QUANTUM COMPUTING 7.

Jozef Gruska

Faculty of Informatics
Brno
Czech Republic

November 20, 2013

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 I

Grover's method applies to problems for which it is hard to find a solution, it is easy to recognize a solution, it is easy to through a list of potential solutions, but hard to find some special structure of the problem to speed-up search for a correct solution

> **Problem - a popular formulation:** In an unsorted database of N items there is exactly 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.

Here is the basic idea of the algorithm - "cooking" a solution.

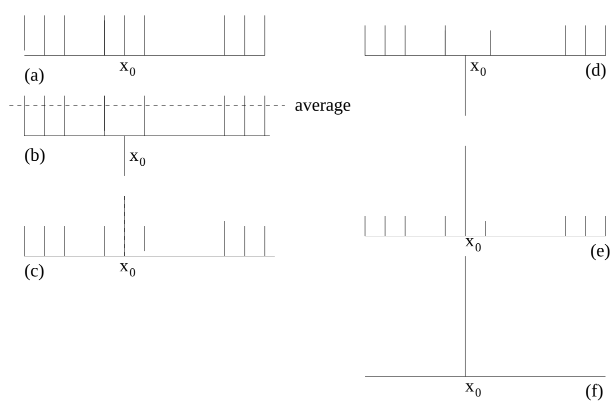


Figure 1: "Cooking" the solution with Grover's algorithm

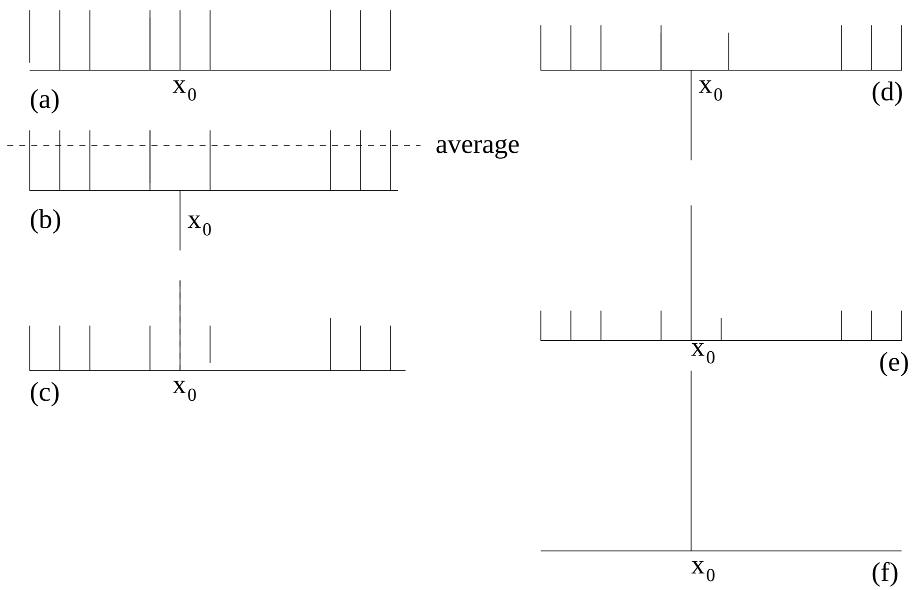


Figure 2: "Cooking" the solution with Grover's algorithm

The figure above shows some steps of the Grover algorithm. Starting state, Figure (a), is equally weighted superposition of all basis states. State $|x_0\rangle$ is the one with $f(x_0) = 1$. Next step, Figure (b), is the state obtained by multiplying with -1 the amplitude of the state $|x_0\rangle$. Figure (c) shows the state after so called inversion over the average is done - the amplitude at $|x_0\rangle$ is increased and amplitudes at all other basis states are decreased. Next step, Figure (d), depicts situation that amplitude at the basis state $|x_0\rangle$ is negated and the next step, Figure (e), is again the result after another inversion about the average is implemented. In case this process iterate a proper number of steps we get the situation that the amplitude at the state $|x_0\rangle$ is (almost) 1 and amplitudes at all other states are (almost) 0. A measurement in such a situation produces x_0 as the classical outcome.

DESIGN of a BLACK BOX

GROVER's SEARCH PROBLEM II

Modified problem: Given an easy to use a black box U_f to compute a function

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

find an x_0 such that $f(x_0) = 1$, for the case that the number t of solutions, that is the number

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

is known

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*

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

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

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

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

$$-\underbrace{H_nV_0^nH_nV_f}_{\text{Grover's iterate}}|\phi\rangle \rightarrow |\phi\rangle.$$

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 $\frac{1}{\sqrt{2^n}} \sum_{x \in \mathbf{F}_2^n} |x\rangle$ 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 $\lfloor \frac{\pi}{4\theta_0} \rceil$. Since

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

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

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

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

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

A VARIATION on GROVER's ALGORITHM

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

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
$$\sin^2((2 \cdot 1 + 1)\theta_0) = \sin^2(\frac{\pi}{2}) = 1.$$

ANOTHER DERIVATION of the GROVER ITERATION

Let $f : \{0,1\}^n \rightarrow \{0,1\}$ be a mapping such that $f(a) = 1$ for a single $a \in \{0,1\}^n$.

Let V_f be a mapping such that for any $x \in \{0,1\}^n$

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

Then for any state $|\psi\rangle$ it holds

$$V_f|\psi\rangle = |\psi\rangle - 2|a\rangle\langle a|\psi\rangle$$

and therefore we can write

$$V_f = \mathbf{1} - 2|a\rangle\langle a|.$$

Therefore, the operator V_f, when acting on any state changes the sign of the amplitude of the basis state $|a\rangle$, while leaving unchanged amplitudues of basis states orthogonal to $|a\rangle$.

CONTINUATION

If we define

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

and consider the operator

$$W = 2|\phi\rangle\langle\phi| - \mathbf{1}$$

then this operator preserves the component of any state along $|\phi\rangle$, while changing the component orthogonal to $|\phi\rangle$.
Grover algorithm can now be defined as an iterative application of the operator WV to the resulting states starting with the initial state $|\phi\rangle$.

Observe that

$$-W = \mathbf{1} - 2|\phi\rangle\langle\phi| = H^{(n)}(\mathbf{1} - 2|0^{(n)}\rangle\langle 0^{(n)}|H^{(n)}$$

ANALYSIS

- Both operators V and W when acting on a superposition of states $|a\rangle$ and $|\phi\rangle$ produce a superposition of the same states.
- Indeed, since $\langle a|\phi\rangle = \frac{1}{\sqrt{2^n}}$, it holds

$$V|a\rangle = -|a\rangle, \quad V|\phi\rangle = |\phi\rangle - \frac{2}{\sqrt{2^n}}|a\rangle$$

$$W|\phi\rangle = |\phi\rangle \quad W|a\rangle = \frac{2}{\sqrt{2^n}}|\phi\rangle - |a\rangle$$

- As a consequence, a repeated application of the operator WV to the resulting states starting with the state $|\phi\rangle$ will always result in a state that will be a superposition of $|a\rangle$ and $|\phi\rangle$.
- If we denote by $|a_\perp\rangle$ a state orthogonal to $|a\rangle$ in the subspace generated by $|a\rangle$ and $|\phi\rangle$, and by γ and θ angles

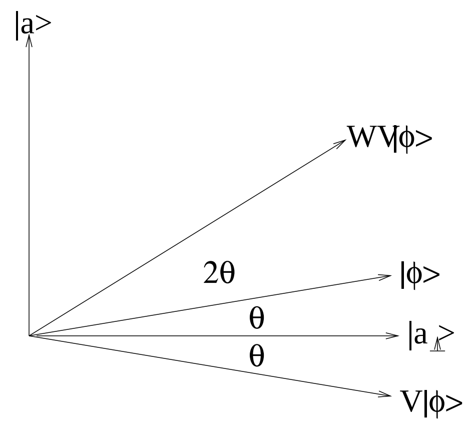
$$\sin\theta = \cos\gamma = \langle a|\phi\rangle = \frac{1}{\sqrt{2^n}}$$

with $\theta = \frac{\pi}{2} - \gamma$, then

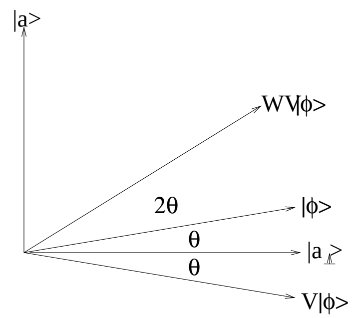
$$\theta \approx \frac{1}{\sqrt{2^n}}$$

for large n.

- The net effect of the operator W in two dimensional plane is to transform any vector by its reflection with respect to the mirror line through the origin along $|\phi\rangle$.
- Similarly, the net effect of the operator V on any vector is its reflection with respect to the vector $|a_\perp\rangle$.



- The net effect of the any application of the product WV, of two operators that are two-dimensional reflections, is therefore a rotation about the angle 2θ.



- Since m iterations will result in the rotation by the angle $2m\theta$, with respect to the initial state $|\phi\rangle$, and θ is very close to $\frac{1}{\sqrt{2^n}}$, the number of iterations needed to come to the state orthogonal to $|a_\perp\rangle$ (that is to the state $|a\rangle$), should be approximately

$$\frac{\pi}{4}\sqrt{2^n}$$

because for $m = \frac{\pi}{4}\sqrt{2^n}$ we have

$$2m\theta = 2\frac{\pi}{4}\sqrt{2^n}\frac{1}{\sqrt{2^n}} = \frac{\pi}{2}$$

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.

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 $f : X \rightarrow Y$, 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

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

  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
   $$|\psi_0\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle|y\rangle$$
   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** $\leftarrow 2^n \sin^2(\frac{f\pi}{p})$.

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

$$\begin{aligned} Q^j|\psi\rangle &= \frac{-i}{\sqrt{2}}(^{(2j+1)i\theta_a}|\psi_+\rangle + e^{-(2j+1)i\theta_a}|\psi_-\rangle && (4) \\ &= \frac{1}{\sqrt{a}}\sin((2j+1)\theta_a)|\psi_1\rangle + \frac{1}{\sqrt{1-a}}\cos((2j+1)\theta_a)|\psi_0\rangle. && (5) \end{aligned}$$

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 now several technical results that were used in the main part of this chapter.

Proof that

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

$$\begin{aligned}
(-H_nV_0^nH_n)_{xy} &= -\sum_{z\in\mathbf{F_2}^n}(H_nR_0^n)_{xz}(H_n)_{zy} && (6)\\
&= -\sum_z\sum_w(H_n)_{xw}(V_0^n)_{wz}(H_n)_{zy} && (7)\\
&= -\frac{1}{2^n}\sum_{z\in\mathbf{F_2^n}-\{0\}}(-1)^{x\cdot z})V_0^n)_{zz}(-1)^{z\cdot y} && (8)\\
&= \frac{1}{2^n}(2-\sum_{z\in\mathbf{F_2^n}-\{0\}}(-1)^{(x+y)\cdot z}) && (9)\\
&= \begin{cases} \frac{2}{2^n}, & \text{if } x\neq y \\ -1+\frac{2}{2^n} & \text{if} x=y \end{cases} && (10)
\end{aligned}$$

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

$$\begin{array}{rl} r_j = & \frac{1}{\sqrt{t}}\sin\theta_j \\ t_j = & \frac{1}{\sqrt{2^n - t}}\cos\theta j \end{array}$$

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

$$\sin\theta_{j+1} = (1 - \frac{2t}{2^n})\sin\theta_j + \frac{2}{2^n}\sqrt{t(2^n - t)}\cos\theta_j \qquad (11)$$

$$\cos\theta_{j+1} = -\frac{2}{2^n}\sqrt{t(2^n - t)}\sin\theta_j + (1 - \frac{2t}{2^n})\cos\theta_j \qquad (12)$$

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

$$\begin{aligned} k_j &= \tfrac{1}{\sqrt{t}}\sin(t\omega + \theta_0), \\ l_j &= \tfrac{1}{\sqrt{2^n - t}}\cos(t\omega + \theta_0). \end{aligned}$$

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 $\omega = 2\theta_0$

$$\begin{aligned} k_j &= \tfrac{1}{\sqrt{t}}\sin((2t+1)\theta_0), \\ l_j &= \tfrac{1}{\sqrt{2^n - t}}\cos((2t+1)\theta_)) \end{aligned}$$

.

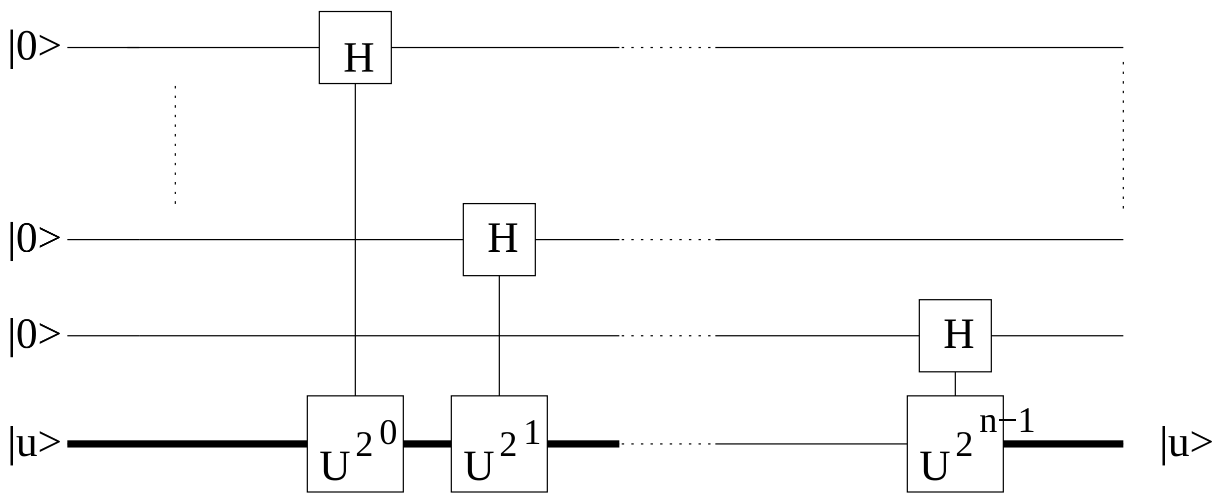
PHASE ESTIMATION

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 means that the first n-qubit of the circuit produces the state



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

The last equality follows from the lemma on next slide.

LEMMA

Let $x \in \{1, \ldots, 2^n - 1\}$ and let its binary representation be $x_1 x_2 \ldots x_n$. For quantum Fourier transform

$$F|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n} |k\rangle$$

it holds

Lemma

$$F|x\rangle = \frac{1}{\sqrt{2^n}}[(|0\rangle + e^{2\pi i 0.x_n}|1\rangle)(|0\rangle + e^{2\pi i 0.x_{n-1}x_n}|1\rangle)\ldots(|0\rangle + e^{2\pi i 0.x_1\ldots x_n}|1\rangle)].$$

Proof This follows form calculations

$$\begin{aligned} F|x\rangle &= \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ixk/2^n}|k\rangle = \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^{1} \ldots \sum_{k_n=0}^{1} \exp(2\pi ix \sum_{l=1}^{n} k_l 2^{-l})|x_1 \ldots x_n\rangle && (13) \\ &= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^{1} \ldots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi ixk_l/2^l}|k_l\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \sum_{k_l=0}^{1} e^{2\pi ixk_l/2^l}|k_l\rangle && (14) \\ &= \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} (|0\rangle + e^{2\pi ix/2^l}|1\rangle) && (15) \end{aligned}$$

AMPLITUDE AMPLIFICATION

In the original Grover's search algorithm the first step is to apply the operator $H^{\otimes n}$ to the state $|0^n\rangle$ to obtain a uniform superposition of all basis states.

The above step can be seen as follows: the operator $H^{\otimes n}$ guesses a solution in such a way that all possible solutions have the same probability.

Grover's idea can be applied to any algorithm A which guesses a solution by setting up some other superposition of all basis states.

The state

$$|\psi\rangle = A|0^n\rangle = \sum_x \alpha_x|x\rangle$$

can be naturally splitted as follows

$$|\psi\rangle = \sum_{x\in X_{\text{good}}} \alpha_x|x\rangle + \sum_{x\in X_{\text{bad}}} \alpha_x|x\rangle$$

Observe that

$$p_{\text{good}} = \sum_{x\in X_{\text{good}}} |\alpha_x|^2 \text{ and } p_{\text{bad}} = \sum_{x\in X_{\text{bad}}} |\alpha_x|^2$$

are probabilities of measuring a good and a bad state.

In a nontrivial case $0 < p_{\text{good}} < 1$, we can consider the states

$$|\psi_{\text{good}}\rangle = \sum_{x\in X_{\text{good}}} \frac{\alpha_x}{\sqrt{p_{\text{good}}}}|x\rangle \quad |\psi_{\text{bad}}\rangle = \sum_{x\in X_{\text{bad}}} \frac{\alpha_x}{\sqrt{p_{\text{bad}}}}|x\rangle$$

and then we can write

$$|\psi\rangle = \sqrt{p_{\text{good}}}|\psi_{\text{good}}\rangle + \sqrt{p_{\text{bad}}}|\psi_{\text{bad}}\rangle$$

or

$$|\psi\rangle = \sin(\theta)|\psi_{\text{good}}\rangle + \cos(\theta)|\psi_{\text{bad}}\rangle$$

where $\theta \in (0, \frac{\pi}{2}), \sin^2(\theta) = p_{\text{good}}$.

The state $|\psi\rangle$ is orthogonal to the state

$$|\bar{\psi}\rangle = \cos(\theta)|\psi_{\text{good}}\rangle - \sin(\theta)|\psi_{\text{bad}}\rangle$$

and therefore

$$\{|\psi\rangle, |\bar{\psi}\rangle\} \text{ and } \{|\psi_{\text{good}}\rangle, |\psi_{\text{bad}}\rangle\}$$

are two orthonormal bases in the same 2-dimensional subspace.

Let us now consider operators $U_{\psi^\perp}$ and U_f defined by

$$U_{\psi^\perp}|\psi\rangle = |\psi\rangle \text{ and } U_{\psi^\perp}|\phi\rangle = -|\phi\rangle$$

for all $|\phi\rangle$ orthogonal to $|\psi\rangle$ and

$$U_f : |x\rangle \rightarrow (-1)^{f(x)}|x\rangle$$

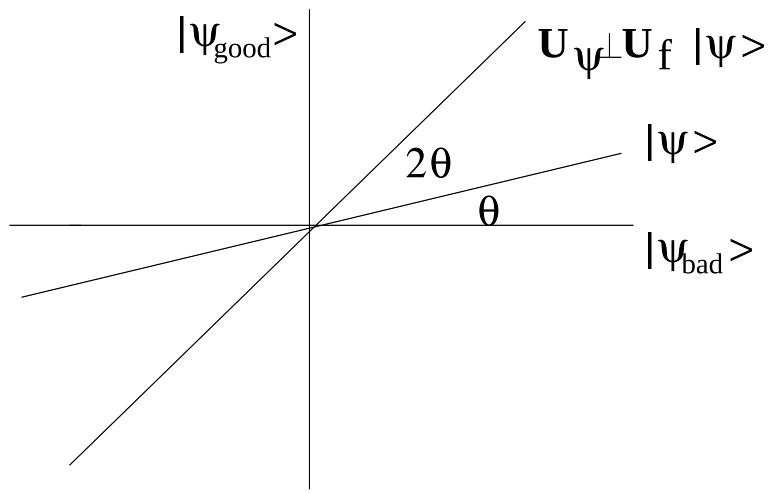
By straightforward calculations one can derive relations

$$U_\psi^\perp U_f|\psi\rangle = \cos(2\theta)|\psi\rangle + \sin(2\theta)|\bar{\psi}\rangle$$

and also

$$U_\psi^\perp U_f|\psi\rangle = \sin(3\theta)|\psi_{\text{good}}\rangle + \cos(3\theta)|\psi_{\text{bad}}\rangle$$

The last state is illustrated in the following figure



Observe now that for any real θ the operator U_f does the following

$$U_f(\sin(\theta)|\psi_{\text{good}}\rangle + \cos(\theta)|\psi_{\text{bad}}\rangle = -\sin(\theta)|\psi_{\text{good}}\rangle + \cos(\theta)|\psi_{\text{bad}}\rangle$$

and therefore U_f performs a reflection about the axis defined by the vector $|\psi_{\text{bad}}\rangle$ and similarly

$$U_\psi^\perp(\sin(\theta)|\psi\rangle + \cos(\theta)|\bar{\psi}\rangle = \sin(\theta)|\psi\rangle - \cos(\theta)|\bar{\psi}\rangle$$

and therefore $U_\psi^\perp$ performs a reflection about the axis defined by the state $|\psi\rangle$.

It is a well-known fact from the elementary geometry that two such reflections correspond to a rotation through the angle 2θ in the 2-dimensional space.

An application of the operator $G = U_{\psi}^{\perp} U_f$ k-times therefore rotates the initial state $|\psi\rangle$ to the state

$$G^k|\psi\rangle = \cos((2k+1)\theta)|\psi_{\text{bad}}\rangle + \sin((2k+1)\theta)|\psi_{\text{good}}$$

If such a state is measured when $(2k+1)\theta \approx \frac{\pi}{2}$, then with very high probability a good basic state is revealed.
For small θ we have $\theta \approx \sin(\theta) = \sqrt{p_{\text{good}}}$ and therefore a measurement should be performed after $k = \approx \frac{\pi}{4\theta} \approx \frac{\pi}{4\sqrt{p_{\text{good}}}]}$ iterations.

An application of such a procedure therefore requires to know the probability with which the operator A guesses a solution to $f(x) = 1$.

QUANTUM AMPLITUDE ESTIMATION and QUANTUM COUNTING

Quantum counting is a problem, given

$$F : \{0, 1, \ldots, N-1\} \rightarrow \{0, 1\}$$

to determine the number t of such x that $f(x) = 1$.

Quantum counting problem is a special case of the following

Amplitude estimation problem:
Given are:

- The operator A with the property that $A|0^n\rangle = \sin(\theta)|\psi_{good}\rangle + \cos(\theta)|\psi_{bad}\rangle$, $0 \leq \theta \leq \frac{\pi}{2}$.
- The operator U_f that maps $|\psi_{good}\rangle \rightarrow -|\psi_{good}\rangle$ and $|\psi_{bad}\rangle \rightarrow |\psi_{bad}\rangle$

The task is to estimate $\sin(\theta)$

In case $A = H^{\otimes n}$ amplitude estimation problem is actually quantum counting problem.

Indeed, if t is number of solutions, then

$$H^{\otimes n}|0^n\rangle = \sqrt{\frac{t}{N}}|\psi_{good} + \sqrt{\frac{N-t}{N}}|\psi_{bad}\rangle$$

and therefore $\sin^2(\theta) = \frac{t}{N}$.

QUANTUM AMPLITUDE ESTIMATION

Let us have an operator

$$A|0^n\rangle = \sum_{j=0}^{2^n-1} \alpha_j |j\rangle$$

and define for $0 < \theta < \frac{\pi}{2}$

$$\sum_{j \in X_{good}} |\alpha_j|^2 = \sin^2(\theta) \qquad \sum_{j \in X_{bad}} |\alpha_j|^2 = \cos^2(\theta)$$

and therefore

$$A|0^n\rangle = \sin\theta|\psi_{good}\rangle + \cos\theta|\psi_{bad}\rangle.$$

As already shown the amplitude amplification through a Grover-iteration like operator Q is actually rotation in the space spanned by the states $|\psi_{good}\rangle, |\psi_{bad}\rangle\}$ through an angle 2θ. Therefore in this space Q is described by the rotation matrix

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

that has eigenvectors

$$\begin{pmatrix} \frac{i}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \qquad \begin{pmatrix} -\frac{i}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

and the corresponding eigenvalues $e^{i2\theta}$ and $e^{-i2\theta}$. Therefore

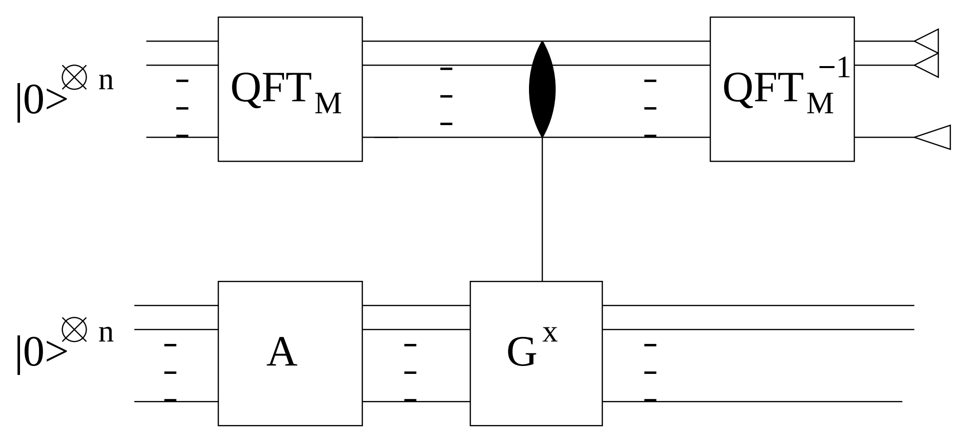
$$|\psi\rangle = e^{i\theta}\frac{1}{\sqrt{2}}|\psi_+\rangle + e^{-i\theta}\frac{1}{\sqrt{2}}|\psi_-\rangle$$

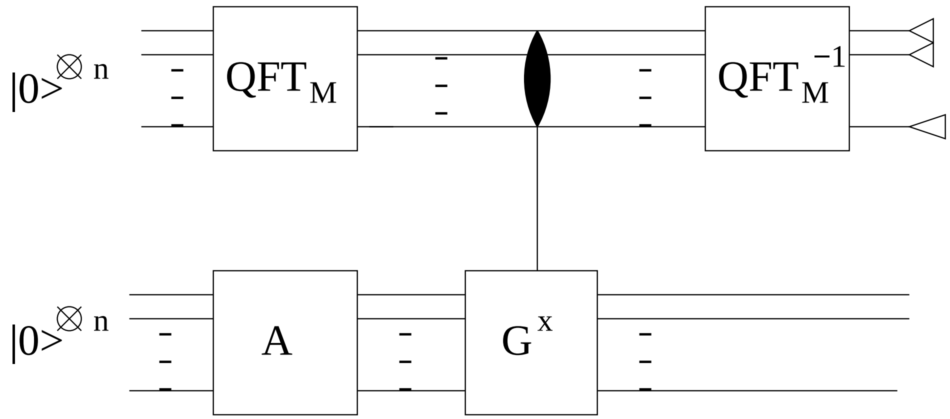
where

$$|\psi_+\rangle = \frac{1}{\sqrt{2}}|\psi_{bad}\rangle + \frac{i}{\sqrt{2}}|\psi_{good}\rangle, \quad |\psi_-\rangle = \frac{1}{\sqrt{2}}|\psi_{bad}\rangle - \frac{i}{\sqrt{2}}|\psi_{good}\rangle$$

Quantum amplitude estimation algorithm works by applying eigenvalue estimation with the second register in the above state $|\psi\rangle$. Such an algorithm gives us an estimate of either 2θ or -2θ.

The quantum amplitude estimation circuit has the form





This is therefore a circuit for quantum amplitude estimation where $M = 2^n$ applications of the search iterate and therefore M applications of U_f are used. A measurement of the top register yields a string representing an integer y. The value $\frac{2xy}{M}$ is an estimate of either 2θ or $2\pi - 2\theta$. The circuit outputs an integer $y \in \{0, 1, 2, \ldots, M-1\}$, where $M = 2^m$, $m \geq 1$ and the estimate of $p = \sin^2(\theta)$ is $\bar{p} = \sin^2(\pi \frac{y}{M})$.