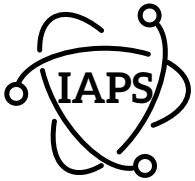
Lecture 21

Grover search algorithm

of the course "Fundamentals of Quantum Computing"

(by  *and* QUANTERALL*)*

Stoyan Mishev



INSTITUTE *for* ADVANCED
PHYSICAL STUDIES

November 18, 2022

Plan

Essence

Words as point in Hilbert space

Steps of the Grover search algorithm

Qiskit notebook

Essence

Lov Kumar Grover

L. Grover, Phys. Rev. Lett. 79(2), 325 (1997)

Completes a search in $\sim \sqrt{N}$ steps (with 50% probability)

Essence

Lov Kumar Grover

L. Grover, Phys. Rev. Lett. 79(2), 325 (1997)

Completes a search in $\sim \sqrt{N}$ steps (with 50% probability) as opposed to the classical $\sim N/2$ steps.

Essence

Lov Kumar Grover

L. Grover, Phys. Rev. Lett. 79(2), 325 (1997)

Completes a search in $\sim \sqrt{N}$ steps (with 50% probability) as opposed to the classical $\sim N/2$ steps.

The objects (haystack) must be represented as points in a Hilber space. The vectors of the objects which we try to find span a subspace in this space.

Essence

Lov Kumar Grover

L. Grover, Phys. Rev. Lett. 79(2), 325 (1997)

Completes a search in $\sim \sqrt{N}$ steps (with 50% probability) as opposed to the classical $\sim N/2$ steps.

The objects (haystack) must be represented as points in a Hilber space. The vectors of the objects which we try to find span a subspace in this space.

The Grover algorithm constructs operators that transform a given initial state into a state which has a maximal component in the subspace of desired objects (*amplitude amplification*).

Definition 6.22 Let S denote the set of objects we are searching for, and let $m \geq 1$ be the cardinality of this set. The set S is called solution set, and we call its elements solutions. For the algorithm to search an $x \in \mathrm{S} \subset \{0, \ldots, N-1\}$, where $N = 2^n$, we define the input and output register as $\mathbb{H}^{I/O} = \mathbb{H}^{\otimes n}$. Furthermore, we denote the set of objects that are not a solution by

Definition 6.22 Let S denote the set of objects we are searching for, and let $m \geq 1$ be the cardinality of this set. The set S is called solution set, and we call its elements solutions. For the algorithm to search an $x \in \mathrm{S} \subset \{0, \ldots, N-1\}$, where $N = 2^n$, we define the input and output register as $\mathbb{H}^{I/O} = ¶\mathbb{H}^{\otimes n}$. Furthermore, we denote the set of objects that are not a solution by

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

and define the subspaces

$$\mathbb{H}_{\mathrm{S}} := \mathrm{Span}\left\{ |x\rangle \,\middle|\, x \in \mathrm{S} \right\} \subset \mathbb{H}^{I/0}$$
$$\mathbb{H}_{\mathrm{S}^{\perp}} := \mathrm{Span}\left\{ |x\rangle \,\middle|\, x \in \mathrm{S}^{\perp} \right\} \subset \mathbb{H}^{I/0}$$

Definition 6.22 Let S denote the set of objects we are searching for, and let $m \geq 1$ be the cardinality of this set. The set S is called solution set, and we call its elements solutions. For the algorithm to search an $x \in \mathrm{S} \subset \{0,\ldots,N-1\}$, where $N = 2^n$, we define the input and output register as $\mathbb{H}^{I/O} = ¶\mathbb{H}^{\otimes n}$. Furthermore, we denote the set of objects that are not a solution by

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

and define the subspaces

$$\mathbb{H}_{\mathrm{S}} := \mathrm{Span}\left\{|x\rangle \,\middle|\, x \in \mathrm{S}\right\} \subset \mathbb{H}^{I/0}$$
$$\mathbb{H}_{\mathrm{S}^{\perp}} := \mathrm{Span}\left\{|x\rangle \,\middle|\, x \in \mathrm{S}^{\perp}\right\} \subset \mathbb{H}^{I/0}$$

and the operators

$$P_{\mathrm{S}} := \sum_{x \in \mathrm{S}} |x\rangle\langle x|$$
$$P_{\mathrm{S}^{\perp}} := \sum_{x \in \mathrm{S}^{\perp}} |x\rangle\langle x| = \mathbf{1}^{\otimes n} - P_{\mathrm{S}}$$

on $\mathbb{H}^{I/O}$ as well as the vectors

Definition 6.22 Let S denote the set of objects we are searching for, and let $m \geq 1$ be the cardinality of this set. The set S is called solution set, and we call its elements solutions. For the algorithm to search an $x \in \mathrm{S} \subset \{0,\ldots,N-1\}$, where $N = 2^n$, we define the input and output register as $\mathbb{H}^{I/O} = \mathbb{H}^{\otimes n}$. Furthermore, we denote the set of objects that are not a solution by

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

and define the subspaces

$$\mathbb{H}_{\mathrm{S}} := \mathrm{Span}\left\{|x\rangle \,\middle|\, x \in \mathrm{S}\right\} \subset \mathbb{H}^{I/0}$$
$$\mathbb{H}_{\mathrm{S}^{\perp}} := \mathrm{Span}\left\{|x\rangle \,\middle|\, x \in \mathrm{S}^{\perp}\right\} \subset \mathbb{H}^{I/0}$$

and the operators

$$P_{\mathrm{S}} := \sum_{x \in \mathrm{S}} |x\rangle\langle x|$$
$$P_{\mathrm{S}^{\perp}} := \sum_{x \in \mathrm{S}^{\perp}} |x\rangle\langle x| = \mathbf{1}^{\otimes n} - P_{\mathrm{S}}$$

on $\mathbb{H}^{I/O}$ as well as the vectors

$$|\Psi_{\mathrm{S}}\rangle := \frac{1}{\sqrt{m}} \sum_{x \in \mathrm{S}} |x\rangle$$
$$|\Psi_{\mathrm{S}^{\perp}}\rangle := \frac{1}{\sqrt{N-m}} \sum_{x \in \mathrm{S}^{\perp}} |x\rangle$$

Every state $|\Psi\rangle \in H^{I/O}$ can be decomposed as:

$$|\Psi\rangle = \left(P_{S^\perp} + P_S\right)|\Psi\rangle = \sum_{x \in S^\perp} \Psi_x |x\rangle + \sum_{x \in S} \Psi_x |x\rangle$$

Remember, measuring the state $|\Psi\rangle$ means:

Definition 5.35 Let $n \in \mathbb{N}$ and for $j \in \{0,\dots,n-1\}$ and $\alpha \in \{0,\dots,3\}$ (or, equivalently, $\alpha \in \{0,x,y,z\}$) define

$$\Sigma_\alpha^j := \mathbf{1}^{\otimes n-1-j} \otimes \sigma_\alpha \otimes \mathbf{1}^{\otimes j} \quad \in \mathrm{B}_{\mathrm{sa}}\left(¶\mathbb{H}^{\otimes n}\right),$$

where the σ_α are as in Definition 2.21. The **observation of a state in the quantum register** $¶\mathbb{H}^{\otimes n}$ is defined as the measurement of all compatible observables

$$\Sigma_z^j = \mathbf{1}^{\otimes n-1-j} \otimes \sigma_z \otimes \mathbf{1}^{\otimes j}$$

for $j \in \{0,\dots,n-1\}$ in the state of the quantum register. Such an observation is also called **read-out** or **measurement** of the register.

The goal of the algorithm to create states $|\Psi\rangle$ for which the probability to observe an $x \in S$ is maximized. This is accomplished by starting from an initial state $|\Psi_0\rangle$ and by applying suitable transformations which increase the component in H_S.

$$\mathbf{P}\left\{\begin{array}{l}\text{Observation of } |\Psi\rangle \text{ projects} \\ \text{onto a state } |x\rangle \text{ with } x \in \mathrm{S}\end{array}\right\} \underbrace{=}_{(2.62)} ||P_{\mathrm{S}}|\Psi\rangle||^2 \underbrace{=}_{(6.137)} \left|\left|\sum_{x\in\mathrm{S}} \Psi_x |x\rangle\right|\right|^2$$
$$\underbrace{=}_{(2.14)} \sum_{x\in\mathrm{S}} |\Psi_x|^2 .$$

Decision if a state is a solution

$$g : \{0,\ldots,N-1\} \longrightarrow \{0,1\}$$
$$x \longmapsto g(x) := \begin{cases} 0 & \text{if } x \in \mathrm{S}^{\perp} \\ 1 & \text{if } x \in \mathrm{S} \end{cases}$$

$$\widehat{U}_g\left(|x\rangle \otimes |y\rangle\right) := |x\rangle \otimes |y \boxplus g(x)\rangle$$

where $|y\rangle$ belongs to an auxiliary register H^W.

Reminder

$$|a \boxplus b\rangle := \bigotimes_{j=m-1}^{0} |a_j \overset{2}{\oplus} b_j\rangle$$

$$u \overset{2}{\oplus} v := (u+v) \mod 2$$

Lemma 6.24 *For the oracle U_g and the state*

$$|\omega_i\rangle = |\omega_f\rangle = |-\rangle := \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

in the auxiliary register $\mathbb{H}^W$ one has for arbitrary $|\Psi\rangle \in \mathbb{H}^{I/O}$

$$\widehat{U}_g\,(|\Psi\rangle \otimes |-\rangle) = (R_{\mathrm{S}^\perp}|\Psi\rangle) \otimes |-\rangle\,,$$

where

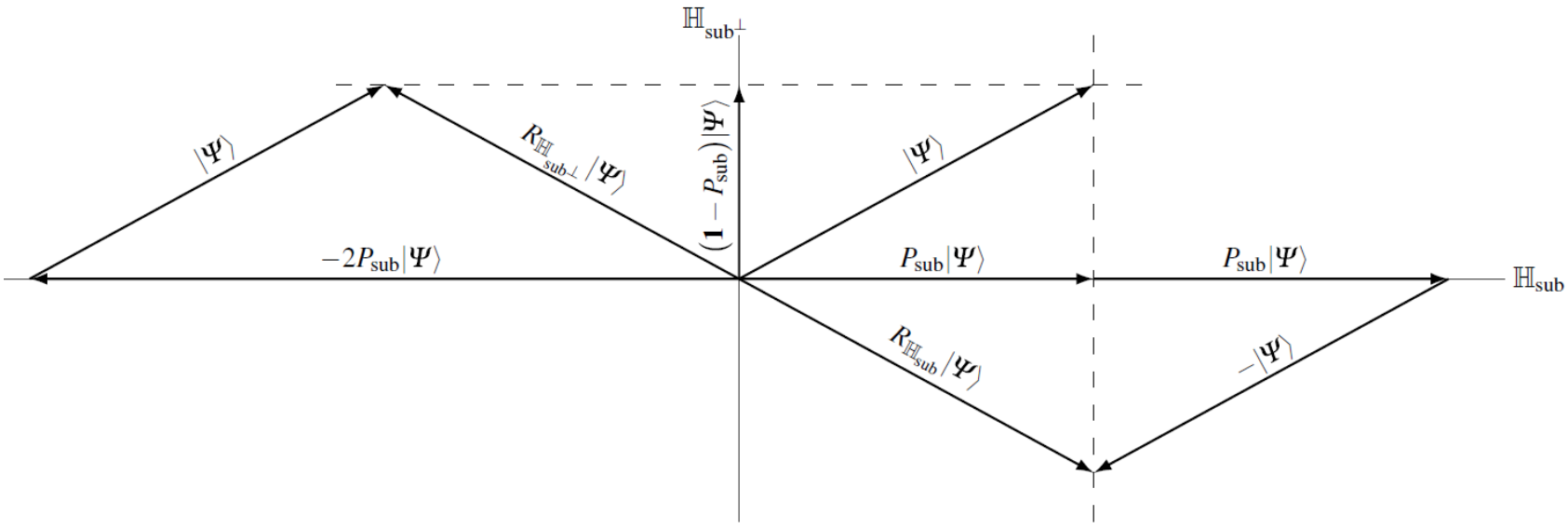
$$\begin{aligned} R_{\mathrm{S}^\perp}|\Psi\rangle &= \sum_{x\in \mathrm{S}^\perp} \Psi_x|x\rangle - \sum_{x\in \mathrm{S}} \Psi_x|x\rangle \\ &= (\mathbf{1}^{\otimes n} - 2P_{\mathrm{S}})|\Psi\rangle\,. \end{aligned}$$

$R_{S^\perp}$ can be viewed as reflection about $H_{S^\perp}$:

Definition 6.25 Let $\mathbb{H}_{\mathrm{sub}}$ be a subspace of the HILBERT space $\mathbb{H}$, and let P_{sub} be the projection onto this subspace. The **reflection about the subspace** $\mathbb{H}_{\mathrm{sub}}$ is defined as the operator

$$R_{\mathrm{sub}} := 2P_{\mathrm{sub}} - \mathbf{1}\,. \tag{6.147}$$

If the subspace is one-dimensional and spanned by a $|\Psi\rangle \in \mathbb{H}$, we simply write R_Ψ and call this a reflection about $|\Psi\rangle$.


$\mathbb{H}_{\text{sub}^\perp}$
$|\Psi\rangle$
$R_{\mathbb{H}_{\text{sub}^\perp}}|\Psi\rangle$
$(\mathbf{1}-P_{\text{sub}})|\Psi\rangle$
$|\Psi\rangle$
$-2P_{\text{sub}}|\Psi\rangle$
$P_{\text{sub}}|\Psi\rangle$
$P_{\text{sub}}|\Psi\rangle$
$\mathbb{H}_{\text{sub}}$
$R_{\mathbb{H}_{\text{sub}}}|\Psi\rangle$
$-|\Psi\rangle$

Definition 6.26 Let S be the solution set with cardinality $m \geq 1$. For the algorithm to search for an $x \in \mathrm{S} \subset \{0,\ldots,N-1\}$, where $N = 2^n$, we define the initial state in the input/output register as

$$|\Psi_0\rangle := \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \in \mathbb{H}^{I/O}. \tag{6.148}$$

Moreover, we define the angle

$$\theta_0 := \arcsin\left(\sqrt{\frac{m}{N}}\right) \in \left[0, \frac{\pi}{2}\right], \tag{6.149}$$

and with the help of $|\Psi_0\rangle$ we define the operator

$$R_{\Psi_0} = 2|\Psi_0\rangle\langle\Psi_0| - \mathbf{1}^{\otimes n} \tag{6.150}$$

on $\mathbb{H}^{I/O}$ as well as the initial state in the composite system

$$|\widehat{\Psi_0}\rangle := |\Psi_0\rangle \otimes |-\rangle \in \mathbb{H}^{I/O} \otimes \mathbb{H}^{W}. \tag{6.151}$$

$$|\Psi_0\rangle = \cos\theta_0 |\Psi_{\mathrm{S}^\perp}\rangle + \sin\theta_0 |\Psi_{\mathrm{S}}\rangle$$

Definition 6.27 The **GROVER iteration** is defined as the operator

$$\widehat{G} := \left(R_{\Psi_0} \otimes \mathbf{1}\right) \widehat{U}_g$$

on $\mathbb{H}^{I/O} \otimes \mathbb{H}^W$.

As we will now show, the GROVER iteration G transforms separable states in $\mathbb{H}^{I/O} \otimes \mathbb{H}^W$ of the form $|\widehat{\Psi}_j\rangle = |\Psi_j\rangle \otimes |-\rangle$ to separable states $|\widehat{\Psi}_{j+1}\rangle = |\Psi_{j+1}\rangle \otimes |-\rangle$ of a similar form. We will see that in the input/output register $\mathbb{H}^{I/O}$ an application of $\widehat{G}$ can then be viewed as *a rotation of $2\theta_0$ in $\mathbb{H}^{I/O}$ in the direction of $|\Psi_S\rangle$*.

Proposition 6.28 *For $j \in \mathbb{N}_0$ let*

$$|\widehat{\Psi}_j\rangle := \widehat{G}^j |\widehat{\Psi}_0\rangle .$$

Then we have for all $j \in \mathbb{N}_0$

$$|\widehat{\Psi}_j\rangle = |\Psi_j\rangle \otimes |-\rangle$$

with $|\Psi_j\rangle \in \mathbb{H}^{I/O}$ and

$$|\Psi_j\rangle = \cos\theta_j |\Psi_{S^\perp}\rangle + \sin\theta_j |\Psi_S\rangle ,$$

where

$$\theta_j = (2j+1)\theta_0 .$$

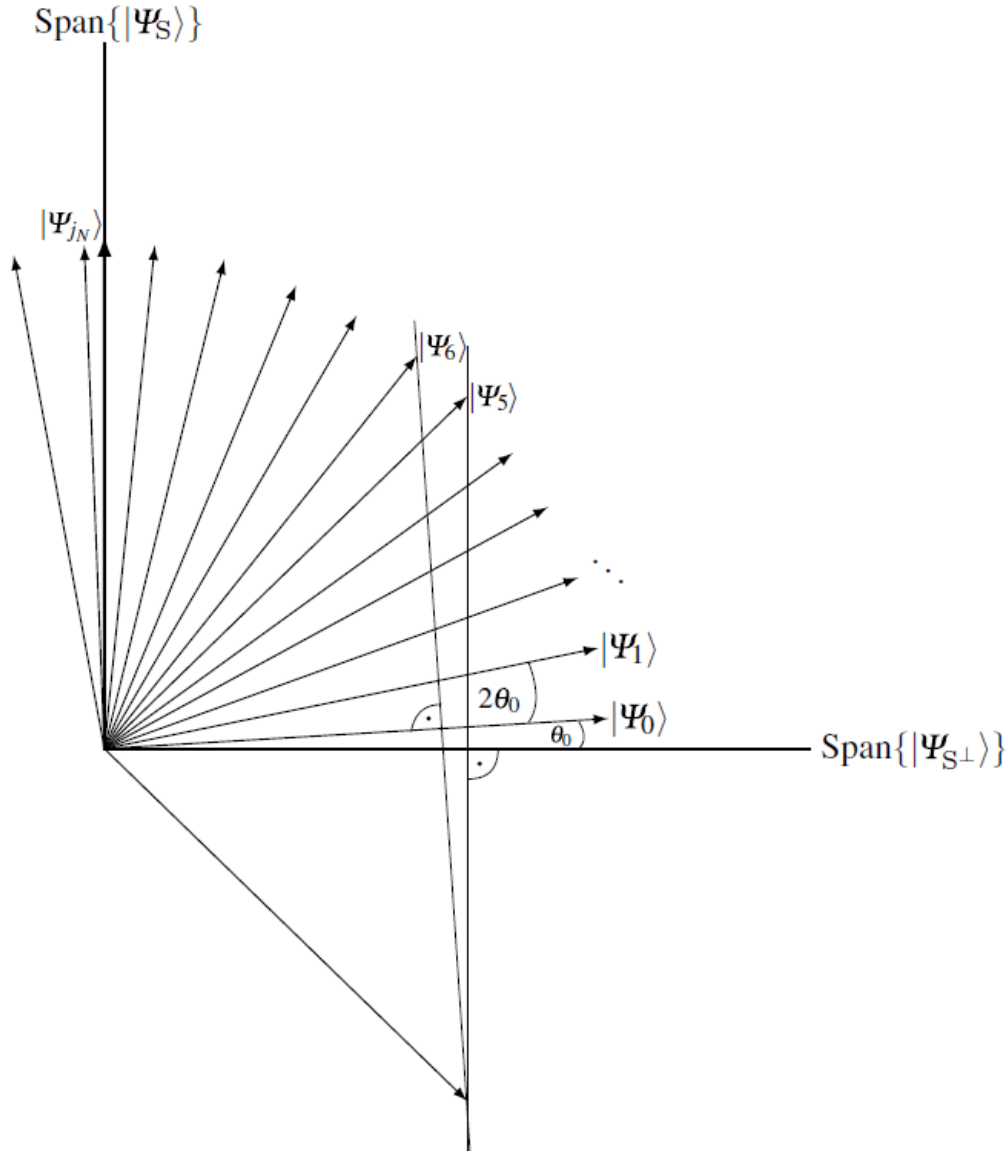


Fig. 6.6 Geometry of the GROVER iteration in the input/output register with $m = 5, N = 2^{10}$ and $j_N = 11$. In the two-dimensional subspace $\mathrm{Span}\{|\Psi_{\mathrm{S}^\perp}\rangle, |\Psi_{\mathrm{S}}\rangle\}$ the initial state $|\Psi_0\rangle$ is rotated towards $|\Psi_{\mathrm{S}}\rangle$. The illustrated transition from $|\Psi_5\rangle$ to $|\Psi_6\rangle$ shows that $\widehat{G}$ in the sub-system I/O first performs a reflection about $|\Psi_{\mathrm{S}^\perp}\rangle$ and then a reflection about $|\Psi_0\rangle$. The vector immediately to the right of $|\Psi_{j_N}\rangle$ is $|\Psi_{\mathrm{S}}\rangle$ and is a state in the subspace $\mathbb{H}_{\mathrm{S}}$ of the solution set. We can see that $|\Psi_{j_N}\rangle$ comes close to that

$$\mathbf{P}\left\{\begin{array}{l}\text{Observation of } |\Psi_j\rangle \text{ projects}\\ \text{onto a state } |x\rangle \text{ with } x \in \mathrm{S}\end{array}\right\} = \left|\left|P_{\mathrm{S}}|\Psi_j\rangle\right|\right|^2 \underbrace{=}_{\substack{(6.137),(6.138),\\(6.154)}} \sin^2\theta_j$$

Lemma 6.29 *Let* S *be the solution set with cardinality* $m \geq 1$*, and let* $N = 2^n$ *be the number of objects in which we search for solutions. If we apply the* GROVER *iteration* $\widehat{G}$

$$j_N := \left\lfloor \frac{\pi}{4\arcsin\left(\sqrt{\frac{m}{N}}\right)} \right\rfloor \tag{6.158}$$

times to $|\widehat{\Psi}_0\rangle$ *and observe the state* $|\Psi_{j_N}\rangle$ *in the input/output register, then the probability to observe in the sub-system* $\mathbb{H}^{I/O}$ *a state* $|x\rangle$ *with* $x \in \mathrm{S}$ *satisfies*

$$\mathbf{P}\left\{\begin{array}{l}\textit{Observation of } |\Psi_j\rangle \textit{ projects}\\ \textit{onto a state } |x\rangle \textit{ with } x \in \mathrm{S}\end{array}\right\} \geq 1 - \frac{m}{N}. \tag{6.159}$$

Steps of the Grover search algorithm

Input: A set $\{0,\ldots,N-1\}$ of $N=2^n$ objects that contains a subset S of $m \geq 1$ objects to be searched for and an oracle-function $g:\{0,\ldots,N-1\}\rightarrow\{0,1\}$ that takes the value 1 in S and the value 0 elsewhere

Step 1: In $\mathbb{H}^{I/O}\otimes\mathbb{H}^{W}=\P\mathbb{H}^{\otimes n}\otimes\P\mathbb{H}$ prepare the composite system in the state $|\widehat{\Psi_0}\rangle=|\Psi_0\rangle\otimes|-\rangle$ with

$$|\Psi_0\rangle=\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle\,.$$

The number of computational steps required for Step 1 scales for $N\rightarrow\infty$ with

$$S_{\textsc{Grover1}}(N)\in O(1)$$

Steps of the Grover search algorithm

Input: A set $\{0,\ldots,N-1\}$ of $N=2^n$ objects that contains a subset S of $m \geq 1$ objects to be searched for and an oracle-function $g : \{0,\ldots,N-1\} \rightarrow \{0,1\}$ that takes the value 1 in S and the value 0 elsewhere

Step 1: In $\mathbb{H}^{I/O} \otimes \mathbb{H}^{W} = \P\mathbb{H}^{\otimes n} \otimes \P\mathbb{H}$ prepare the composite system in the state $|\widehat{\Psi}_0\rangle = |\Psi_0\rangle \otimes |-\rangle$ with

$$|\Psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \,.$$

The number of computational steps required for Step 1 scales for $N \rightarrow \infty$ with

$$S_{\text{GROVER1}}(N) \in O(1)$$

Step 2: With $\theta_0 = \arcsin\left(\sqrt{\frac{m}{N}}\right)$ apply the transform $\widehat{G} = (R_{\Psi_0} \otimes \mathbf{1})\widehat{U}_g$

$$j_N = \left\lfloor \frac{\pi}{4\theta_0} \right\rfloor$$

times to $|\widehat{\Psi}_0\rangle$ in order to transform the composite system to the state

$$|\widehat{\Psi}_{j_N}\rangle = \widehat{G}^{j_N} |\widehat{\Psi}_0\rangle \,.$$

The number of computational steps required for Step 2 scales for $N \rightarrow \infty$ with

$$S_{\text{GROVER2}}(N) \in O\left(\sqrt{\frac{N}{m}}\right)$$

Step 3: Observe the sub-system $\mathbb{H}^{I/O}$ and infer from the observed state $|x\rangle$ the value $x \in \{0,\ldots,N-1\}$. The number of computational steps required for Step 3 scales for $N \longrightarrow \infty$ with

$$S_{\text{GROVER3}}(N) \in O(1)$$

Step 3: Observe the sub-system $\mathbb{H}^{I/O}$ and infer from the observed state $|x\rangle$ the value $x \in \{0,\ldots,N-1\}$. The number of computational steps required for Step 3 scales for $N \to \infty$ with

$$S_{\text{GROVER3}}(N) \in O(1)$$

Step 4: By evaluating $g(x)$, check if $x \in \mathrm{S}$. The number of computational steps required for Step 4 scales for $N \to \infty$ with

Step 3: Observe the sub-system $\mathbb{H}^{I/O}$ and infer from the observed state $|x\rangle$ the value $x \in \{0,\ldots,N-1\}$. The number of computational steps required for Step 3 scales for $N \to \infty$ with

$$S_{\text{GROVER3}}(N) \in O(1)$$

Step 4: By evaluating $g(x)$, check if $x \in \mathrm{S}$. The number of computational steps required for Step 4 scales for $N \to \infty$ with

Output: A solution $x \in \mathrm{S}$ with probability no less than $1 - \frac{m}{N}$

Qiskit notebook

https://qiskit.org/textbook/ch-algorithms/grover.html

NEXT LECTURE

NOVEMBER 11, 2022

THANK YOU FOR YOUR ATTENTION!

БЛАГОДАРЯ ЗА ВНИМАНИЕТО!