

Grover's algorithm

Ryuhei Mori

Tokyo Institute of Technology

16, Nov., 2021

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

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

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

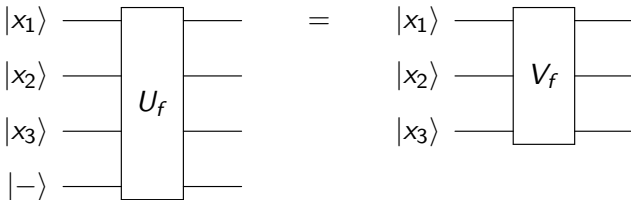
How many times, do we have to evaluate U_f ?

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

Unitary matrix for Grover's algorithm

Another unitary

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



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

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

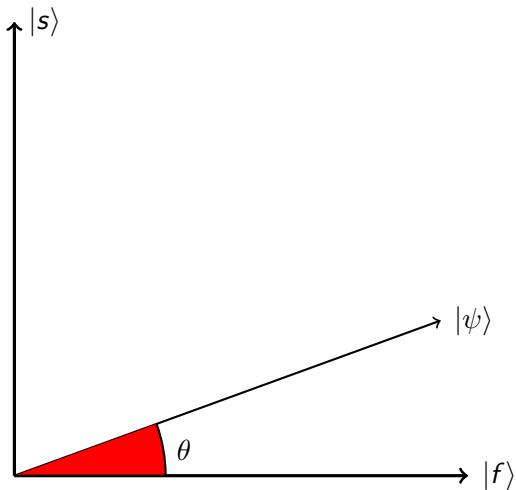
$$|s\rangle := \frac{1}{\sqrt{M}} \sum_{x:f(x)=1} |x\rangle$$
$$|f\rangle := \frac{1}{\sqrt{N-M}} \sum_{x:f(x)=0} |x\rangle.$$

Then,

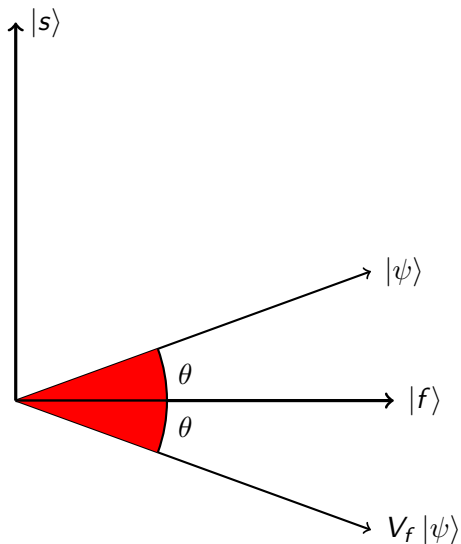
$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{N}} \sum_{x=1}^N |x\rangle = \sqrt{\frac{M}{N}} |s\rangle + \sqrt{\frac{N-M}{N}} |f\rangle \\ &= \sin \theta |s\rangle + \cos \theta |f\rangle \end{aligned}$$

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

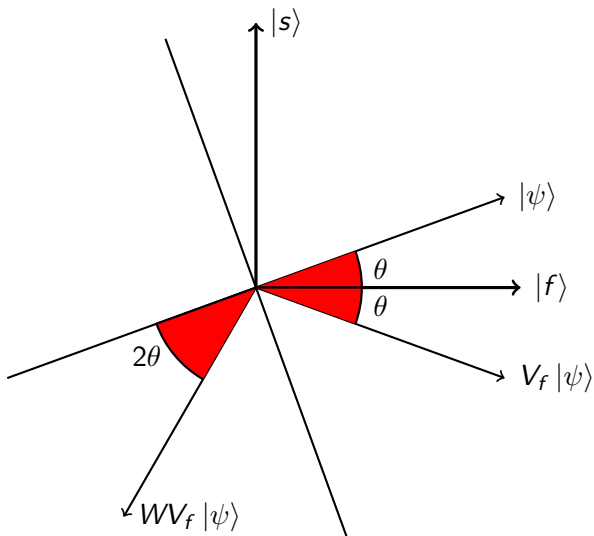
Analysis of Grover's algorithm



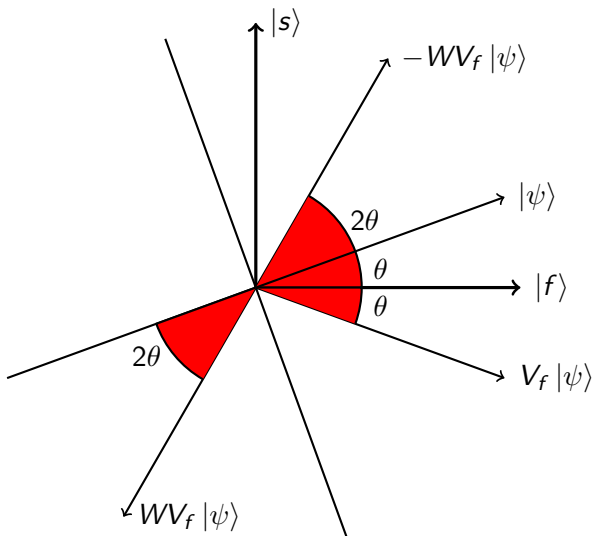
Analysis of Grover's algorithm



Analysis of Grover's algorithm



Analysis of Grover's algorithm



Analysis of Grover's algorithm

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

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 algorithm

[Boyer, Brassard, Høyer, and Tapp 1998]

- 1 Initialize $m = 1$ and set $\lambda = 8/7$.
- 2 Choose an integer j uniformly from $0, 1, \dots, m$.
- 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 step 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].

Optimality of Grover's search

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

$$|\psi_x^i\rangle := (U_k V_x U_{k-1} V_x \cdots U_{i+1} V_x)(U_i U_{i-1} \cdots U_1) |\psi_0\rangle$$

$$|\psi_x^0\rangle = U_k V_x U_{k-1} V_x \cdots V_x U_1 V_x |\psi_0\rangle$$

$$|\psi_x^k\rangle = U_k U_{k-1} \cdots U_1 |\psi_0\rangle$$

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

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

“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

$$1 + \langle a|b \rangle \langle b|c \rangle \langle c|a \rangle + \langle a|c \rangle \langle b|a \rangle \langle c|b \rangle$$

$$- |\langle b|c \rangle|^2 - |\langle a|c \rangle|^2 - |\langle a|b \rangle|^2 \geq 0$$

$$\implies 1 + |\langle a|b \rangle \langle b|c \rangle \langle c|a \rangle| + |\langle a|c \rangle \langle b|a \rangle \langle c|b \rangle|$$

$$- |\langle b|c \rangle|^2 - |\langle a|c \rangle|^2 - |\langle a|b \rangle|^2 \geq 0$$

$$\iff 1 + \cos(\theta_{ab}) \cos(\theta_{bc}) z + z \cos(\theta_{ab}) \cos(\theta_{bc})$$

$$- \cos^2(\theta_{bc}) - z^2 - \cos^2(\theta_{ab}) \geq 0$$

$$\iff z^2 - 2 \cos(\theta_{ab}) \cos(\theta_{bc}) z$$

$$+ \cos^2(\theta_{bc}) + \cos^2(\theta_{ab}) - 1 \leq 0$$

$$\iff (z - \cos(\theta_{ab}) \cos(\theta_{bc}))^2 - \cos^2(\theta_{ab}) \cos^2(\theta_{bc})$$

$$+ \cos^2(\theta_{bc}) + \cos^2(\theta_{ab}) - 1 \leq 0$$

$$\iff (z - \cos(\theta_{ab}) \cos(\theta_{bc}))^2 \leq (1 - \cos^2(\theta_{ab})) (1 - \cos^2(\theta_{bc}))$$

The triangle inequality

$$(z - \cos(\theta_{ab}) \cos(\theta_{bc}))^2 \leq \sin^2(\theta_{ab}) \sin^2(\theta_{bc})$$

$$\implies z \geq \cos(\theta_{ab}) \cos(\theta_{bc}) - \sin(\theta_{ab}) \sin(\theta_{bc})$$

$$\iff z \geq \cos(\theta_{ab} + \theta_{bc})$$

$$\iff \arccos(|\langle c|a \rangle|) \leq \theta_{ab} + \theta_{bc} \quad \arccos \text{ is decreasing for } [-1, +1]$$

$$\iff \theta_{ca} \leq \theta_{ab} + \theta_{bc}$$

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_σ 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 $U_\sigma |\psi_0\rangle$, 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 U_σ is $p_{\text{succ}}(\sigma(x))$. The probability of success of the symmetrized algorithm is $\frac{1}{N!} \sum_\sigma p_{\text{succ}}(\sigma(x)) = \frac{1}{N} \sum_z p_{\text{succ}}(z)$ regardless of the choice of the oracle V_x .

Inequalities

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

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

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

Inequalities

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

Put everything together

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

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

$$\begin{aligned}\frac{\pi}{2} &\leq \arccos(\sqrt{p_{\text{succ}}}) + 2k\theta + \theta \\ \iff \cos\left(\frac{\pi}{2} - (2k+1)\theta\right) &\geq \sqrt{p_{\text{succ}}} \quad \text{if } (2k+1)\theta \leq \frac{\pi}{2} \\ \iff \sin^2((2k+1)\theta) &\geq p_{\text{succ}}.\end{aligned}$$

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 **asymptotically optimal** [Ito and Mori 2021].

Assignments

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