| - \mathbf{I}$.
- The unitary operator of the combined effect of Steps 2–4 is

$$H^{\otimes n}(2|0\rangle\langle 0| - \mathbf{I})H^{\otimes n} = 2|\psi\rangle\langle\psi| - \mathbf{I}$$

where $|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$.

Thus the Grover iteration G can be rephrased as $(2|\psi\rangle\langle\psi| - \mathbf{I})O$.

Geometric visualization

Grover iteration can be regarded as a **rotation** in the two-dimensional spaces, which is spanned by solution and non-solution.

Geometric visualization

Namely, we define

$$|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_{x:f(x)=0} |x\rangle \quad \text{and} \quad |\beta\rangle \equiv \frac{1}{\sqrt{M}} \sum_{x:f(x)=1} |x\rangle$$

where

- $|\alpha\rangle$ is the (normalized) non-solution to the search problem,
- $|\beta\rangle$ is the (normalized) solution.

W.l.o.g., the number $M = |\{x : f(x) = 1\}|$ is mush less than N.

Geometric visualization

Then the maximal superposition is

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle .$$

With $\cos(\frac{\theta}{2}) = \sqrt{\frac{N-M}{N}}$ and $\sin(\frac{\theta}{2}) = \sqrt{\frac{M}{N}}$ for some small θ, we get

$$|\psi\rangle = \cos(\tfrac{\theta}{2}) |\alpha\rangle + \sin(\tfrac{\theta}{2}) |\beta\rangle .$$

Geometric visualization

$$|\psi\rangle = \cos(\tfrac{\theta}{2})\,|\alpha\rangle + \sin(\tfrac{\theta}{2})\,|\beta\rangle$$

$$\Downarrow$$

$$O\,|\psi\rangle = \cos(-\tfrac{\theta}{2})\,|\alpha\rangle + \sin(-\tfrac{\theta}{2})\,|\beta\rangle$$

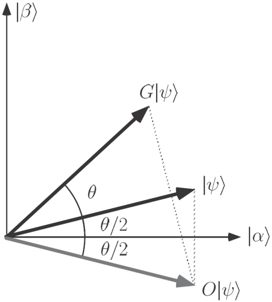
$$\Downarrow$$

$$G = (2\,|\psi\rangle\langle\psi| - I)\,O$$

$$\begin{aligned} G\,|\psi\rangle &= \cos(2\tfrac{\theta}{2} - (-\tfrac{\theta}{2}))\,|\alpha\rangle + \sin(2\tfrac{\theta}{2} - (-\tfrac{\theta}{2}))\,|\beta\rangle \\ &= \cos(\tfrac{3\theta}{2})\,|\alpha\rangle + \sin(\tfrac{3\theta}{2})\,|\beta\rangle \end{aligned}$$

$$\Downarrow$$

$$G^k\,|\psi\rangle = \cos(\tfrac{2k+1}{2}\theta)\,|\alpha\rangle + \sin(\tfrac{2k+1}{2}\theta)\,|\beta\rangle$$



Performance Analysis

The iteration times R is

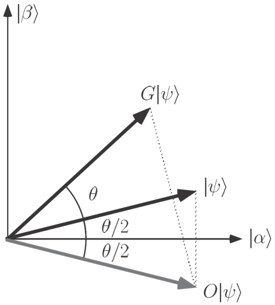
$$R = \left[\frac{\pi/2 - \theta/2}{\theta}\right] = \left[\frac{\pi - \theta}{2\theta}\right]$$

thus

$$R = \left\lceil \frac{\pi}{2\theta} \right\rceil$$

As $\frac{\theta}{2} \geq \sin(\frac{\theta}{2}) = \sqrt{\frac{M}{N}}$, we could get

$$R = \left\lceil \frac{\pi}{4} \cdot \sqrt{\frac{N}{M}} \right\rceil$$



That is, $R \in \mathscr{O}(\sqrt{\frac{N}{M}})$ times of Grover iterations could be performed in order to obtain a solution to the search problem with high probability!

Summary

- G is a rotation in the two-dimensional space spanned by $|\alpha\rangle$ and $|\beta\rangle$, rotating the space by θ radians per application of G.
- Repeated application of the Grover iteration rotates the state vector close to $|\beta\rangle$, i.e. the integer $\lceil \frac{\pi}{2\theta} \rceil$ times.
- An observation in the computational basis produces with high probability one of the outcomes superposed in $|\beta\rangle$, which is the solution to the search problem.

Grover algorithm

Input: 1. an oracle O which performs the transformation $O|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$, where $f(x) = 1$ iff $x = x_0$;
2. $n+1$ qubits in the state $|0\rangle$.

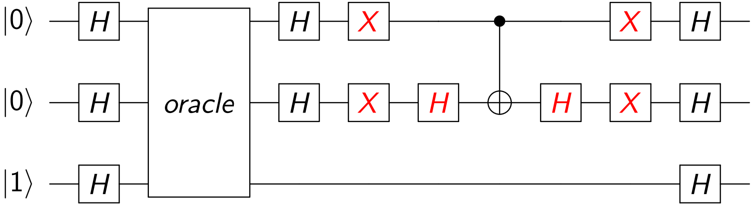
Output: x_0.

1: $|0\rangle^{\otimes n}|1\rangle$ ▷ initial state
2: $\rightarrow \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle[\frac{|0\rangle-|1\rangle}{\sqrt{2}}]$ ▷ apply $H^{\otimes n}$ to the first n quibits, and H to the last qubit
3: $\rightarrow [(2|\psi\rangle\langle\psi| - \mathbf{I})O]^R \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle[\frac{|0\rangle-|1\rangle}{\sqrt{2}}]$
$\approx |x_0\rangle[\frac{|0\rangle-|1\rangle}{\sqrt{2}}]$ ▷ apply the Grover iteration $R = \left\lceil \frac{\pi}{4} \cdot \sqrt{\frac{N}{M}} \right\rceil$ times.
4: $\rightarrow x_0$ ▷ measure the first n quibits.

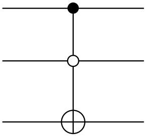
Complexity: $\mathscr{O}(\sqrt{2^n})$ operations. Succeeds with probability $\mathscr{O}(1)$.

A two-bit example

The quantum circuit which performs the initial Hadamard transforms and a single Grover iteration G is



If we search for the string $x_0 = 10$. The oracle can be the circuits on the right.



A two-bit example

The input state is

$$|\phi_0\rangle = |00\rangle \otimes |1\rangle .$$

After applying Hadamard gate to it, we could get

$$\begin{aligned}
|\phi_1\rangle &= \tfrac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \otimes |-\rangle \\
&= [\tfrac{1}{2}|00\rangle + \tfrac{1}{2}(|01\rangle + |10\rangle + |11\rangle)] \otimes |-\rangle \\
&= [\tfrac{\sqrt{3}}{2}|\alpha\rangle + \tfrac{1}{2}|\beta\rangle] \otimes |-\rangle \\
&= [\cos(\tfrac{\pi}{6})|\alpha\rangle + \sin(\tfrac{\pi}{6})|\beta\rangle] \otimes |-\rangle
\end{aligned}$$

Thus the initial state of Grover iteration is $|\psi\rangle = \frac{\sqrt{3}}{2}|\alpha\rangle + \frac{1}{2}|\beta\rangle$, which implies

- $\theta/2 = \pi/6$ from the coefficients of $|\alpha\rangle$ and $|\beta\rangle$, and
- a single rotation by $\theta = \pi/3$ moves $|\psi\rangle$ to $|\beta\rangle$.

Thus exactly one iteration is required!

Homework

EX1. Show that the unitary operator corresponding to the phase shift in the Grover iteration is $2|0\rangle\langle 0| - \mathbf{I}$.

References

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In *Proc. 28th Annual ACM Symposium on Theory of Computing*, STOC '96, page 212–219. ACM.