Grover's algorithm

Ryuhei Mori

Tokyo Institute of Technology

Searching problem

Searching problem:

$$f : \{1, 2, \dots, N\} \rightarrow \{0, 1\}$$

Find $x \in \{1, 2, \dots, N\}$ satisfying $f(x) = 1$.

How many times, do we have to evaluate $f(x)$?

Obviously, $O(N)$.

Quantum searching problem

Unitary oracle

$$U_f \left|x\right\rangle \left|y\right\rangle = \left|x\right\rangle \left|y \oplus f(x)\right\rangle .$$

Find $x \in \{1, 2, \ldots, N\}$ satisfying $f(x) = 1$.

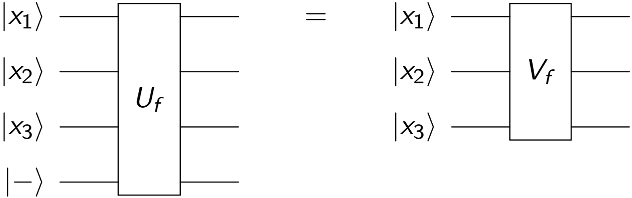
How many times, do we have to evaluate U_f ?

$O(\sqrt{N})$ by Grover's algorithm.

Unitary matrix for Grover's algorithm

Another unitary

$$V_f \left|x\right\rangle = (-1)^{f(x)} \left|x\right\rangle .$$



$$\left|x\right\rangle \left|-\right\rangle \longmapsto U_f \left|x\right\rangle \left|-\right\rangle = (-1)^{f(x)} \left|x\right\rangle \left|-\right\rangle .$$

Grover's algorithm

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

$$V_f = I - 2 \sum_{x:f(x)=1} |x\rangle \langle x|$$

$$W := I - 2 |\psi\rangle \langle\psi| .$$

Then, $G := -WV_f$ is called the Grover's operator.

The Grover's algorithm just measures $G^k |\psi\rangle$ by the computational basis $\{|x\rangle\}_x$ for some appropriately chosen k.

The two dimensional subspace

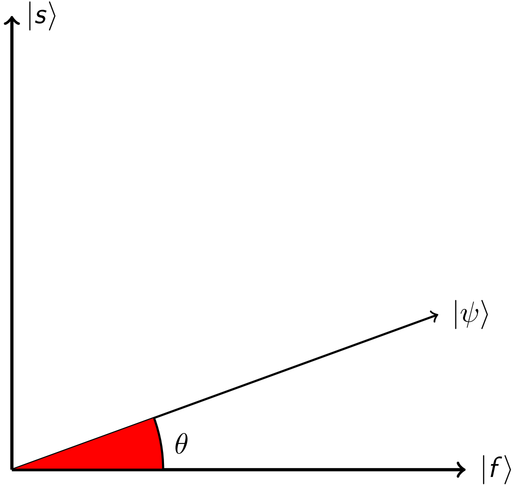
$$
\begin{aligned}
|s\rangle &:= \frac{1}{\sqrt{M}} \sum_{x:f(x)=1} |x\rangle \\
|f\rangle &:= \frac{1}{\sqrt{N-M}} \sum_{x:f(x)=0} |x\rangle .
\end{aligned}
$$

Then,

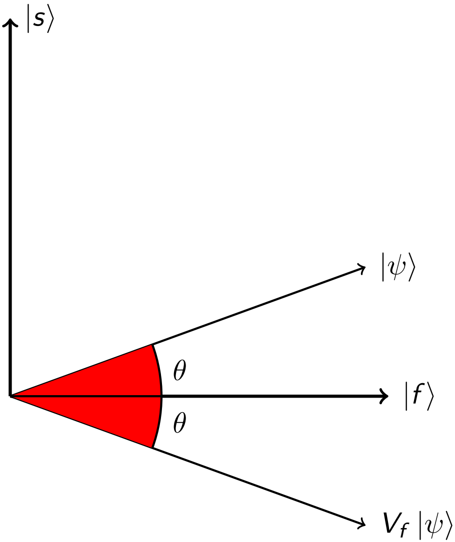
$$
\begin{aligned}
|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle &= \sqrt{\frac{M}{N}}\,|s\rangle + \sqrt{\frac{N-M}{N}}\,|f\rangle \\
&= \sin\theta\,|s\rangle + \cos\theta\,|f\rangle
\end{aligned}
$$

where $\theta := \arcsin\sqrt{\frac{M}{N}}$.

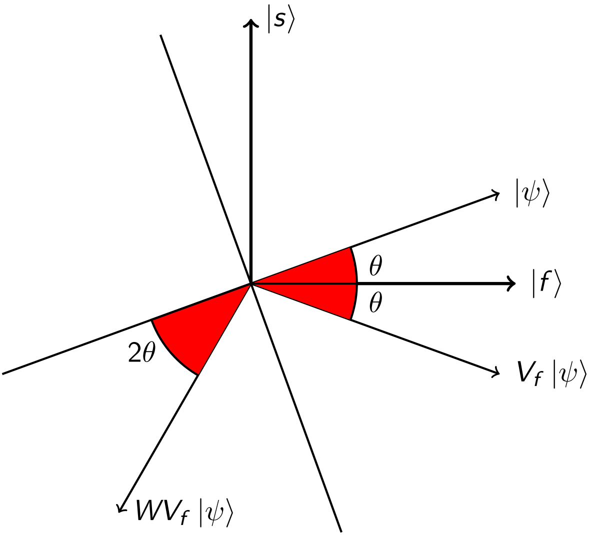
Analysis of Grover's algorithm



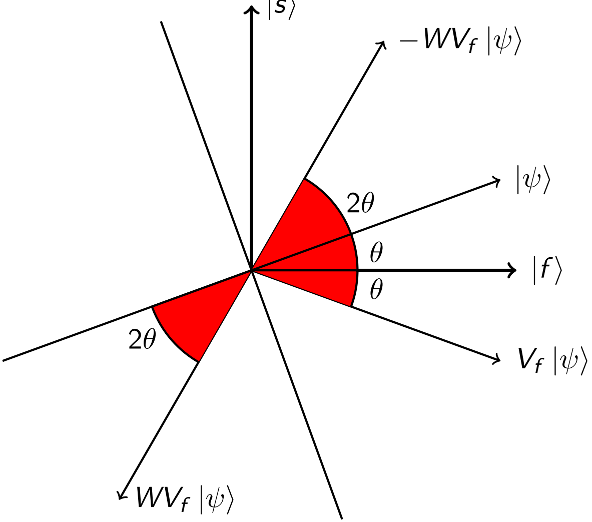
Analysis of Grover's algorithm



Analysis of Grover's algorithm



Analysis of Grover's algorithm



Analysis of Grover's algorithm

$$(-WV_f)^k |\psi\rangle = \sin((2k+1)\theta)\,|s\rangle + \cos((2k+1)\theta)\,|f\rangle$$

The probability of success is $\sin^2((2k+1)\theta)$.

Choose k satisfying

$$(2k+1)\theta \approx \frac{\pi}{2} \iff k \approx \frac{\pi}{4\theta}$$

Here, $\sin\theta = \sqrt{\frac{M}{N}} \iff \theta \approx \sqrt{\frac{M}{N}}$. Hence, $k \approx \frac{\pi}{4}\sqrt{\frac{N}{M}}$.

[Grover 1996]

Grover's search is exactly optimal for $M = 1$ [Zalka 1999], and general M [Ito and Mori 2021].

Grover's algorithm

[Boyer, Brassard, Høyer, and Tapp 1998]

1. Initialize $m = 1$ and set $\lambda = 8/7$.
2. Choose an integer j uniformly from $0, 1, \ldots, m$.
3. Apply Grover's algorithm with j iterations.
4. If solution is not found, set $m \leftarrow \min(\lambda m, \sqrt{N})$ and go back to setp 2.

This algorithm solves the "OR problem"
with $O(\sqrt{N/M})$ query for U_f.

Applications of Grover's algorithm

- $O^*(2^{n/2})$ algorithm for SAT.
- $O^*(2^{n/3})$ algorithm for the subset sum [Brassard et al. 1997].
- $O(1.728^n)$ algorithm for the travelling salesman problem [Ambainis et al. 2019].
- $O(1.914^n)$ algorithm for the graph coloring problem [Shimizu and Mori 2020].

Summary

- Grover's search solves the quantum searching problem in time $O(\sqrt{N})$.
- Grover's search is exactly optimal if $M = 1$ [Zalka 1999].
- For general M, Grover's search is exactly optimal [Ito and Mori 2021].

Assignments

1. Show two distinct eigenvalues and corresponding eigenvectors of the Grover operator $-WV_f$.