Grover's algorithm

Ryuhei Mori

Tokyo Institute of Technology

20, Nov., 2020

Searching problem

Searching problem:

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

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

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

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

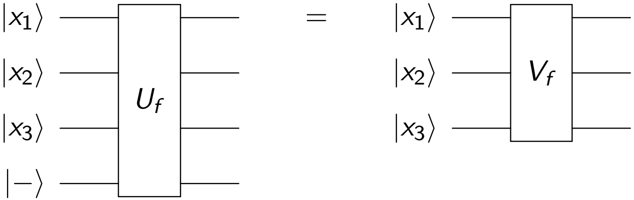
How many times, do we have to evaluate U_f ?

$O(\sqrt{N})$ 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 for some appropriately chosen k.

The two dimensional subspace

$$|s\rangle := \frac{1}{\sqrt{M}} \sum_{x:f(x)=1} |x\rangle$$

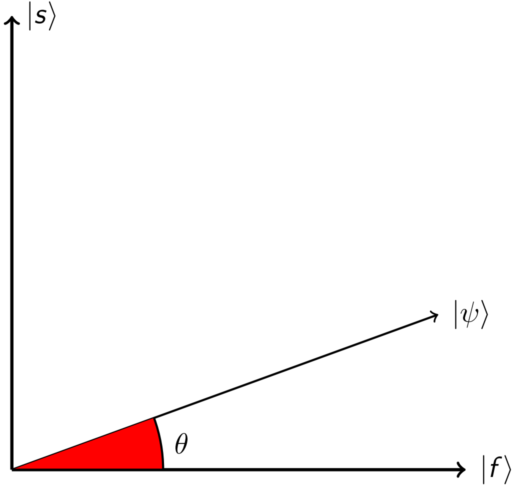
$$|f\rangle := \frac{1}{\sqrt{N-M}} \sum_{x:f(x)=0} |x\rangle \,.$$

Then,

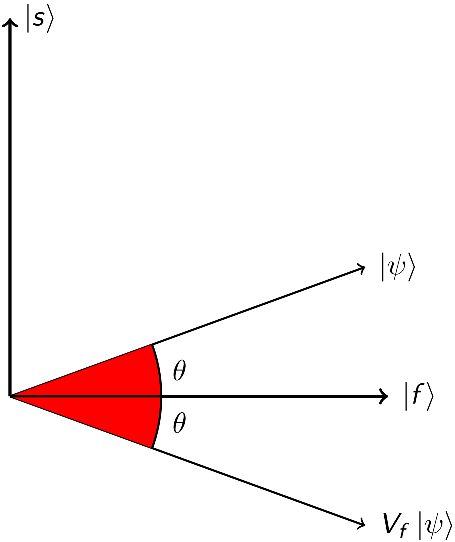
$$\begin{aligned}|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle &= \sqrt{\frac{M}{N}}\,|s\rangle + \sqrt{\frac{N-M}{N}}\,|f\rangle \\ &= \sin\theta\,|s\rangle + \cos\theta\,|f\rangle\end{aligned}$$

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

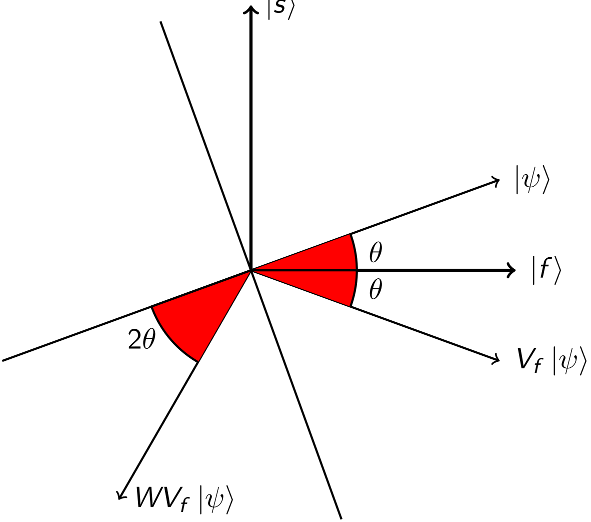
Analysis of Grover's algorithm



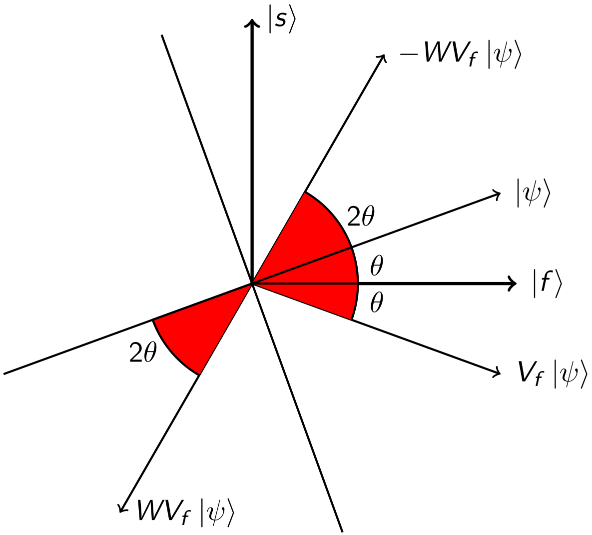
Analysis of Grover's algorithm



Analysis of Grover's algorithm



Analysis of Grover's algorithm



Analysis of Grover's algorithm

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

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 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 2019].

Optimality of Grover's search

Let $V_x := I - 2\left|x\right\rangle\left\langle x\right|$.

$$\begin{aligned}
\left|\psi_x^i\right\rangle &:= (U_k V_x U_{k-1} V_x \cdots U_{i+1} V_x)(U_i U_{i-1} \cdots U_1)\left|\psi_0\right\rangle \\
\left|\psi_x^0\right\rangle &= U_k V_x U_{k-1} V_x \cdots V_x U_1 V_x \left|\psi_0\right\rangle \\
\left|\psi_x^k\right\rangle &= U_k U_{k-1} \cdots U_1 \left|\psi_0\right\rangle
\end{aligned}$$

For any "distance" function D for $\left\{\left|a\right\rangle \in \mathbb{C}^N \mid \left\langle a|a\right\rangle = 1\right\}$,

$$\begin{aligned}
&\frac{1}{N}\sum_x D\left(\left|x\right\rangle, \left|\neq x\right\rangle\right) \\
&\leq \frac{1}{N}\sum_x \left(D\left(\left|x\right\rangle, \left|\psi_x^0\right\rangle\right) + \sum_{i=0}^{k-1} D\left(\left|\psi_x^i\right\rangle, \left|\psi_x^{i+1}\right\rangle\right) + D\left(\left|\psi_x^k\right\rangle, \left|\neq x\right\rangle\right)\right).
\end{aligned}$$

“Distance” function

Let

$$D(|a\rangle, |b\rangle) := \arccos |\langle a|b\rangle|.$$

For any normalized $|a\rangle$, $|b\rangle$, $|c\rangle$,

$$\begin{bmatrix} 1 & \langle a|b\rangle & \langle a|c\rangle \\ \langle b|a\rangle & 1 & \langle b|c\rangle \\ \langle c|a\rangle & \langle c|b\rangle & 1 \end{bmatrix} \succeq 0.$$

The determinant of this matrix is

$$\begin{aligned} &1 + \langle a|b\rangle \langle b|c\rangle \langle c|a\rangle + \langle a|c\rangle \langle b|a\rangle \langle c|b\rangle \\ &- \langle b|c\rangle \langle c|b\rangle - \langle a|c\rangle \langle c|a\rangle - \langle a|b\rangle \langle b|a\rangle \geq 0. \end{aligned}$$

The triangle inequality

$$
\begin{aligned}
& 1 + \langle a|b\rangle \langle b|c\rangle \langle c|a\rangle + \langle a|c\rangle \langle b|a\rangle \langle c|b\rangle \\
& - |\langle b|c\rangle|^2 - |\langle a|c\rangle|^2 - |\langle a|b\rangle|^2 \geq 0 \\
\implies \quad & 1 + |\langle a|b\rangle \langle b|c\rangle \langle c|a\rangle| + |\langle a|c\rangle \langle b|a\rangle \langle c|b\rangle| \\
& - |\langle b|c\rangle|^2 - |\langle a|c\rangle|^2 - |\langle a|b\rangle|^2 \geq 0 \\
\iff \quad & 1 + \cos(\theta_{ab})\cos(\theta_{bc})z + z\cos(\theta_{ab})\cos(\theta_{bc}) \\
& - \cos^2(\theta_{bc}) - z^2 - \cos^2(\theta_{ab}) \geq 0 \\
\iff \quad & z^2 - 2\cos(\theta_{ab})\cos(\theta_{bc})z \\
& + \cos^2(\theta_{bc}) + \cos^2(\theta_{ab}) - 1 \leq 0 \\
\iff \quad & (z - \cos(\theta_{ab})\cos(\theta_{bc}))^2 - \cos^2(\theta_{ab})\cos^2(\theta_{bc}) \\
& + \cos^2(\theta_{bc}) + \cos^2(\theta_{ab}) - 1 \leq 0 \\
\iff \quad & (z - \cos(\theta_{ab})\cos(\theta_{bc}))^2 \leq \left(1 - \cos^2(\theta_{ab})\right)\left(1 - \cos^2(\theta_{bc})\right)
\end{aligned}
$$

The triangle inequality

$$
\begin{aligned}
& (z - \cos(\theta_{ab})\cos(\theta_{bc}))^2 \leq \sin^2(\theta_{ab})\sin^2(\theta_{bc}) \\
\implies\quad & z \geq \cos(\theta_{ab})\cos(\theta_{bc}) - \sin(\theta_{ab})\sin(\theta_{bc}) \\
\iff\quad & z \geq \cos(\theta_{ab} + \theta_{bc}) \\
\iff\quad & \arccos(|\langle c|a\rangle|) \leq \theta_{ab} + \theta_{bc} \qquad \text{arccos is decreasing for } [-1, +1] \\
\iff\quad & \theta_{ca} \leq \theta_{ab} + \theta_{bc}
\end{aligned}
$$

Symmetrization

Let P_σ be a permutation matrix satisfying $P_\sigma |x\rangle = |\sigma(x)\rangle$ for a permutation σ on $\{1, 2, \dots, N\}$.

Symmetrization of algorithm U:

1. Choose a permutation σ with uniform probability.
2. Run U' that is U in which all V_x is replaced by $P_\sigma V_x {P_\sigma}^\dagger$. Note that $P_\sigma V_x {P_\sigma}^\dagger = V_{\sigma(x)}$
3. Measure the state $U' |\psi_0\rangle$, and obtain an outcome y. Output $\sigma^{-1}(y)$.

Let $p_{\text{succ}}(x)$ be the probability of success of the algorithm U if the oracle is V_x.

Then, the probability of success of the modified algorithm is $\frac{1}{N} \sum_z p_{\text{succ}}(z)$ regardless of the choice of the oracle V_x.

Inequalities

$$
\begin{aligned}
\frac{\pi}{2} &= \frac{1}{N}\sum_x D\left(|x\rangle, |\neq x\rangle\right) \\
&\leq \frac{1}{N}\sum_x \left(D\left(|x\rangle, |\psi_x^0\rangle\right) + \sum_{i=0}^{k-1} D\left(|\psi_x^i\rangle, |\psi_x^{i+1}\rangle\right) + D\left(|\psi_x^k\rangle, |\neq x\rangle\right) \right).
\end{aligned}
$$

$$
\frac{1}{N}\sum_x D\left(|x\rangle, |\psi_x^0\rangle\right) = \frac{1}{N}\sum_x \arccos\left(|\langle x|\psi_x^0\rangle|\right) = \arccos\left(\sqrt{p_{\mathrm{succ}}}\right).
$$

$$
\frac{1}{N}\sum_x D\left(|\psi_x^k\rangle, |\neq x\rangle\right) = \frac{1}{N}\sum_x \arccos\left(|\langle \psi_x^k| \neq x\rangle|\right) = \arccos\left(\sqrt{1-\frac{1}{N}}\right).
$$

Inequalities

$$
\begin{aligned}
\frac{1}{N}\sum_x D\left(\left|\psi_x^i\right\rangle, \left|\psi_x^{i+1}\right\rangle\right) &= \frac{1}{N}\sum_x \arccos\left(\left|\left\langle \psi_x^i \middle| \psi_x^{i+1}\right\rangle\right|\right) \\
= \frac{1}{N}\sum_x \arccos\left(\left|\left\langle\varphi\right| V_x \left|\varphi\right\rangle\right|\right) &\le \arccos\left(\frac{1}{N}\sum_x \left|\left\langle\varphi\right| V_x \left|\varphi\right\rangle\right|\right) \\
\le \arccos\left(\left|\frac{1}{N}\sum_x \left\langle\varphi\right| V_x \left|\varphi\right\rangle\right|\right) &= \arccos\left(\left|\left\langle\varphi\right|\left(1-\frac{2}{N}\right) I \left|\varphi\right\rangle\right|\right) \\
&= \arccos\left(1-\frac{2}{N}\right)
\end{aligned}
$$

Put everything together

$$\frac{\pi}{2} = \frac{1}{N}\sum_x D\left(|x\rangle, |\neq x\rangle\right)$$

$$\leq \frac{1}{N}\sum_x \left(D\left(|x\rangle, |\psi_x^0\rangle\right) + \sum_{i=0}^{k-1} D\left(|\psi_x^i\rangle, |\psi_x^{i+1}\rangle\right) + D\left(|\psi_x^k\rangle, |\neq x\rangle\right)\right)$$

$$\leq \arccos\left(\sqrt{p_{\text{succ}}}\right) + k \arccos\left(1 - \frac{2}{N}\right) + \arccos\left(\sqrt{1 - \frac{1}{N}}\right)$$

Since $\theta = \arccos\left(\sqrt{\frac{N-1}{N}}\right)$,

$$\frac{\pi}{2} \leq \arccos\left(\sqrt{p_{\text{succ}}}\right) + 2k\theta + \theta$$

$$\iff \cos\left(\frac{\pi}{2} - (2k+1)\theta\right) \geq \sqrt{p_{\text{succ}}} \qquad \text{if } (2k+1)\theta \leq \frac{\pi}{2}$$

$$\iff \sin^2\left((2k+1)\theta\right) \geq p_{\text{succ}}.$$

[Zalka 1999]

Summary

- Grover's search solves the quantum searching problem in time $O(\sqrt{N})$.
- Grover's search is exactly optimal if $M = 1$.
- For general M, Grover's search is asymptotically optimal.