QUANTUM COMPUTING 7.

Jozef Gruska

Faculty of Informatics
Brno
Czech Republic

May 13, 2007

7.GROVER's ALGORITHMS and AMPLITUDE AMPLIFICATION

Grover's search algorithm and its modifications will be presented an analyzed in this chapter as well as some related problems concerning design of efficient quantum algorithms.

GROVER's SEARCH PROBLEM

Grover's method applies to problems for which it is hard to find a solution, but it is easy to check a to-be-solution.

> **Problem:** In an unsorted database of N items there is one, x_0, satisfying an easy to verify condition P. Find x_0.

Classical algorithms need in average $\frac{N}{2}$ checks.
Quantum algorithm exists that needs $\mathcal{O}(\sqrt{N})$ steps.

Modified problem: Given an easy to compute black-box function

$$f : \{0,1\}^n \rightarrow \{0,1\}$$

find an x_0 such that $f(x_0) = 1$ (let there is single such x_0). Basic idea of the algorithm:

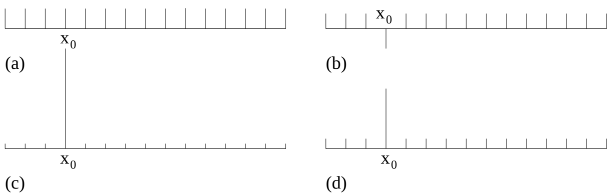


Figure 1: "Cooking" the solution with Grover's algorithm

We shall deal also with a more general problem. Namely that there is more than one solution, especially the case that the following number is known

$$t = |\{x \mid f(x) = 1\}|$$

INVERSION ABOUT THE AVERAGE

Example 0.1 (Inversion about the average) *The unitary transformation*

$$D_n : \sum_{i=0}^{2^n-1} a_i|\phi_i\rangle \rightarrow \sum_{i=0}^{2^n-1} (2E - a_i)|\phi_i\rangle,$$

where E *is the average of* $\{a_i \,|\, 0 \leq i < 2^n\}$*, can be performed by the matrix*

$$-H_n V_0^n H_n = D_n = \begin{pmatrix} -1 + \frac{2}{2^n} & \frac{2}{2^n} & \cdots & \frac{2}{2^n} \\ \frac{2}{2^n} & -1 + \frac{2}{2^n} & \ddots & \frac{2}{2^n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{2^n} & \frac{2}{2^n} & \cdots & -1 + \frac{2}{2^n} \end{pmatrix}.$$

The name of the operation comes from the fact that $2E - x = E + E - x$ *and therefore the new value is as much above (below) the average as it was initially below (above) the average—which is precisely the inversion about the average.*
The matrix D_n *is clearly unitary and it can be shown to have the form* $D_n = -H_n V_0^n H_n$*, where*

$$V_0^n[i,j] = 0 \text{ if } i \neq j, V_0^n[1,1] = -1 \text{ and } V_0^n[i,i] = 1 \text{ if } 1 < i \leq n.$$

Let us consider again the unitary transformation

$$D_n : \sum_{i=0}^{2^n-1} a_i|\phi_i\rangle \to \sum_{i=0}^{2^n-1} (2E - a_i)|\phi_i\rangle,$$

and the following example:
Example: Let $a_i = a$ if $i \neq x_0$ and $a_{x_0} = -a$. Then

$$E = a - \frac{2}{2^n}a$$

$$2E - a_i = \begin{cases} a - \frac{4}{2^n}a \text{ if } i \neq x_0 \\ 2E - a_{x_0} = 3a - \frac{4}{2^n}a; \text{ otherwise} \end{cases}$$

GROVER's SEARCH ALGORITHM

Start in the state

$$|\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

and iterate $\lfloor \frac{\pi}{4}\sqrt{2^n} \rfloor$ times the transformation

$$-\underbrace{H_n V_0^n H_n V_f}_{\text{Grover's iterate}} |\phi\rangle \rightarrow |\phi\rangle.$$

Finally, measure the register to get x_0 and check whether $f(x_0) = 1$. If not, repeat the procedure.

It has been shown that the above algorithm is optimal for finding the solution with probability $> \frac{1}{2}$.

In the case that there are t solutions, repeat the above iteration

$$\left\lfloor \frac{\pi}{4}\sqrt{\frac{2^n}{t}} \right\rfloor \quad \text{times}$$

ANALYSIS of GROVER's ALGORITHM

Denote

$$X_1 = \{x \mid f(x) = 1\} \qquad X_0 = \{x \mid f(x) = 0\}$$

and denote the state after jth iteration of Grover's iterate $-H_n V_0^n H_n V_f$ as

$$|\phi_j\rangle = k_j \sum_{x \in X_1} |x\rangle + l_j \sum_{x \in X_0} |x\rangle$$

with

$$k_0 = \frac{1}{\sqrt{2^n}} = l_0.$$

Since

$$|\phi_{j+1}\rangle = -H_n V_0^n H_n V_f |\phi_j\rangle,$$

it holds

$$k_{j+1} = \frac{2^n - 2t}{2^n} k_j + \frac{2(2^n - t)}{2^n} l_j, \quad l_{j+1} = \frac{2^n - 2t}{2^n} l_j - \frac{2t}{2^n} k_j$$

what yields

$$k_j = \frac{1}{\sqrt{t}} \sin((2j+1)\theta)$$

$$l_j = \frac{1}{\sqrt{2^n - t}} \cos((2j+1)\theta)$$

where

$$\sin^2 \theta = \frac{t}{2^n}.$$

Recurrence relations therefore provide

$$k_j = \frac{1}{\sqrt{t}}\sin((2j+1)\theta), \quad l_j = \frac{1}{\sqrt{2^n - t}}\cos((2j+1)\theta)$$

where

$$\sin^2\theta = \frac{t}{2^n}.$$

The aim now is to find such an j which maximizes k_j and minimizes l_j. Take j such that $\cos((2j+1)\theta) = 0$, that is $(2j+1)\theta = (2m+1)\frac{\pi}{2}$.

Hence

$$j = \frac{\pi}{4\theta} - \frac{1}{2} + \frac{m\pi}{2\theta}$$

what yields

$$j_0 = \lceil \frac{\pi}{4\theta} \rceil,$$

and because

$$\sin^2\theta = \frac{t}{2^n}$$

we have

$$0 \leq \sin\theta \leq \sqrt{\frac{t}{2^n}}$$

and therefore

$$j_0 = \mathcal{O}\left(\sqrt{\frac{2^n}{t}}\right).$$

A MORE DETAILED ANALYSIS

Theorem Let $f \in \mathbf{F_2^n} \rightarrow \{0,1\}$ and let there be exactly t elements $x \in \mathbf{F}_2^n$ such that $f(x)=1$. Assume that $0 < t < \frac{3}{4}2^n$, and let $\theta_0 \in [0, \pi/3]$ be chosen such that $\sin^2\theta_0 = \frac{t}{2^n} \leq \frac{3}{4}$. After $\lfloor \frac{\pi}{4\theta_0} \rceil$ iterations of the Grover iterates on the initial superposition $\frac{1}{\sqrt{2^n}} \Sigma_{x \in \mathbf{F}_2^n} |x\rangle$ the probability of finding a solution is at least $\frac{1}{4}$.

Proof The probability of seeing a desired element is given by $\sin^2((2j+1)\theta_0)$ and therefore $j = -\frac{1}{2} + \frac{\pi}{4\theta_0}$ would give a probability 1.

Therefore we need only to estimate the error when $-\frac{1}{2} + \frac{\pi}{4\theta_0}$ is replaced by $\lfloor \frac{\pi}{4\theta_0} \rfloor$. Since

$$\lfloor \frac{\pi}{4\theta_0} \rfloor = -\frac{1}{2} + \frac{\pi}{4\theta_0} + \delta$$

for some $|\delta| \leq \frac{1}{2}$, we have

$$(2\lfloor \frac{\pi}{4\theta_0} \rfloor + 1)\theta_0 = \frac{\pi}{2} + 2\delta\theta_0,$$

and therefore the distance of $(2\lfloor \frac{\pi}{4\theta_0} \rfloor + 1)\theta_0$ from $\frac{\pi}{2}$ is $|2\delta\theta_0| \leq \frac{\pi}{3}$. This implies

$$\sin^2((2\lfloor \frac{\pi}{4\theta_0} \rfloor + 1)\theta_0) \geq \sin^2(\frac{\pi}{2} - \frac{\pi}{3}) = \frac{1}{4}.$$

A VARIATION on GROVER's ALGORITHM

Input A black box function $f : \mathbf{F}_2^n \rightarrow \{0,1\}$ and $k = |\{x \mid f(x) = 1\}| > 0$

Output: an y such that $f(y) = 1$

Algorithm:

1. If $t > \frac{3}{4}2^n$, then choose randomly an $y \in \mathbf{F}_2^n$ and stop.
2. Otherwise compute $r = \lfloor \frac{\pi}{4\theta_0} \rfloor$, where $\theta_0 \in [0, \pi/3]$ and $\sin^2 \theta_0 = \frac{t}{2^n}$ and apply Grover's iterate G_n r times starting with the state
$$\frac{1}{\sqrt{2^n}} \sum_{x \in \mathbf{F}_2^n} |x\rangle$$
and measure the resulting state to get some y.

If the first step is apply we get correct outcome with probability $\frac{3}{4}$ and if second step is applied then with probability at least $\frac{1}{4}$.
Very special case is $t = \frac{1}{4}2^n$. On such a case $\sin^2 \theta_0 = \frac{1}{4}$ and therefore $\theta_0 = \frac{\pi}{6}$. The probability to get the correct result after one step is then
$$\sin^2((2 \cdot 1 + 1)\theta_0) = \sin^2(\frac{\pi}{2}) = 1.$$

THE CASE of UNKNOWN NUMBER of SOLUTIONS

To deal with the general case – that number of elements we search for is not known – we will need the following technical lemma:

Lemma For any real α and any positive integer m

$$\sum_{r=0}^{m-1} \cos((2r+1)\alpha) = \frac{\sin(2m\alpha)}{2\sin\alpha}.$$

MAIN LEMMA

Lemma Let $f : \mathbf{F}_2^n \to \{0,1\}$ be a blackbox function with $t \leq \frac{3}{4}2^n$ solutions and $\theta_0 \in [0, \frac{\pi}{3}]$ be defined by $\sin^2\theta_0 = \frac{t}{2^n}$. Let $m > 0$ be any integer and $r \in_r [0, m-1]$. If Grover's iterate is applied to the initial state

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \mathbf{F}_2^n} |x\rangle$$

r times, then the probability of seeing a solution is

$$P_r = \frac{1}{2} - \frac{\sin(4m\theta_0)}{4m\sin(2\theta_0)}$$

and if $m > \frac{1}{\sin(2\theta_0)}$, then $P_r \geq \frac{1}{4}$.

Proof We know that the probability of seeing solution after$r$ iteration of Grover's iterate is $\sin^2((2r+1)\theta_0)$.

Therefore if $r \in_r [0, m-1]$, then the probability of seeing a solution is

$$\begin{aligned} P_m &= \frac{1}{m}\sum_{r=0}^{m-1}\sin^2((2r+1)\theta_0) && (1)\\ &= \frac{1}{2m}\sum_{r=0}^{m-1}(1-\cos((2r+1)2\theta_0)) && (2)\\ &= \frac{1}{2}-\frac{\sin(4m\theta_0)}{4m\sin(2\theta_0)}. && (3)\end{aligned}$$

Moreover, if $m \geq \frac{1}{\sin(2\theta_0)}$, then

$$\sin(4m\theta_0) \leq 1 = \frac{1}{\sin(2\theta_0)}\sin(2\theta_0) \leq m\sin(2\theta_0$$

and therefore $\frac{\sin(4m\theta_0)}{4m\sin(2\theta_0)} \leq \frac{1}{4}$ what implies that $P_m \geq \frac{1}{4}$

ALGORITHM

Input A blackbox function $f : \mathbf{F}_2^n \rightarrow \{0, 1\}$.

Output An $y \in \mathbf{F}_2^n$ such that $f(y) = 1$.

Algorithm

1. Choose an $x \in_r \mathbf{F}_2^n$ and if $f(x) = 1$ then output x and stop.
2. Choose $r \in_r [0, m-1]$, where $m = \sqrt{2^n} + 1$ and apply Grover's iterate G_n r times to
$$\frac{1}{\sqrt{2^n}} \sum_{x \in \mathbf{F}_2^n} |x\rangle$$
. Observe the outcome to get some y.

Algorithm works. Indeed, if $t > \frac{3}{4}2^n$, then algorithm will output a solution after the first step with probability at least $\frac{3}{4}$, Otherwise

$$m \geq \sqrt{\frac{2^n}{t}} \geq \frac{1}{\sin(2\theta_0)}$$

and the fact that we get a proper outcome with probability at least $\frac{1}{4}$ follows from previous lemma.

ANOTHER DERIVATION of GROVER's ALGORITHM

Given is an $f : \{0, 1, 2, \ldots, 2^n - 1\} \rightarrow \{0, 1\}$ for which there is a single y such that $f(x) = \delta_{xy}$. Given is also an oracle $\mathcal{O}$ that can identify y if y comes as an input for $\mathcal{O}$. Namely, $\mathcal{O}$ provides for $x \in \{0, 1, 2, \ldots, 2^n - 1\}$

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

We can say that oracle marks the solution by shifting the phase.
The crucial ingidient is the following Grover operator, defined as the one performing the following sequence of actions:

1. apply the oracle $\mathcal{O}$;
2. apply the Hadamard transform H_n;
3. apply the conditional phase shift $F_c|0\rangle = |0\rangle$ and $F_c|x\rangle = -|x\rangle$ for $x > 0$;
4. aply H_n again.

Observe that $F_c = 2|0\rangle\langle 0| - I$ and therefore the Grover operator G has the form

$$G = H_n F_c H_n \mathcal{O} = H_n(2|0\rangle\langle 0| - I)H_n\mathcal{O}$$

If we denote

$$|\psi_n\rangle = H_n|0\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$$

and take into consideration that $H_n^2 = I$, the Grover operator has the form

$$G = (2|\psi_n\rangle\langle\psi_n| - I)\mathcal{O}.$$

We show now that G can be seen as a two-dimensional rotation. Indeed, denote

$$|\alpha\rangle = \frac{1}{\sqrt{2^n - 1}}\sum_{x \neq y}|x\rangle$$

and then

$$|\psi_n\rangle = \sqrt{1 - \frac{1}{2^n}}|\alpha\rangle + \sqrt{\frac{1}{2^n}}|y\rangle.$$

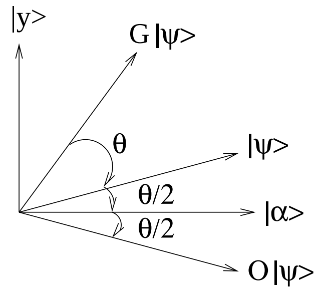
Observe now that the oracle $\mathcal{O}$ actually performs a reflection acros $|\alpha\rangle$ in the plane $\mathcal{P}$ spanned by $|\alpha\rangle$ and $|y\rangle$. Indeed, it holds

$$\mathcal{O}(a|\alpha\rangle + b|y\rangle) = a|\alpha\rangle - b|y\rangle.$$

Similarly, operator $2|\psi\rangle\langle\psi| - I$ performs a reflection in $\mathcal{P}$ acros $|\psi\rangle$. Indeed, if $|\psi_n^\perp\rangle$ is a unit vector orthogonal to $|\psi_n\rangle$ in $\mathcal{P}$, then

$$(2|\psi_n\rangle\langle\psi_n| - I)(a|\psi_n\rangle + b|\psi_n^\perp\rangle) = a|\psi_n\rangle - b|\psi_n^\perp\rangle$$

However, the product of two reflections, with respects to lines L_1 and L_2, is a rotation, by an angle that is twice the angle between these two lines. This also tells us that $G^k|\psi_n\rangle$ remains in $\mathcal{P}$ for all k



The rotation angle can be now obtained as follows: Let

$$\cos(\theta/2) = \sqrt{\frac{2^n - 1}{2^n}}$$

and then

$$|\psi_n = \psi =\rangle \cos(\frac{\theta}{2})|\alpha\rangle + \sin(\frac{\theta}{2})|y\rangle,$$

and therefore, see the figure above,

$$G|\psi_n\rangle = \cos(\frac{3\theta}{2})|\alpha\rangle + \sin(\frac{3\theta}{2})|y\rangle$$

and

$$G^k|\psi_n\rangle = \cos(\frac{2k-1}{2}\theta)|\alpha\rangle + \sin(\frac{2k-1}{2}\theta)|y\rangle$$

and the rest of reasoning is similar as in the first proof.

QUANTUM SEARCH in ORDERED LISTS

A related problem to that of a search in an unordered list is a search in an ordered list of n items.

- The best upper bound known today is $\frac{3}{4}\lg n$.
- The best lower bound known today is $\frac{1}{12}\lg n - \mathcal{O}(1)$.

EFFICIENCY of GROVER's SEARCH

There are at least four different proofs that Grover's search is asymptotically optimal.

Quite a bit is known about the relation between the error ε and the number T of queries when searching an unordered list of n elements.

- ε can be an arbitrary small constant if $\mathcal{O}(\sqrt{n})$ queries are used, but not when $o(\sqrt{n})$ queries are used.
- ε can be at most $\frac{1}{2^{n^{\alpha}}}$ using $\mathcal{O}(n^{0.5+\alpha})$ queries.
- To achieve no error ($\varepsilon = 0$), $\theta(n)$ queries are needed.

APPLICATIONS of GROVER's SEARCH

There is a variety of applications of Grover's search algorithm. Let us mention some of them.

- **Extremes of functions computation** (minimum, maximum).
- **Collision problem** Task is to find, for a given black-box function $f : X \to Y$, two different $x \neq y$ such that $f(x) = f(y)$, given a promise that such a pair exist.

  On a more general level an analogical problem deals with the so-called **r-to-one functions** every element of their image has exactly r pre-images. It has been shown that there is a quantum algorithm to solve collision problem for r-to-one functions in quantum time $\mathcal{O}((n/r)^{1/3})$. It has been shown in 2003 by Shi that the above upper bound cannot be asymptotically improved.
- **Verification of predicate calculus formulas.** Grover's search algorithm can be seen as a method to verify formulas

  $$\exists x P(x),$$

  where P is a black-box predicate.

  It has been shown that also more generalized formulas of the type

  $$\forall x_1 \exists y_1 \forall x_2 \exists y_2 \ldots \forall x_k \exists y_k P(x_1, y_1, x_2, y_2, \ldots, x_k, y_k)$$

  can be verified quantumly with the number of queries $\mathcal{O}(\sqrt{2^{(2k)}})$.

QUANTUM MINIMUM FINDING ALGORITHM

Problem: Let $s = s_1, s_2, \ldots, s_n$ be an unsorted sequence of distinct elements. Find an m such that s_m is minimal.

Classical search algorithm needs $\theta(n)$ comparisons.

QUANTUM SEARCH ALGORITHM

1. Choose as a first "threshold" a random $y \in \{1, \ldots, n\}$.
2. Repeat the following three steps until the total running time is more than $22.5\sqrt{n} + 1.4\lg^2 n$.

   2.1. Initialize
   $$|\psi_0\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |i\rangle|y\rangle$$
   and consider an index i as **marked** if $s_i < s_y$.

   2.2. Apply Grover search to the first register to find an marked element.

   2.3. Measure the first register. If y' is the outcome and $s_{y'} < s_y$, take as a new threshold the index y'.
3. Return as the output the last threshold y.

It is shown in my book that the above algorithm finds the minimum with probability at least $\frac{1}{2}$ if the measurement is done after a total number of $\theta(\sqrt{n})$ operations.

QUANTUM COUNTING

There is a quantum algorithm, a combination of Shor's and Grover's algorithms, to count approximately the number of solutions of the equation $f(x) = 1$, where $f : \{0,1\}^n \rightarrow \{0,1\}$, that is asymptotically more efficient than any classical algorithm for counting.

Basic idea: At the Grover's algorithm amplitudes k_j and l_j vary with the number of iterations, according to a periodic function. This period is directly related to the size of sets X_0 and X_1. An estimation of the common period, using Quantum Fourier Transform, provides an approximation of the size of the sets X_0 and X_1.

Quantum algorithm presented below for approximate counting has two parameters: A black-box function f and a $p = 2^k$ for some k (to set up the precision of approximation).

The algorithm uses two transformations

$$C_f : |m, \psi\rangle \rightarrow |m, G_f^{(m)}\psi\rangle,$$

$$F_p : |k\rangle \rightarrow \frac{1}{\sqrt{2^k}} \sum_{l=0}^{p-1} e^{2\pi ikl/p}|l\rangle,$$

where G_f is Grover iterate for f and $G_f^{(m)}$ denotes its m-th iteration.

ALGORITHM COUNT(f,p)

1. $|\psi_0\rangle \leftarrow (H_n \otimes H_n)|0^{(n)}, 0^{(n)}\rangle$;
2. $|\psi_1\rangle \leftarrow C_f|\psi_0\rangle$;
3. $|\psi_2\rangle \leftarrow F_p \otimes I|\psi_1\rangle$;
4. $f \leftarrow$ **if measure of** $|\psi_2\rangle > \frac{p}{2}$ **then** $p - \mathcal{M}(|\psi_2\rangle)$ **else** $\mathcal{M}(|\psi_2\rangle)$;
5. **output** $\leftarrow 2^n \sin^2(\frac{f\pi}{p})$.

$\boxed{\text{EXTRAS}}$

GROVER's SEARCH – MOTIVATION/GENERALIZATION

In Grover's search the Grover iterate, that can be written in the form

$$Q = -H_n I_0 H_n I_{x_0}$$

is applied to the initial state

$$|\psi_0\rangle = H|0^{(n)}\rangle,$$

where I_j is the operator that inverts sign at j, that is

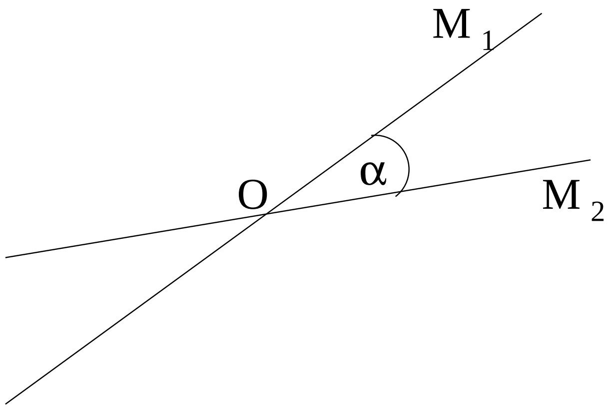
$$I_j|x\rangle = \begin{cases} -|x\rangle & \text{if x=j;} \\ |x\rangle; & \text{otherwise} \end{cases}$$

We shall see that the Hadamard transformation can be replaced, in the Grover iterate, by any unitary transformation.

We shall also provide motivation for all components of Grover's iterate and Grover's search.

The basic observation is a simple result from elementary geometry.

Lemma 0.2 *Let M_1 and M_2 be two lines in the plane intersecting at the point O and let α be the angle from M_1 to M_2.*
Then the operation of reflection with respect to M_1, followed by reflection with respect to M_2 is just the rotation by angle 2α around the point O.


M 1
O
α
M 2

OBSERVATION

For any state $|\psi\rangle$ the operator

$$I_{|\psi\rangle} = I - 2|\psi\rangle\langle\psi|$$

is the operator of reflection in the hyperplane orthogonal to $|\psi\rangle$.

Example 0.3 *Any state $|\phi\rangle$ can be uniquely expressed in the form*

$$|\phi\rangle = \alpha|\psi\rangle + \beta|\psi^{\perp}\rangle,$$

where $|\psi^{\perp}\rangle$ is a state orthogonal to $|\psi\rangle$.

In such a case

$$I_{|\psi\rangle}|\phi\rangle = (I - 2|\psi\rangle\langle\psi|)|\phi\rangle = -\alpha|\psi\rangle + \beta|\psi^{\perp}\rangle$$

that is the parallel component is inverted, the orthogonal is unchanged.

Example 0.4

$$I_{|x_0\rangle} = I - 2|x_0\rangle\langle x_0|.$$

Lemma 0.5 *If $|\phi\rangle$ is any state then $I_{|\psi\rangle}$ preserves the 2-dimensional subspace spanned by $|\phi\rangle$ and $|\psi\rangle$.*

Proof. It holds

$$I_{|\psi\rangle}|\psi\rangle = -|\psi\rangle$$

and

$$I_{|\psi\rangle}|\phi\rangle = -\alpha|\psi\rangle + \beta|\psi^{\perp}\rangle = -2\alpha|\psi\rangle + \alpha|\psi\rangle + \beta|\psi^{\perp}\rangle = -2\alpha|\psi\rangle + |\phi\rangle.$$

Lemma 0.6 *For any unitary operator U it holds*

$$UI_{|\psi\rangle}U^{-1} = I_{U|\psi\rangle}.$$

Proof.

$$\begin{aligned} UI_{|\psi\rangle}U^{-1} &= U(I - 2|\psi\rangle\langle\psi|)U^{-1} && (4) \\ & I - 2U|\psi\rangle\langle\psi|U^{-1} = I - 2|U\psi\rangle\langle U\psi| = I_{U|\psi\rangle} && (5) \end{aligned}$$

Generalized Grover iterate

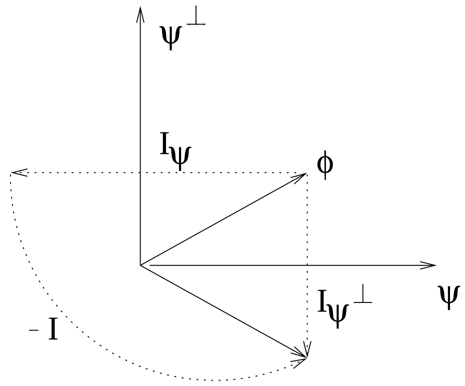
$$Q = -UI_0U^{-1}I_{x_0}$$

has therefore the form

$$Q = -I_{U|0^{(n)}\rangle}I_{|x_0\rangle}$$

Lemma 0.7 *For any two dimensional real (vector)* ψ

$$-I_\psi = I_{\psi^\perp}.$$



Generalized Grover's iterate can therefore be written as

$$Q = I_{|w\rangle} I_{|x_0\rangle},$$

where $|w\rangle$ is orthogonal to $U|0^{(n)}\rangle$ and lies in the plane of $U|0^{(n)}\rangle$ and $|x_0\rangle$.

Since we are working with real coordinates in two-dimensional subspace spanned by $U|0^n\rangle$, $|x_0\rangle$, previous theorem shows that Grover's iterate Q is just operation of rotation through the angle 2α, where α is the angle between $|w\rangle$ and $|x_0\rangle$. Hence

$$\cos\alpha = \langle x_0|w\rangle \qquad \sin\alpha = \langle x_0|U|0^{(n)}\rangle\rangle.$$

NEW INTERPRETATION of GROVER's SEARCH

Problem: Given I_{x_0} as a black box, find x_0.

Idea: Apply I_{x_0} to a (random) state $|\omega\rangle$, or to a $U|0^{(n)}\rangle$ for a (random) unitary transformation U.

By previous results transformation

$$I_{|\omega\rangle} I_{|x_0\rangle}$$

provides a way moving around in the subspace spanned by $|x_0\rangle$ and $|\omega\rangle$ — it is just a rotation by twice the angle between $|x_0\rangle$ and $|\omega\rangle$.

The idea is to use such a rotation that gets us fast from $|\omega\rangle$ to $|x_0\rangle$ (*this process is called* **amplitude amplification**) and when we are close to $|x_0\rangle$, then to perform measurement in the standard basis $\{|i\rangle\}_{i=0}^{2^n-1}$ to get x_0.

Problem: We do not know the angle α between $|\omega\rangle$ and $|x_0\rangle$ and, consequently, we do not know the angle 2α of rotation provided by $I_{|\omega\rangle} I_{|x_0\rangle}$ and therefore we do not know how many times to apply Grover's iterate.

Solution: If we choose $|\omega\rangle = \frac{1}{\sqrt{2^n}} \Sigma_{i=0}^{2^n-1} |i\rangle$, then

$$\cos\alpha = \langle x_0, \omega\rangle = \frac{1}{\sqrt{2^n}}.$$

PROPERTIES of the INVERSION I_ψ

A good insight into Grover's algorithm provides **inversion** $I_{|\psi\rangle} = I - 2|\psi\rangle\langle\psi|$ in Hilbert space H about the hyperplane perpendicular to $|\psi\rangle$. In the case of basis states $I_{|x\rangle} = V_f(|x\rangle)$, where $f(x_0) = 1$ and $f(x) = 0$ otherwise.

Definition Let for $|\psi\rangle, |\xi\rangle \in H$, $\langle\psi|\xi\rangle$ be real. Let us define

$$\mathcal{S}_C = \textit{span}(|\psi\rangle, |\xi\rangle) = \{x|\psi\rangle + y|\xi\rangle, x, y \in \mathbf{C}\}$$

$$\mathcal{S}_R = \textit{span}(|\psi\rangle, |\xi\rangle) = \{x|\psi\rangle + y|\xi\rangle, x, y \in \mathbf{R}\}$$

to be complex and real inner product subspaces of H. If $|\psi\rangle$ and $|\xi\rangle$ are linearly independent, then $\mathcal{S}_R$ is a 2-dimensional real inner-product space lying inside the complex 2-dimensional subspace $\mathcal{S}_C$.

Theorem Let $|\psi\rangle, |\xi\rangle \in H$ be pure states with real inner product. It holds

- Both $\mathcal{S}_C$ and $\mathcal{S}_R$ are invariant under mappings $I_{|\psi\rangle}$ and $I_{|\xi\rangle}$.
- If $L_{|\psi^\perp\rangle}$ is the line in the plane $\mathcal{S}_R$ which passes through the origin and is perpendicular to $|\psi\rangle$, then $I_{|\psi\rangle}$ restricted to $\mathcal{S}_R$ is a reflection in the line $L_{|\psi^\perp\rangle}$.
- If $|\psi^\perp\rangle$ is a unit vector in $\mathcal{S}_R$ perpendicular to $|\psi\rangle$, then $\mathcal{S}_R$, then $-I_{|\psi\rangle} = I_{|\psi^\perp\rangle}$.
- If U is a unitary transformation on H, then

$$UI_{|\psi\rangle}U^* = I_{U|\psi\rangle}.$$

Another View of Grover's Algorithm

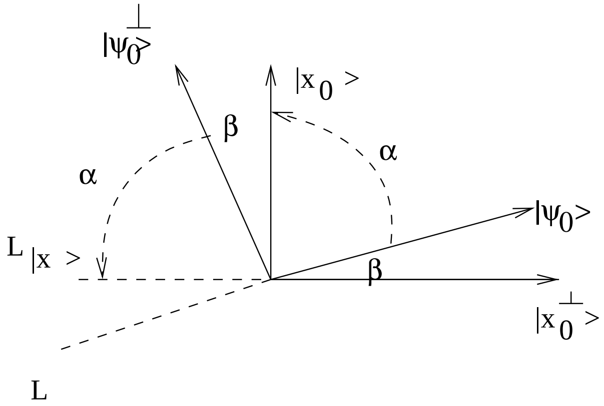
Grover's iterate has now for $|\psi_0\rangle = H|0\rangle$ the form

$$Q = -HI_{|0\rangle}HI_{|x_0\rangle} = -I_{|\psi_0\rangle}I_{|x_0\rangle}$$

In particular, for a restriction of Q to $\mathcal{S}_R$,

$$Q|_{\mathcal{S}_R} = I_{|\psi_0^\perp\rangle}I_{|x_0\rangle}$$

is the composition of two inversions in $\mathcal{S}_R$: the first inversion is in the line $L_{|x_0^\perp\rangle}$ in $\mathcal{S}_R$ passing through the origin and having $|x_0\rangle$ as a normal; the second in the line $L_{|\psi_0\rangle}$ passing through the origin having $|\psi_0^\perp\rangle$ as a normal.



The key next result is the already mentioned theorem from plane geometry:

Theorem If L_1 and L_2 are lines in the Euclidean 2-dimensional plane intersecting at a point O; and if β is the angle from L_1 to L_2, then reflection in L_1 followed by reflection in L_2 is just rotation by the angle 2β about the point O.

Corollary If β is the angle from $|x_0^{\perp}\rangle$ to $|\psi_0\rangle$, then $Q|_{\mathcal{S}_R} = I_{|\psi_0^{\perp}\langle} I_{|x_0\rangle}$ is a rotation about the origin by the angle 2β.

GROVER's ALGORITHM

The key idea of Grover's algorithm is to move $|\psi_0\rangle = H|0\rangle$ toward the unknown state $|x_0\rangle$ by successively applying the rotation given by Q to $|\psi_0\rangle$. Indeed, starting with the state

$$|\psi_0\rangle = \sin\beta|x_0\rangle + \cos\beta|x_0^\perp\rangle$$

after k applications of Grover's iterate Q we get the state

$$|\psi_k\rangle = Q^k|\psi_0\rangle = \sin[(2k+1)\beta]|x_0\rangle + \cos[(2k+1)\beta]|x_0^\perp\rangle.$$

This iteration has to be applied k times such that

$$\sin[(2k+1)\beta]$$

is as close to 1 as possible. Hence

$$k = \lfloor\frac{\pi}{4\beta} - \frac{1}{2}\rfloor)$$

where

$$\frac{1}{\sqrt{2^n}} = \langle x_0|\psi_0\rangle = \cos(\frac{\pi}{2} - \beta) = \sin\beta.$$

The probability of error is

$$\cos^2[(2k+1)\beta] \leq \sin^2\beta \leq \sin^2\beta = \frac{1}{2^n}.$$

GENERALIZED GROVER ALGORITHM

Biham et al. (2000) analyzed evolution of amplitudes, number of iterations, and the probability of finding a state x such that $f(x) = 1$, for so far the most general version of Grover algorithm.

They consider an arbitrary initial state

$$|\psi_0\rangle = \sum_{x \in X_1} k_x |x\rangle + \sum_{x \in X_0} l_x |x\rangle.$$

In addition, instead, of the initial rotation $V_f = I_f^{\pi} = \sum_x e^{i\pi f(x)} |x\rangle\langle x|$ of marked states (x such that $f(x) = 1$) a rotation by an arbitrary phase γ is considered

$$I_f^{\gamma} = \sum_x e^{i\gamma f(x)} |x\rangle\langle x|.$$

In addition, in the rotation by the inversion $G = -H_n I_0^{\pi} H_n$, the Hadamard transformation H_n is replaced by an arbitrary unitary matrix U and, in addition, the rotation I_0^{π}, is replaced by the rotation of a fixed basis state $|s\rangle$ by an arbitrary angle β. G has now the form

$$G = -U I_s^{\beta} U^*,$$

where

$$I_s^{\beta} = I - (1 - e^{i\beta}) |s\rangle\langle s|$$

and therefore

$$G = (1 - e^{i\beta}) |\theta\rangle\langle\theta|,$$

where $|\theta\rangle = U|s\rangle$ and the Grover's iterate has therefore the form $G I_f^{\gamma}$.

Amplitude amplification

Another natural generalization of Grover's search yields additional important quantum algorithm design techniques.

Problem: Let $f : X \rightarrow \{0,1\}$ be a function that partition X into good ($f(x)=1$) and bad ($f(x)=0$) elements and let $\mathcal{A}$ be a quantum algorithm such that $\mathcal{A}|0\rangle = \Sigma_{x \in X}\, \alpha_x |x\rangle$ and, finally, let a be the probability that a good element is obtained if $\mathcal{A}|0\rangle$ is measured.

In average we need to repeat the process of running $\mathcal{A}$, measuring the outcome and checking it (using f), about $\frac{1}{a}$ times, to find a good element.

Amplitude amplification is a process that allows to find a good x after expected $\frac{1}{\sqrt{a}}$ number of applications of the algorithm $\mathcal{A}$ and of its inverse, assuming $\mathcal{A}$ makes no measurement.

In the case a is known, a good x can be found in the worst case after $\frac{1}{\sqrt{a}}$ applications of $\mathcal{A}$ and of its inverse.

This quadratic speed-up can be obtained also for a large family of search problems (for which there are faster classical algorithms as the naive quantum ones).

Amplitude amplification – details

Let H be a Hilbert space and $\mathbf{Z} = \{0, 1, \ldots, 2^n - 1\}$ be a set of names of its basis states. Let a mapping $f : \mathbf{Z} \rightarrow \{0, 1\}$ partition of $\mathbf{Z}$ into good $(f(x) = 1)$ and bad ($f(x) = 0$) states. Good (bad) basis states generate good (bad) subspace H_1 (H_0).

For each pure state $|\psi\rangle \in H$ there is a unique decomposition

$$|\psi\rangle = |\psi_1\rangle + |\psi_0\rangle,$$

where $|\psi_i\rangle \in H_i$.

The probability that measurement of $|\psi\rangle$ provides a good (bad) state is $\langle\psi_1|\psi_1\rangle = a$ ($\langle\psi_0|\psi_0\rangle = 1 - a$).

The amplification process is realized by repeatedly applying the operator

$$Q = -\mathcal{A} I_0 \mathcal{A}^{-1} I_f$$

The first key point is that Q maps subspace H_ψ spanned by vectors $|\psi_1\rangle$ and $|\psi_0\rangle$ into itself. Indeed, it holds

$$Q|\psi_1\rangle = (1 - 2a)|\psi_1\rangle - 2a|\psi_0\rangle$$
$$Q|\psi_0\rangle = 2(1 - a)|\psi_1\rangle - (2a - 1)|\psi_0\rangle$$

because

$$Q = I_\psi I_{\psi_0},$$

where

$$I_\psi = I - 2|\psi\rangle\langle\psi|, \quad I_{\psi_0} = I - \frac{2}{1-a}|\psi_0\rangle\langle\psi_0|.$$

Let $H_\psi^\perp$ be the orthogonal complement of H_ψ in H. The operator $\mathcal{A}I_0\mathcal{A}^*$ acts as identity on $H_\psi^\perp$ and therefore Q^2 acts as identity on $H_\psi^\perp$ and every eigenvector on $H_\psi^\perp$ has eigenvalues $+1$ and -1.

In order to understand the action of Q on an arbitrary state $|\chi\rangle$ it is therefore sufficient to understand the action of Q on the projection of $|\chi\rangle$ on H_ψ.

The operator Q is unitary and on H_ψ it has two eigenvectors

$$|\psi_\pm\rangle = \frac{1}{2}(\frac{1}{\sqrt{a}}|\psi_1\rangle \pm \frac{i}{\sqrt{1-a}}|\psi_0\rangle),$$

provided $0 < a < 1$ and eigenvalues are

$$\lambda_\pm = e^{\pm i2\theta_a},$$

where θ_a is such an angle in $[0, \pi/2]$ defined by

$$\sin^2(\theta_a) = a = \langle\psi_1|\psi_1\rangle.$$

Since

$$\mathcal{A}|0\rangle = |\psi\rangle = \frac{-i}{\sqrt{2}}(e^{i\theta_a}|\psi_+\rangle - e^{-i\theta_a}|\psi_-\rangle)$$

It is now clear that after j applications of iterate Q yields

$$
\begin{aligned}
Q^j|\psi\rangle &= \frac{-i}{\sqrt{2}}(^{(2j+1)i\theta_a}|\psi_+\rangle + e^{-(2j+1)i\theta_a}|\psi_-\rangle && (6)\\
&= \frac{1}{\sqrt{a}}\sin((2j+1)\theta_a)|\psi_1\rangle + \frac{1}{\sqrt{1-a}}\cos((2j+1)\theta_a)|\psi_0\rangle. && (7)
\end{aligned}
$$

On this basis it is straightforward to show:
Theorem(Quadratic speedup) Let $\mathcal{A}$ be a quantum algorithm that uses no measurement and $f : \{0, 1, \ldots, 2^n - 1\} \rightarrow \{0, 1\}$. If the initial probability of success is a, then after computing $Q^m\mathcal{A}|0]\rangle$, where $m = \lceil\pi/4\theta_a\rceil$, where $\sin^2\theta_a = a$, $0 < \theta_a \leq \frac{\pi}{2}$, the outcome is good with probability at least $\max(1 - a, a)$.

In the case of the original Grover's algorithm $a = \frac{1}{2^n}$

Quadratic speed-up without knowing a

Theorem(Quadratic speed-up without knowing a.) There exists a quantum algorithm **QSearch** with the following properties. Let $\mathcal{A}$ be any quantum algorithm that uses no measurement, and let $f : \{0, 1, \ldots, 2^n\} \rightarrow \{0, 1\}$. Let a be success probability of $\mathcal{A}$. Algorithm **QSearch** finds a good solution using $\theta(\frac{1}{\sqrt{a}})$ if $a > 0$, and otherwise runs infinitely.

Algorithm QSearch:

1. Set $l = 0$ and $c \in (1, 2)$, apply $\mathcal{A}$ to the initial state $|0\rangle$ and measure the system. If the output is a good state, then stop.
2. Increase l by 1 and set $M = \lfloor c^l \rfloor$.
3. Choose randomly $j \in [1, M]$ and apply Q^j to $\mathcal{A}|0\rangle$
4. Measure the resulting state. If the outcome $|z\rangle$ is good, then output z; otherwise go to step 2.

Correctness of the algorithm is obvious. If $a > 3/4$, then we find with large probability a good solution in Step 2. Otherwise steps 3 and 4 are repeated until a good solution is found (if it exists). A difficult task is to show that the probability of success is as claimed.

APPENDIX

We prove here several technical results that were used in the main part of this chapter.

Proof that

$$-H_nV_0^nH_n = D_n = \begin{pmatrix} -1+\frac{2}{2^n} & \frac{2}{2^n} & \cdots & \frac{2}{2^n} \\ \frac{2}{2^n} & -1+\frac{2}{2^n} & \ddots & \frac{2}{2^n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{2^n} & \frac{2}{2^n} & \cdots & -1+\frac{2}{2^n} \end{pmatrix}.$$

$$\begin{aligned}
(-H_nV_0^nR_n)_{xy} &= -\sum_{z\in \mathbf{F_2}^n}(H_nR_0^n)_{xz}(H_n)_{zy} && (8)\\
&= -\sum_z\sum_w (H_n)_{xw}(V_0^n)_{wz}(H_n)_{zy} && (9)\\
&= -\frac{1}{2^n}\sum_{z\in\mathbf{F_2^n}}(-1)^{x\cdot z})R_n)_{zz}(-1)^{z\cdot y} && (10)\\
&= \frac{1}{2^n}(2-\sum_{z\in\mathbf{F_2^n}}(-1)^{(x+y)\cdot z}) && (11)\\
&= \begin{cases} \frac{2}{2^n}, & \text{if } x\neq y \\ -1+\frac{2}{2^n} & \text{if} x=y \end{cases} && (12)
\end{aligned}$$

Solution of recurrent equations (Hirvensalo, 2001)

$$k_{j+1} = \frac{2^n - 2t}{2^n} k_j + \frac{2(2^n - t)}{2^n} l_j, \quad l_{j+1} = \frac{2^n - 2t}{2^n} l_j - \frac{2t}{2^n} k_j$$

with the initial condition

$$k_0 = \frac{1}{\sqrt{2^n}} = l_0.$$

It is clear that all K_j and l_j are real and all points (k_j, l_j) are points of the ellipse defined by equation

$$tr_j^2 + (2^n - t) l_j^2 = 1.$$

Hence

$$r_j = \frac{1}{\sqrt{t}} \sin \theta_j$$
$$\frac{1}{\sqrt{2^n - t}} \cos \theta j$$

for some number θ_j. Our basic recursion for $r_{j=1}$ and l_{j+1}

$$\sin \theta_{j+1} = (1 - \frac{2t}{2^n}) \sin \theta_j + \frac{2}{2^n} \sqrt{t(2^n - t)} \cos \theta_j \quad (13)$$

$$\cos \theta_{j+1} = -\frac{2}{2^n} \sqrt{t(2^n - t)} \sin \theta_j + (1 - \frac{2t}{2^n}) \cos \theta_j \quad (14)$$

Since t is number of elements such that $f(y) = 1$ we have $1 - \frac{2t}{2^n} \in [-1, 1]$. we can therefore choose $\omega \in [0, \pi]$ such that $\cos\omega = 1 - \frac{2t}{2^n}$. This then implies that $\sin\omega = \frac{2}{2^n}\sqrt{t(2^n - t)}$ and therefore our recurrent equations get a nice form

$$\sin\theta_{j+1} = \sin(\theta_j + \omega)$$

$$\cos\theta_{j+1} = \cos(\theta_j + \omega).$$

and since the boundary condition gives us $\sin^2\theta_0 = \frac{t}{2^n}$ we have as a solution of our recurrences

$$k_j = \frac{1}{\sqrt{t}}\sin(t\omega + \theta_0),$$
$$l_j = \frac{1}{\sqrt{2^n - t}}\cos(t\omega + \theta_0).$$

where $\theta_0 \in [0, \pi/2]$ and $\omega \in [0, \pi]$. Since $\cos\omega = 1 - \frac{2t}{2^n}$ we have

$$\cos\omega = 1 - 2\sin^2\theta_0 = \cos 2\theta_0$$

and so $\omega = 2\theta_0$

$$k_j = \frac{1}{\sqrt{t}}\sin((2t+1)\theta_0),$$
$$l_j = \frac{1}{\sqrt{2^n - t}}\cos((2t+1)\theta_))$$

.

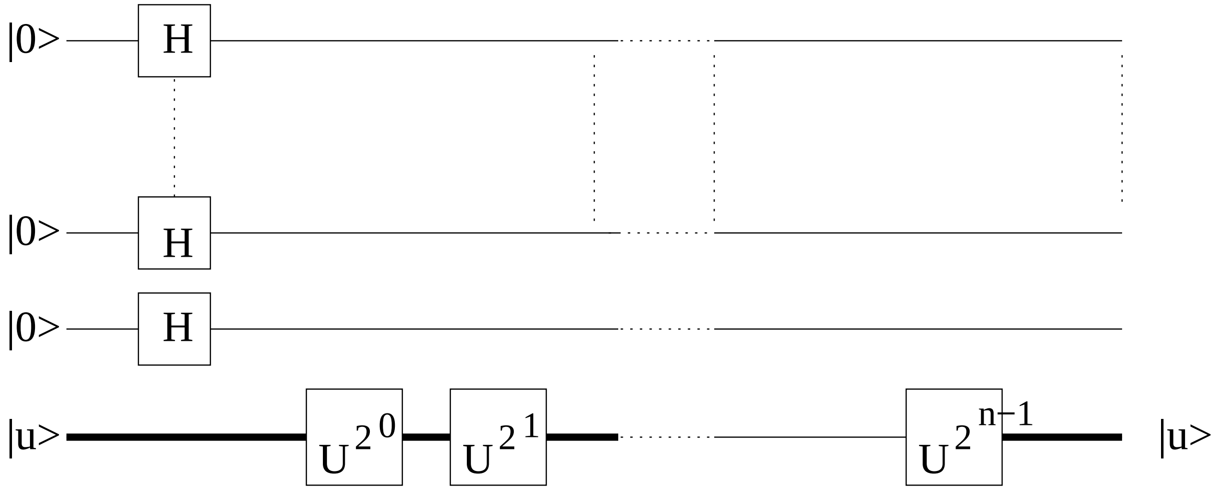
PHASE ESTIMATION

Closely related to implementation of Fourier transform is a method for phase estimation. Given is a unitary operator U with an eigenvector $|u\rangle$ and eigenvalue $e^{2\pi i\phi}$, where $|\phi\rangle$ is unknown. The task is to determine ϕ.

For a related control-U^j-gate it holds

$$U^j(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)]|u\rangle = \frac{1}{\sqrt{2}}(|0\rangle|u\rangle + e^{2\pi ij\phi}|1\rangle|u\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi j\phi}|1\rangle)|u\rangle.$$

This menas that the first n-qubit of the circuit produces the state



$$\frac{1}{\sqrt{2^n}}\bigotimes_{t=1}^{n}(|0\rangle + e^{2\pi i2^{t-1}\phi}|1\rangle) = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1} e^{2\pi ik\phi}|k\rangle$$

The last equality follows from the lemma on next slide.