QUANTUM COMPUTING 7.

Jozef Gruska

Faculty of Informatics
Brno
Czech Republic

October 27, 2002

6. SEARCH ALGORITHMS

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

GROVER's SEARCH PROBLEM

Grover's method seems to apply 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:

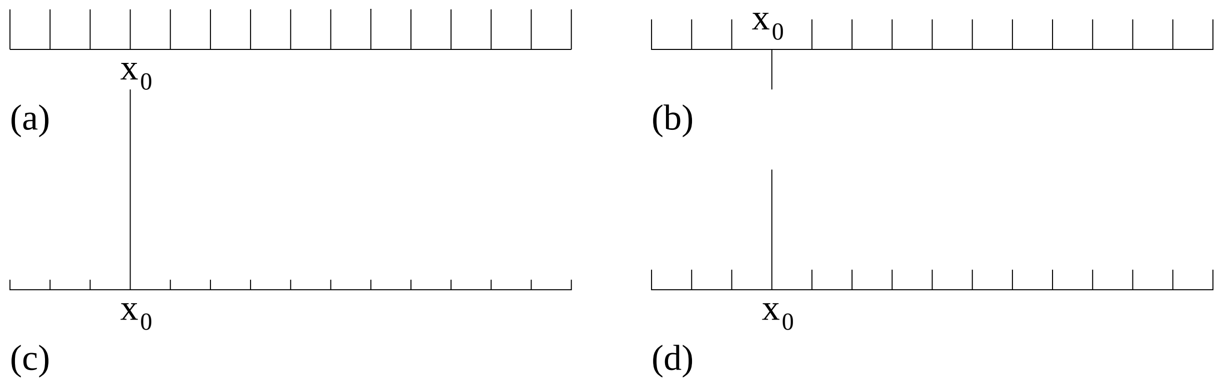


Figure 1: "Cooking" the solution with Grover's algorithm

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

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

is known.

INVERSION ABOUT THE AVERAGE

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

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

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

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

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*

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

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

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

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

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

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

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

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 $\frac{1}{12}\lg n - \mathcal{O}(n)$.

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 (ε), $\theta(n)$ 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 $\mathcal{O}((n/r)^{1/3})$. No nontrivial lower bound is known for this problem.
- **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 new threshold index y'.
3. Return last threshold y.

It is shown in the 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 $\mathcal{O}(\sqrt{n})$ of 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.

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 sets X_0 and X_1.

Quantum algorithm presented below for approximate counting has two parameters: A black-box function f and an $p = 2^k$ 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 $\leftarrow 2^n \sin^2(\frac{f\pi}{p})$.

$\boxed{\text{EXTRAS}}$

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 $I_{|x_0\rangle} = V_f(|x\rangle)$, 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

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

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

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 of the complex 2-dimensional space $\mathcal{S}_C$.

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

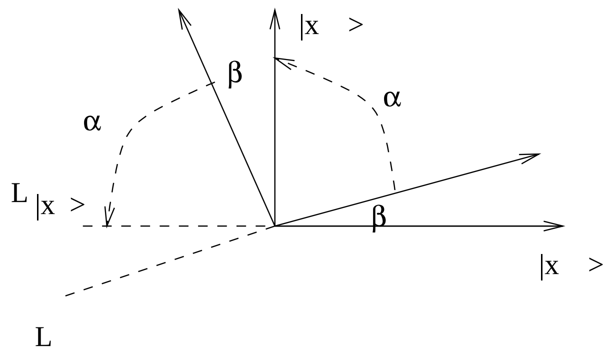
Grover's iterate has now for $|\psi_0\rangle = H|0\rangle$ the form

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

In particular

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

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



The key next result is the following 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 $Q|_{\mathcal{S}_R} = I_{|\psi_0^\perp}I_{|x_0\rangle}$ 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 time-evolution of amplitudes, optimal number of iterations, and the probability of finding a (smoked) 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, 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 $f : X \to \{0,1\}$ 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 - basic idea

If a probabilistic algorithm provides a solution of a problem with a probability $p > 0$, then by repeating the algorithm we can increase the probability of success by a constant at each run.

Amplitude amplification technique increases probability amplitude of success roughly by a constant at each run.

Because amplitudes correspond to squares of probabilities, it suffices to repeat amplitude amplification procedure approximately $\frac{1}{\sqrt{a}}$ times to achieve success with probability almost 1.

Observe that in Grover's search problem the initial probability of success by the measurement is $\frac{1}{2^n}$.

Amplitude estimation

A combination of ideas of Grover's and Shor's algorithms allows to perform **amplitude estimation**, a process that allows to estimate the probability a.

An application of amplitude estimation techniques allows to estimate the number of x such that $f(x) = 1$. This is also called **quantum counting**.

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

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

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:

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