University of Jyväskylä - Course TIEJ6003

Introduction to Quantum Computing

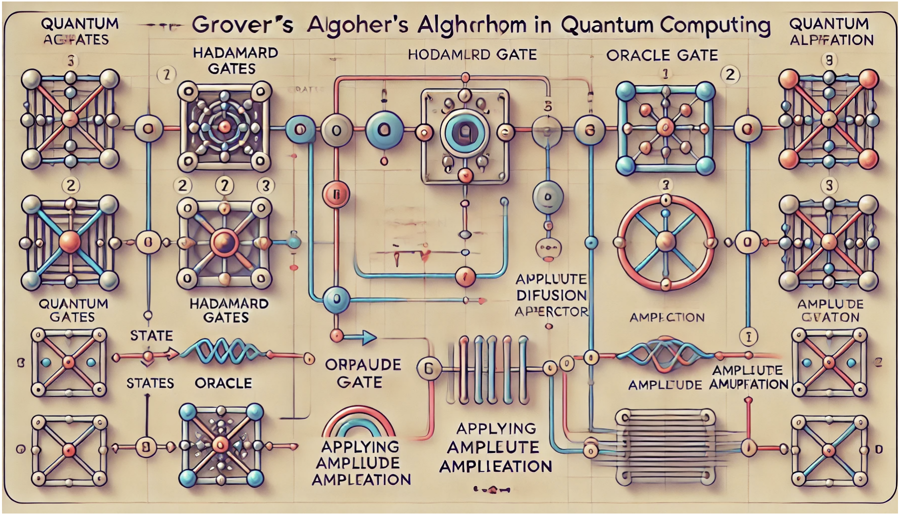
Day-05a

Prof. Ofer Shir
oshir@alumni.Princeton.EDU

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Summer 2024
Jyväskylä, Finland

Grover Search Algorithm



the challenge: unstructured search

We would like to devise a method to locate known objects (‘needles’) in a large unordered set (‘haystack’) of N objects.

Suppose that f is a function from $\{0, 1, \ldots, N-1\} \to \{0, 1\}$, and the target is to locate some x for which $f(x) = 1$.
For simplicity, assume a single *winner* w for which $f(w) = 1$.

Evaluating $f(x)$ for random x will locate w in an expected $N/2$ steps (alternatively, $\mathcal{O}(\frac{N}{2})$ steps to find the object with probability 50%).

Grover developed a quantum algorithm to this end and published it in 1996. His method achieves a success-probability greater than 50% in $\mathcal{O}(\sqrt{N})$ steps!

introducing the oracle

We assume that we are provided with a black-box that has the ability to *recognize* solutions to the problem.

This assumption is not as strong as it may sound at first - there are many black-box problems in reality whose solutions may be recognized once located. We shall call it the *oracle*.

Intuitively, the oracle enables us to define a Hilbert subspace of winners versus non-winners, and to define a rotation in this subspace toward the winners.

It will be beneficial to work with the uniform superposition state $|h\rangle = \frac{1}{\sqrt{N}} \sum_{0 \leq x < N} |x\rangle$ (prepared by $H^{\otimes n} |0\rangle^{\otimes n}$).
Then, starting with $|h\rangle$, we will repeatedly apply rotations for T iterations and measure!

the oracle formalized

The oracle's recognition is signalled via a qubit $|q\rangle$, and altogether the oracle's operation may be formally described as follows:

$$\mathcal{U}_{\text{oracle}} |x\rangle |q\rangle = |x\rangle |q \oplus f(x)\rangle \,. \tag{1}$$

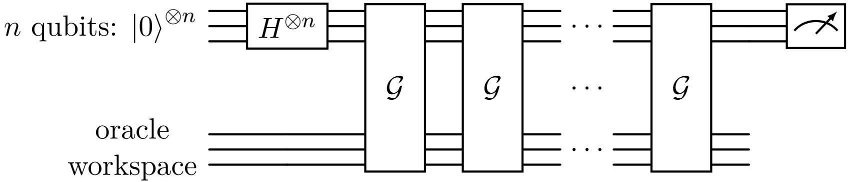
Importantly, it pays off to apply this operator on the superposition state $(|0\rangle - |1\rangle)/\sqrt{2}$ (similar to Deutsch-Jozsa):

$$\mathcal{U}_{\text{oracle}} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

In practice, the oracle *marks* the solution by *shifting its phase*.

Given an unstructured search with M solutions, it turns out that a solution can be located by calling the oracle $\mathcal{O}(\sqrt{N/M})$ times.

quantum search: schematic circuit



The Grover operator $\mathcal{G}$ represents an iteration, which subsequently applies the Oracle followed by the so-called Diffusion operator $\mathcal{D}$:

$$\mathcal{G} := \mathcal{U}_{\text{oracle}}\mathcal{D}$$

the Grover iteration

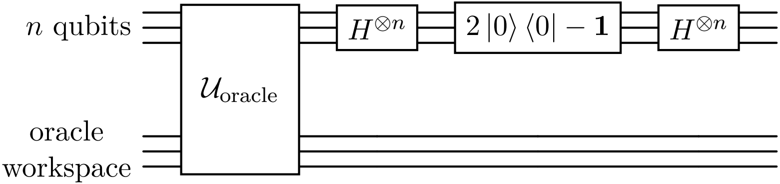
The Grover operator $\mathcal{G}$ is applied repeatedly as a subroutine in each iteration. It can be broken down to four steps:

1. Call the oracle $\mathcal{U}_{\text{oracle}}$
2. Apply the Hadamard transform $H^{\otimes n}$
3. Conditionally apply phase shift:
   if $x > 0$ **then** $|x\rangle \to -|x\rangle$
   else $|0\rangle \to |0\rangle$
4. Apply the Hadamard transform $H^{\otimes n}$

The combined effect of steps 2+3+4 is the reflection on the uniform superposition $|h\rangle$ (the Diffusion operator $\mathcal{D}$):

$$H^{\otimes n}\left(2\,|0\rangle^{\otimes n}\langle 0|^{\otimes n} - I^{\otimes n}\right)H^{\otimes n} = 2\,|h\rangle\langle h| - I^{\otimes n} = \mathcal{D}$$

Grover iteration: concrete circuit per $\mathcal{G}$



$$
\begin{aligned}
\mathcal{G} &:= \mathcal{D}\,\mathcal{U}_{\text{oracle}} \\
\mathcal{U}_{\text{oracle}} &:= \mathbf{1} - 2\,|w\rangle\,\langle w| \\
\mathcal{D} &:= 2\,|h\rangle\,\langle h| - \mathbf{1}
\end{aligned}
$$

subspace framework

Let S denote the set of objects we are searching for, and let $M \geq 1$ be its cardinality. S is the *solution set* ("*winners*"), and its elements are called the *solutions*.

We denote the set of objects that are not a solution ("*non-winners*") by

$$S^{\perp} := \{0, 1, \ldots, N-1\} \setminus S$$

and accordingly construct two vectors:

$$|\Psi_S\rangle := \frac{1}{\sqrt{M}} \sum_{x \in S} |x\rangle \qquad |\Psi_{S^{\perp}}\rangle := \frac{1}{\sqrt{N-M}} \sum_{x \in S^{\perp}} |x\rangle \tag{2}$$

projections

By considering the two projection operators onto the two subspaces

$$P_S := \sum_{x \in S} |x\rangle \langle x| \qquad P_{S^\perp} := \sum_{x \in S^\perp} |x\rangle \langle x| = \mathbf{1} - P_S, \tag{3}$$

and by recalling that $S \cup S^\perp = \{0, 1, \ldots, N-1\}$, every state can be expanded in the computational basis as follows

$$|\psi\rangle = (P_S + P_{S^\perp}) |\psi\rangle = \sum_{x \in S} \psi_x |x\rangle + \sum_{x \in S^\perp} \psi_x |x\rangle = \alpha |\Psi_S\rangle + \beta |\Psi_{S^\perp}\rangle \tag{4}$$

In particular, the uniform superposition state $|h\rangle$ can be expanded as:

$$|h\rangle = \sqrt{\frac{M}{N}} |\Psi_S\rangle + \sqrt{\frac{N-M}{N}} |\Psi_{S^\perp}\rangle \tag{5}$$

interpretation: reflections

By observing the 2D subspace spanned by $|\Psi_S\rangle$ (“the good”) and $|\Psi_{S^\perp}\rangle$ (“the bad”), Grover’s iteration may be interpreted as two *reflection* operations when starting with $|h\rangle$:

1. $\mathcal{U}_{\text{oracle}}$ performs a *reflection* about the vector $|\Psi_{S^\perp}\rangle$.
2. $\mathcal{D}$ performs a *reflection* about the vector $|h\rangle$.

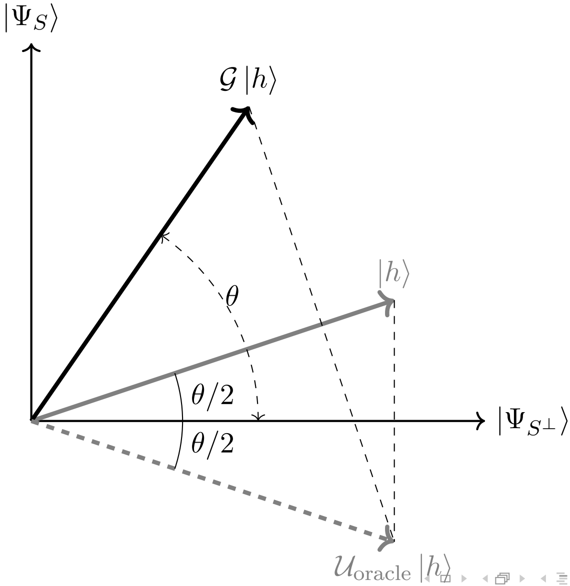
Importantly, the repeated application of $\mathcal{G}$ always keeps the states in the plane defined by $|\Psi_S\rangle$ and $|\Psi_{S^\perp}\rangle$.

Altogether, $\mathcal{G}$ yields a rotation defined as

$$\mathcal{G} := \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, \tag{6}$$

with θ satisfying $\sin\theta = 2\sqrt{M(N-M)}/N$.

geometric visualization



Grover formalized per $M = 1$

Inputs: (1) a black-box oracle $\mathcal{U}_{\text{oracle}}$ which performs the operation $\mathcal{U}_{\text{oracle}} \left|x\right\rangle \left|q\right\rangle = \left|x\right\rangle \left|q \oplus f(x)\right\rangle$.
(2) $(n+1)$ qubits in the state $\left|0\right\rangle$.
Outputs: x_0.
Runtime: $\mathcal{O}(\sqrt{2^n})$ operations. Succeeds with probability $\mathcal{O}(1)$.

Procedure:
$$
\begin{aligned}
&\left|\psi_0\right\rangle = \left|0\right\rangle^{\otimes n} \left|0\right\rangle \\
&\left|\psi_1\right\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \left|x\right\rangle \left[\frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}}\right] \\
&\to \left[\mathcal{D}\mathcal{U}_{\text{oracle}}\right]^T \left|\psi_1\right\rangle \approx \left|x_0\right\rangle \left[\frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}}\right] \\
&\to x_0
\end{aligned}
$$

Grover: complexity and aftermath

Now that the search is reduced to rotations in the plane of $\{|\Psi_S\rangle, |\Psi_{S^\perp}\rangle\}$, the algorithm's complexity is reduced to the question

"*how many radians are needed to approach* $|\Psi_S\rangle$?"

Given the starting point $|h\rangle = \sqrt{\frac{M}{N}}\,|\Psi_S\rangle + \sqrt{\frac{N-M}{N}}\,|\Psi_{S^\perp}\rangle$, rotating it through $\arccos(\sqrt{M/N})$ radians will drive the system to $|\Psi_S\rangle$:

$$T = \texttt{round}\left(\frac{\arccos(\sqrt{M/N})}{\theta}\right) \leq \left\lceil \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rceil . \tag{7}$$

$\mathcal{O}(\sqrt{N/M})$ Grover iterations (and thus oracle calls) are required, versus $\mathcal{O}(N/M)$ oracle calls that are required classically.