Quantum search algorithms

Guojing Tian

Institute of Computing Technology, CAS

6.13, 2019

中科院计算所
INSTITUTE OF COMPUTING TECHNOLOGY, CAS

Outline

1. Grover's algorithm
   - the oracle
   - the procedure
   - geometric visualization
   - performance
2. quantum simulation
   - quantum search as a quantum simulation
   - input and output
   - Hamiltonian
   - simulate
   - resource costs
3. quantum counting

the oracle

- search space: N **elements**
- focus: **index**, which is just a number in $[0, N-1]$, rather than the element itself

the oracle

- search space: N **elements**
- focus: **index**, which is just a number in $[0, N-1]$, rather than the element itself
- assume $N = 2^n$, so the index can be stored in n bits; M solutions
- A particular instance of the search problem can be represented by a function f, i.e.,

$$f(x) = \begin{cases} 1, & \text{if } x \text{ is a solution to the search problem} \\ 0, & \text{if } x \text{ is not a solution to the search problem} \end{cases}$$

Suppose we are supplied with a quantum oracle with the ability to recognize solutions to the search problem.

the oracle qubit

The oracle is a unitary operator, O, defined by its action on the computational basis:

$$|x\rangle|q\rangle \xrightarrow{O} |x\rangle|q \oplus f(x)\rangle,$$

where $|x\rangle$ is the index register, $\oplus$ denotes addition modulo 2, and the oracle qubit $|q\rangle$ is a single qubit which is flipped if $f(x) = 1$ and is unchanged otherwise.

If the initial oracle qubit is in the state $(|0\rangle - |1\rangle)/\sqrt{2}$, then the final state will be

$$|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \xrightarrow{O} (-1)^{f(x)}|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).$$

If the initial oracle qubit is in the state $(|0\rangle - |1\rangle)/\sqrt{2}$, then the final state will be

$$|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \xrightarrow{O} (-1)^{f(x)}|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).$$

Notice the state of the oracle qubit is not changed, thus the action of the oracle may be written:

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

If the initial oracle qubit is in the state $(|0\rangle - |1\rangle)/\sqrt{2}$, then the final state will be

$$|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \xrightarrow{O} (-1)^{f(x)}|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).$$

Notice the state of the oracle qubit is not changed, thus the action of the oracle may be written:

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

That is to say, the oracle marks the solutions to the search problem by shifting the phase of the solution.

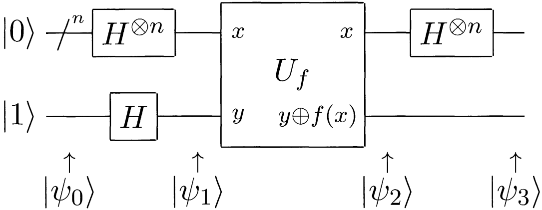
Deutsch-Jozsa algorithm

- Setting: Alice selects a number x from 0 to $2^n - 1$, and mails it in a letter to Bob;
  Bob calculates $f(x)$ (constant or balanced) and replies with the result 0 or 1.
- Goal: Alice will **determine** whether Bob has chosen a constant or a balanced function, corresponding with him as little as possible.

Deutsch-Jozsa algorithm

- Setting: Alice selects a number x from 0 to $2^n - 1$, and mails it in a letter to Bob;
  Bob calculates $f(x)$ (constant or balanced) and replies with the result 0 or 1.
- Goal: Alice will **determine** whether Bob has chosen a constant or a balanced function, corresponding with him as little as possible.

- Classical: $2^n/2 + 1$ queries
- Quantum: 1 query using U_f to calculate $f(x)$


$|0\rangle$
n
$H^{\otimes n}$
x
x
U_f
$H^{\otimes n}$
$|1\rangle$
H
y
$y \oplus f(x)$
$|\psi_0\rangle$
$|\psi_1\rangle$
$|\psi_2\rangle$
$|\psi_3\rangle$

Algorithm: Deutsch–Jozsa

Inputs: (1) A black box U_f which performs the transformation $|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$, for $x \in \{0, \ldots, 2^n - 1\}$ and $f(x) \in \{0, 1\}$. It is promised that $f(x)$ is either *constant* for all values of x, or else $f(x)$ is *balanced*, that is, equal to 1 for exactly half of all the possible x, and 0 for the other half.

Outputs: 0 if and only if f is constant.

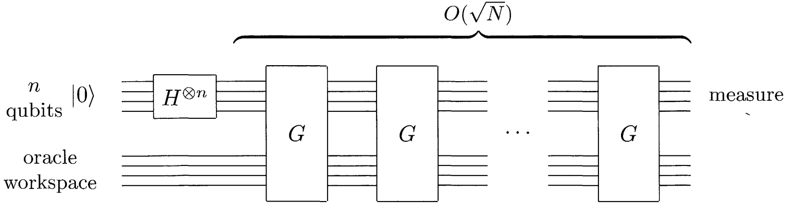
Runtime: One evaluation of U_f. Always succeeds.

Procedure:

1.	$\|0\rangle^{\otimes n}\|1\rangle$	initialize state
2.	$\rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \|x\rangle \left[\frac{\|0\rangle - \|1\rangle}{\sqrt{2}}\right]$	create superposition using Hadamard gates
3.	$\rightarrow \sum_x (-1)^{f(x)} \|x\rangle \left[\frac{\|0\rangle - \|1\rangle}{\sqrt{2}}\right]$	calculate function f using U_f
4.	$\rightarrow \sum_z \sum_x \frac{(-1)^{x \cdot z + f(x)} \|z\rangle}{\sqrt{2^n}} \left[\frac{\|0\rangle - \|1\rangle}{\sqrt{2}}\right]$	perform Hadamard transform
5.	$\rightarrow z$	measure to obtain final output z

the procedure

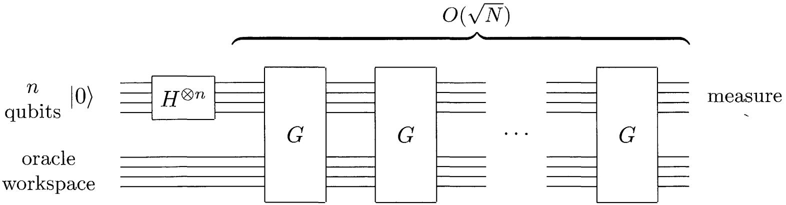
Schematically, the search algorithm operates as shown below.



- The oracle may employ work qubits for its implementation, but the analysis of the quantum search algorithm involves only the n-qubit register.
- Goal: to find a solution to the search problem, using the smallest possible number of the applications of the oracle.

the procedure

Schematically, the search algorithm operates as shown below.



- The oracle may employ work qubits for its implementation, but the analysis of the quantum search algorithm involves only the n-qubit register.
- Goal: to find a solution to the search problem, using the smallest possible number of the applications of the oracle.

G???

The quantum search algorithm consists of repeated application known as the Grover iteration or Grover operator, which we denote G. And it may be broken up into four steps:

1. Apply the oracle O.

The quantum search algorithm consists of repeated application known as the Grover iteration or Grover operator, which we denote G. And it may be broken up into four steps:

1. Apply the oracle O.
2. Apply the Hadamard transform $H^{\otimes n}$.

The quantum search algorithm consists of repeated application known as the Grover iteration or Grover operator, which we denote G. And it may be broken up into four steps:

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

$$|x\rangle \rightarrow -(-1)^{\delta_x}|x\rangle.$$

Q1: Show that the unitary operator corresponding to the phase shift in the G is $2|0\rangle\langle 0| - I$.

The quantum search algorithm consists of repeated application known as the Grover iteration or Grover operator, which we denote G. And it may be broken up into four steps:

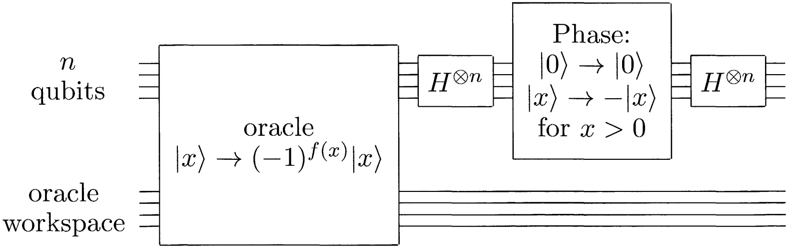
1. Apply the oracle O.
2. Apply the Hadamard transform $H^{\otimes n}$.
3. Perform a conditional phase shift with every computational basis state except $|0\rangle$ receiving a phase shift of -1,

$$|x\rangle \rightarrow -(-1)^{\delta_x}|x\rangle.$$

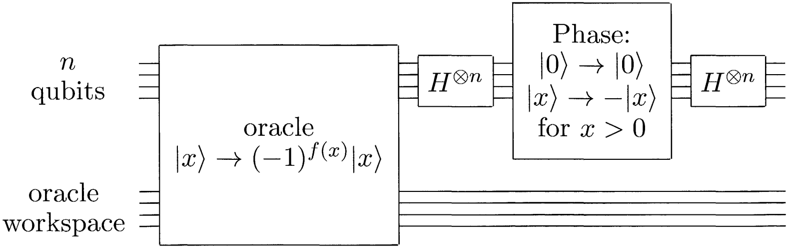
4. Apply the Hadamard transform $H^{\otimes n}$.

Q1: Show that the unitary operator corresponding to the phase shift in the G is $2|0\rangle\langle 0| - I$.

Each of the operations in the G may be efficiently implemented on a quantum computer.



Each of the operations in the G may be efficiently implemented on a quantum computer.



$$G = (2|\psi\rangle\langle\psi| - I)\,O, \quad \text{where}|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle.$$

geometric visualization

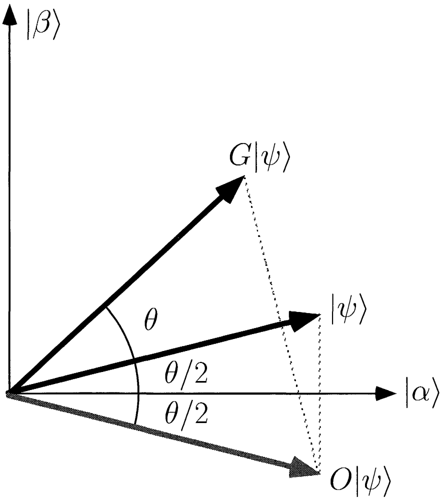
Actually, the Grover iteration "G" can be regarded as a rotation in the two-dim space spanned by the starting vector $|\psi\rangle$ and the superposition.

- $|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_x'' |x\rangle$, where x indicates all non-solutions;
- $|\beta\rangle \equiv \frac{1}{\sqrt{M}} \sum_x' |x\rangle$, where x indicates all solutions.

geometric visualization

Actually, the Grover iteration "G" can be regarded as a rotation in the two-dim space spanned by the starting vector $|\psi\rangle$ and the superposition.

- $|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_x'' |x\rangle$, where x indicates all non-solutions;
- $|\beta\rangle \equiv \frac{1}{\sqrt{M}} \sum_x' |x\rangle$, where x indicates all solutions.
- Thus, $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle$.



where $\cos\frac{\theta}{2} = \sqrt{\frac{N-M}{M}}$, then $|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$.

performance

How many times must "G" be repeated in order to rotate $|\psi\rangle$ near $|\beta\rangle$ (the solution space)?

- $R = \left[\frac{arccos\sqrt{M/N}}{\theta}\right]$, with $\theta/2$ error

performance

How many times must "G" be repeated in order to rotate $|\psi\rangle$ near $|\beta\rangle$ (the solution space)?

- $R = \left[\frac{arccos\sqrt{M/N}}{\theta}\right]$, with $\theta/2$ error
- If $M \ll N$, then $\theta \approx \sin\theta \approx 2\sqrt{M/N}$, thus the angular error in the final state is at most $\theta/2 \approx \sqrt{M/N}$.

performance

How many times must "G" be repeated in order to rotate $|\psi\rangle$ near $|\beta\rangle$ (the solution space)?

- $R = \left[\frac{arccos\sqrt{M/N}}{\theta}\right]$, with $\theta/2$ error
- If $M \ll N$, then $\theta \approx \sin\theta \approx 2\sqrt{M/N}$, thus the angular error in the final state is at most $\theta/2 \approx \sqrt{M/N}$.
- note that $R \leq \lceil \pi/2\theta \rceil$, so the lower bound on $\theta \longrightarrow$ an upper bound on R

$$\frac{\theta}{2} \geq \sin\frac{\theta}{2} = \sqrt{\frac{M}{N}} \Longrightarrow R \leq \lceil \frac{\pi}{4}\sqrt{\frac{M}{N}} \rceil$$

The quantum search algorithm $(M = 1)$ is summarized below.

The quantum search algorithm ($M = 1$) is summarized below.

Inputs: (1) a black box oracle O which performs the transformation $O|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle$, where $f(x) = 0$ for all $0 \leq x < 2^n$ except x_0, for which $f(x_0) = 1$; (2) $n + 1$ qubits in the state $|0\rangle$.

Outputs: x_0.

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

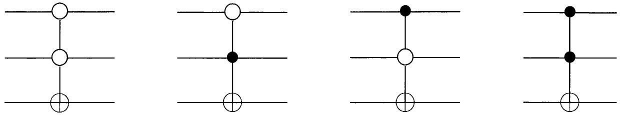
Procedure:

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

example

Here is an explicit example illustrating how the quantum search algorithm works on a search space of size $N = 4$.

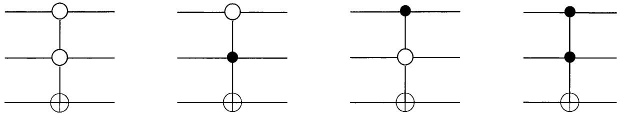
- The **oracle** can be taken to be one of the four circuits:



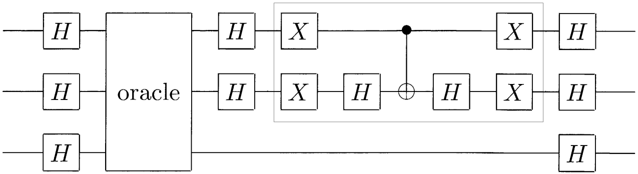
example

Here is an explicit example illustrating how the quantum search algorithm works on a search space of size $N = 4$.

- The **oracle** can be taken to be one of the four circuits:



- The whole circuit is as follows.

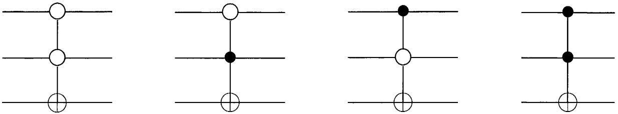


where the gates in the box perform $2|00\rangle\langle 00| - I$.

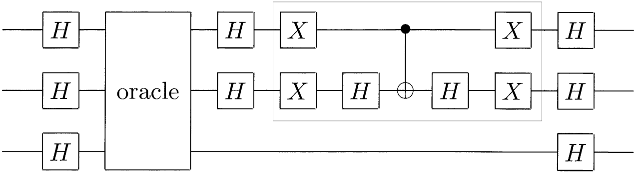
example

Here is an explicit example illustrating how the quantum search algorithm works on a search space of size $N = 4$.

- The **oracle** can be taken to be one of the four circuits:



- The whole circuit is as follows.



where the gates in the box perform $2|00\rangle\langle 00| - I$.

- $|\psi\rangle^{\pi/6} \xrightarrow{\theta=\pi/3} |\beta\rangle$, that is, exactly one iteration.

quantum search as a quantum simulation

How would one **dream up** the quantum search algorithm (Grover's algorithm) from **a state of ignorance**?

quantum search as a quantum simulation

How would one **dream up** the quantum search algorithm (Grover's algorithm) from **a state of ignorance**?

Next we will sketch a heuristic means by which one can 'derive' this search algorithm, in the hope of lending some intuition as to the tricky task of quantum algorithm design.

quantum search as a quantum simulation

How would one **dream up** the quantum search algorithm (Grover's algorithm) from **a state of ignorance**?

Next we will sketch a heuristic means by which one can 'derive' this search algorithm, in the hope of lending some intuition as to the tricky task of quantum algorithm design.

1. specify the problem to be solved **(input and output)**
2. guess a **Hamiltonian** to solve the problem, and verify that it does work
3. find a procedure to **simulate** the Hamiltonian
4. analyze the **resource costs** of the simulation

input and output

input: $|\psi\rangle$

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

output: $|x\rangle$, where x is the solution.

Hamiltonian

$$e^{-iHt}|\psi\rangle = |x\rangle$$

Hamiltonian

$$e^{-iHt}|\psi\rangle = |x\rangle$$

H should be entirely from the terms $|\psi\rangle$ and $|x\rangle$, i.e., it must be a sum of terms like $|\psi\rangle\langle\psi|, |x\rangle\langle x|, |\psi\rangle\langle x|, |x\rangle\langle\psi|$, and the simplest choice is

$$H = |x\rangle\langle x| + |\psi\rangle\langle\psi|$$

Hamiltonian

$$e^{-iHt}|\psi\rangle = |x\rangle$$

H should be entirely from the terms $|\psi\rangle$ and $|x\rangle$, i.e., it must be a sum of terms like $|\psi\rangle\langle\psi|, |x\rangle\langle x|, |\psi\rangle\langle x|, |x\rangle\langle\psi|$, and the simplest choice is

$$H = |x\rangle\langle x| + |\psi\rangle\langle\psi|$$

$$\begin{aligned}
e^{-iHt}|\psi\rangle &\overset{H=I+\alpha(\beta X+\alpha Z)}{\Longrightarrow} e^{-it}\Big[\cos(\alpha t)|\psi\rangle - i\sin(\alpha t)(\beta X + \alpha Z)|\psi\rangle\Big] \\
&\overset{\text{global phase}}{\Longrightarrow} \cos(\alpha t)|\psi\rangle - i\sin(\alpha t)(\beta X + \alpha Z)|\psi\rangle \\
&\overset{(\beta X+\alpha Z)|\psi\rangle=|x\rangle}{\Longrightarrow} \cos(\alpha t)|\psi\rangle - i\sin(\alpha t)|x\rangle \\
&\overset{t=\pi/2\alpha}{\Longrightarrow} |x\rangle, \quad \text{and} \quad t = \pi\sqrt{N}/2
\end{aligned}$$

simulate

$$e^{-iH\Delta t} = e^{-i|x\rangle\langle x|\Delta t} e^{-i|\psi\rangle\langle\psi|\Delta t}$$

simulate

$$e^{-iH\Delta t} = e^{-i|x\rangle\langle x|\Delta t} e^{-i|\psi\rangle\langle\psi|\Delta t}$$

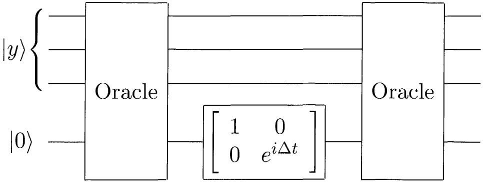


Figure 6.4. Circuit implementing the operation $\exp(-i|x\rangle\langle x|\Delta t)$ using two oracle calls.

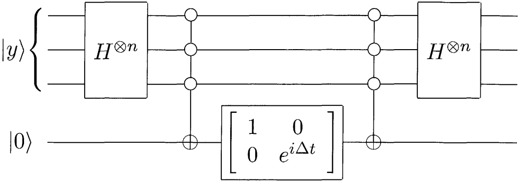


Figure 6.5. Circuit implementing the operation $\exp(-i|\psi\rangle\langle\psi|\Delta t)$, for $|\psi\rangle$ as in (6.24).

resource costs

$$U(\Delta t) \equiv e^{-iH\Delta t} = e^{-i|x\rangle\langle x|\Delta t} e^{-i|\psi\rangle\langle\psi|\Delta t}$$

Define

$$|x\rangle\langle x| = (I + Z)/2 = (I + \hat{z}\cdot\vec{\sigma})/2, \text{ where } \hat{z} = (0,0,1),$$
$$|\psi\rangle\langle\psi| = (I + \vec{\psi}\cdot\vec{\sigma})/2, \text{ where } \vec{\psi} = (2\alpha\beta, 0, (\alpha^2 - \beta^2)),$$
$$\cos(\theta/2) = \cos^2(\Delta t/2) - \sin^2(\Delta t/2)\vec{\psi}\cdot\hat{z},$$

then

$$U(\Delta t) = \left(\cos^2\left(\frac{\Delta t}{2}\right) - \sin^2\left(\frac{\Delta t}{2}\right)\vec{\psi}\cdot\hat{z}\right) I$$
$$-2i\sin\left(\frac{\Delta t}{2}\right)\left(\cos\left(\frac{\Delta t}{2}\right)\frac{\vec{\psi}+\hat{z}}{2} + \sin\left(\frac{\Delta t}{2}\right)\frac{\vec{\psi}\times\hat{z}}{2}\right)\cdot\vec{\sigma}\,.$$

Upon substitution $\vec{\psi} \cdot \hat{z} = \alpha^2 - \beta^2 = (2/N - 1)$, we obtain

$$\cos\left(\frac{\theta}{2}\right) = 1 - \frac{2}{N}\sin^2\left(\frac{\Delta t}{2}\right).$$

In order to maximize the rotation angle θ, the smart thing is to choose $\Delta t = \pi$, then we obtain

$$\cos(\frac{\theta}{2}) = 1 - \frac{2}{N},$$

and for large N,

$$\theta \approx \frac{4}{\sqrt{N}}.$$

Indeed, if $\Delta t = \pi$, then the quantum simulation is identical with the original quantum search algorithm, since

$$e^{-i|\psi\rangle\langle\psi|\pi} = I - 2|\psi\rangle\langle\psi|,$$

$$e^{-i|x\rangle\langle x|\pi} = I - 2|x\rangle\langle x|.$$

These are identical to the steps making up the Grover iteration.

quantum algorithms as quantum simulations

amplitude amplification

If the initial superposition state in Grover's algorithm is replaced by any other state, say $|\phi\rangle = U|0\rangle$, then how to do the quantum search?

amplitude amplification

If the initial superposition state in Grover's algorithm is replaced by any other state, say $|\phi\rangle = U|0\rangle$, then how to do the quantum search?

$$G = (2|\phi\rangle\langle\phi| - I)\,O = U(2|0\rangle\langle 0| - I)\,U^\dagger\,O$$

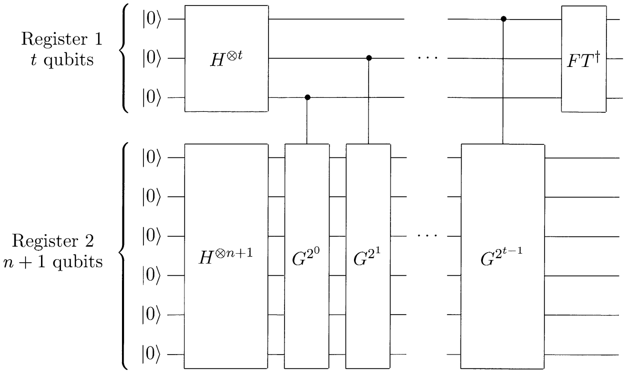
quantum counting

How quickly can we determine the number of solutions, M, to an N item search problem, if M is not known in advance?

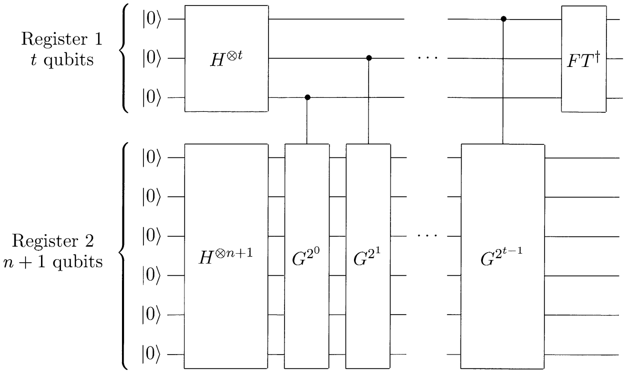
quantum counting

How quickly can we determine the number of solutions, M, to an N item search problem, if M is not known in advance?

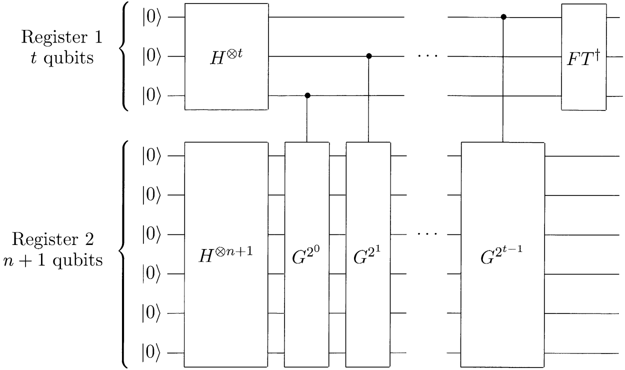
- classical: $\Theta(N)$
- quantum: Grover iteration + phase estimation



- $G = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \Longrightarrow$ eigenvalues $e^{i\theta}$, $e^{i(2\pi-\theta)}$



- $G = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \Longrightarrow$ eigenvalues $e^{i\theta}, e^{i(2\pi-\theta)}$
- $\cos(\frac{\theta}{2}) = \sqrt{\frac{2N-M}{2N}} \Longrightarrow \sin^2(\frac{\theta}{2}) = \frac{M}{2N}$



- $G = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \Longrightarrow$ eigenvalues $e^{i\theta}$, $e^{i(2\pi-\theta)}$
- $\cos(\frac{\theta}{2}) = \sqrt{\frac{2N-M}{2N}} \Longrightarrow \sin^2(\frac{\theta}{2}) = \frac{M}{2N}$
- $t \equiv m + \lceil \log(2 + 1/2\epsilon) \rceil$, with 2^{-m}-accuracy, $(1-\epsilon)$-succ. prob.

Summary

1. Grover's algorithm
   - the oracle
   - the procedure
   - geometric visualization
   - performance
2. quantum simulation
   - quantum search as a quantum simulation
   - input and output
   - Hamiltonian
   - simulate
   - resource costs
3. quantum counting