State preparation based on Grover’s algorithm in the presence of global information about the state

Andrei N. Soklakov and Rüdiger Schack

Department of Mathematics, Royal Holloway, University of London, Egham, Surrey TW20 0EX, United Kingdom

3 October 2004

Abstract

In a previous paper [1] we described a quantum algorithm to prepare an arbitrary state of a quantum register with arbitrary fidelity. Here we present an alternative algorithm which uses a small number of quantum oracles encoding the most significant bits of the absolute value of the complex amplitudes, and a small number of oracles encoding the most significant bits of the phases. The algorithm given here is considerably simpler than the one described in [1], on the assumption that a sufficient amount of knowledge about the distribution of the absolute values of the complex amplitudes is available.

1 Overview

The first step of many quantum computer algorithms is the preparation of a quantum register in a simple initial state, e.g., the equal superposition of all computational basis states. Some applications of quantum computers, such as the simulation of a physical system [2, 3, 4], require the initial preparation of more general states. Here we consider the state preparation problem in the case that the Hilbert-space dimension of the quantum register is so large that listing the complex coefficients of the state is impractical.

In a previous publication [1] we have shown how to use elements of Grover’s algorithm [5] to prepare a register of $\log_2 N$ qubits, with arbitrary fidelity, in an approximation to the state

$$|\Psi\rangle = \sum_{x=0}^{N-1} \sqrt{p(x)} e^{2\pi i \phi(x)} |x\rangle \quad (1)$$

for any probabilities $p(x)$ and phases $\phi(x)$. We assume that $N$ is an integer power of 2. Here and throughout the paper, $|0\rangle, |1\rangle, \ldots$ denote computational basis states.

We will now describe an alternative algorithm to achieve the same goal, i.e., to prepare the quantum register in a state $|\tilde{\Psi}\rangle$ such that the fidelity, $|\langle \tilde{\Psi} | \Psi \rangle|$, is close to 1. In the
A description of the algorithm below, we introduce three positive integer parameters, $T$, $T'$, and $a$. We will indicate how to choose these parameters, and derive a lower bound on the fidelity $|\langle \tilde{\Psi} | \Psi \rangle|$ in terms of them. We will also show how the required computational resources scale with these parameters. This will put us in a position to compare the two versions of the algorithm. See Ref. [1] for a comparison with the state-preparation algorithms by Kaye and Mosca [6] and Grover and Rudolph [7].

The functions $p(x)$ and $\phi(x)$ are assumed to be given in the form of classical algorithms. The function $p(x)$ is used to construct a set of quantum oracles as follows. Let $T$ be a positive integer. For $k = 1, \ldots, T$, we define

$$O_k(x) = c_k(x),$$

where $c_k(x) \in \{0, 1\}$ are the coefficients in the binary expansion

$$\sqrt{\eta N p(x)} = \sum_{k=1}^{\infty} c_k(x) 2^{-k},$$

and where $\eta$ is a positive real number, $\eta < 1$, such that

$$p(x) \leq \frac{1}{\eta N} \text{ for all } x.$$

We extend this definition beyond the domain of the function $p$ by setting $O_k(x) = 0$ for $x \geq N$. The quantum oracles are unitary operators defined by

$$\hat{O}_k |x\rangle = (-1)^{O_k(x)} |x\rangle,$$

which can be realized as quantum gate sequences using the classical algorithm to compute the probabilities $p(x)$. For each oracle, we define the number of solutions

$$N_k = \sum_x O_k(x).$$

Now let $T'$ be a positive integer, and let $c'_k(x) \in \{0, 1\}$ be the coefficients in the binary expansion

$$\phi(x) = \sum_{k=1}^{\infty} c'_k(x) 2^{-k}.$$

For $k = 1, \ldots, T'$, we define unitary operations, $U_1, \ldots, U_{T'}$, on our quantum register by

$$U_k |x\rangle = e^{2\pi i c'_k(x)/2^k} |x\rangle.$$

The operators $U_k$ are conditional phase shifts that can be realized as quantum gate sequences using the classical algorithm to compute the phases $\phi(x)$.

The algorithm can now be described as follows. Choose a suitable (small) number, $a$, of auxiliary qubits, and define $L = \log_2 N + a$. Prepare a register of $L$ qubits in the state

$$|\Psi^0\rangle = (2^a N)^{-1/2} \sum_{x=0}^{2^a N-1} |x\rangle.$$
For \( k = 1, \ldots, T \), define the Grover operator
\[
\hat{G}(O_k, t_k) = \left( (2|\Psi^0\rangle\langle\Psi^0| - \hat{I})\hat{O}_k \right)^{t_k} ,
\] (10)
where \( \hat{I} \) is the \( L \)-qubit identity operator, and where the integer “times” \( t_k \) are defined in Eq. (42) below. Apply the Grover operators successively to the register to create the state
\[
|\Psi_T\rangle = \hat{G}(O_T, t_T) \cdots \hat{G}(O_1, t_1)|\Psi^0\rangle .
\] (11)

Now measure the auxiliary qubits in the computational basis. If one of the outcomes is 1 (the probability for this will be shown to be small), this stage of the algorithm has failed, and one has to start again by preparing the register in the state \( |\Psi^0\rangle \) as in Eq. (9). Otherwise, i.e., if all outcomes are 0, this stage of algorithm has succeeded, and the resulting state of the remaining \( L - a = \log_2 N \) qubits, which we denote by \( |\tilde{\Psi}_T\rangle \), will be a good approximation to the real-amplitude state
\[
|\Psi_T\rangle = \sum_{x=0}^{N-1} \sqrt{p(x)} |x\rangle ,
\] (12)
obtained from our target state \( |\Psi\rangle \) by setting the phases \( \phi(x) \) to zero.

The final stage of the algorithm adds phases to the state \( |\tilde{\Psi}_T\rangle \) by applying the operators \( U_1, \ldots, U_{T'} \),
\[
|\tilde{\Psi}\rangle = U_1 U_2 \cdots U_{T'} |\tilde{\Psi}_T\rangle .
\] (13)
In the next section, we analyse the dependence of the state \( |\Psi_T\rangle \) on the numbers \( t_k \), and thus motivate the definition (42). At the end of the section, we derive upper bounds on the numbers \( t_k \) and therefore on the required number of oracle calls. In the final section, we derive a lower bound on the fidelity in terms of the parameters \( T, T' \) and \( a \).

## 2 Number of oracle calls

In the following we will use the notation \( 1 : n \) to index an ordered sequence of \( n \) symbols, for example,
\[
q_{1:n} = q_1, \ldots, q_n .
\] (14)
Using this notation, the statement \( q_{1:n} = c_{1:n} \) means that \( q_j = c_j \) for any \( j = 1, \ldots, n \).

We define a set of refined oracles,
\[
O_{q_{1:n}}(x) = \begin{cases} 
1 & \text{if } q_{1:n} = c_{1:n}(x) , \\
0 & \text{otherwise} ,
\end{cases}
\] (15)
which can be expressed in terms of the oracles \( O_k \) as follows.
\[
O_{q_{1:n}}(x) = \prod_{k=1}^{n} \left[ O_k(x) - 1 + q_k \right] .
\] (16)
Let $\Omega_{q_{1,k}}$ be the set of values that are accepted by the oracle $O_{q_{1,k}}$, i.e.

$$\Omega_{q_{1,k}} = \{ x : O_{q_{1,k}}(x) = 1 \}. \quad (17)$$

Furthermore, denote by $N_{q_{1,k}}^k$ the size of the set $\Omega_{q_{1,k}}$:

$$N_{q_{1,k}}^k = \sum_x O_{q_{1,k}}(x). \quad (18)$$

The first stage of our algorithm takes the initial state $|\Psi_0\rangle$ through a series of intermediate states, $|\Psi_k\rangle$, to the state $|\Psi_T\rangle$. Due to the properties of the Grover operators, $\hat{G}(O_k, t_k)$, the intermediate states are of the form

$$|\Psi_k\rangle = \sum_{q_{1,k}} \sum_{x \in \Omega_{q_{1,k}}} A_{q_{1,k}}^k |x\rangle, \quad (19)$$

where

$$A_{q_{1,k}}^k = B^k + \sum_{j=1}^{k} q_j h_j, \quad (20)$$

where the features $h_j$ are positive numbers determined by the times $t_k$, and where the $B^k$ are real numbers determined by the normalization conditions $\langle \Psi^k | \Psi^k \rangle = 1$.

We show next how the features $h_k$ depend on the numbers of Grover iterations $t_k$.

### 2.1 General oracle

We will be using the following result of Biham et. al. [1]. Consider an oracle $O$, which accepts $r$ values (out of the total of $2^a N$, i.e., $\sum_{x=0}^{2^a N-1} O(x) = r$). We shall call such values of $x$ *good*, as opposed to *bad* values of $x$ that are rejected by the oracle. Using different notation for the coefficients of good and bad states, we have that after $t$ Grover iterations an arbitrary quantum state

$$|\Psi_{\text{ini}}\rangle = \sum_{\text{good } x} g_{x,\text{ini}} |x\rangle + \sum_{\text{bad } x} b_{x,\text{ini}} |x\rangle \quad (21)$$

is transformed into

$$|\Psi_{\text{fin}}\rangle = \hat{G}(O, t) |\Psi_{\text{ini}}\rangle = \sum_{\text{good } x} g_{x,\text{fin}} |x\rangle + \sum_{\text{bad } x} b_{x,\text{fin}} |x\rangle. \quad (22)$$

Let $g_{x,\text{ini}}$ and $b_{x,\text{ini}}$ be the averages of the initial amplitudes of the good and the bad states respectively:

$$g_{x,\text{ini}} = \frac{1}{r} \sum_{\text{good } x} g_{x,\text{ini}} , \quad b_{x,\text{ini}} = \frac{1}{2^a N - r} \sum_{\text{bad } x} b_{x,\text{ini}} , \quad (23)$$

and similarly for the final amplitudes

$$g_{x,\text{fin}} = \frac{1}{r} \sum_{\text{good } x} g_{x,\text{fin}} , \quad b_{x,\text{fin}} = \frac{1}{2^a N - r} \sum_{\text{bad } x} b_{x,\text{fin}} , \quad (24)$$
Let us also define
\[ \Delta g^\text{ini}_x = g^\text{ini}_x - \bar{g}^\text{ini} \]
\[ \Delta b^\text{ini}_x = b^\text{ini}_x - \bar{b}^\text{ini} . \] (25)

In other words, \( \Delta g^\text{ini}_x \) and \( \Delta b^\text{ini}_x \) define the features of the initial amplitude functions \( g^\text{ini}_x \) and \( b^\text{ini}_x \) relative to their averages \( \bar{g}^\text{ini} \) and \( \bar{b}^\text{ini} \cdot \) Biham et al. have shown that the change of the amplitudes is essentially determined by the change of the averages:
\[ g^\text{fin}_x = \bar{g}^\text{fin} + \Delta g^\text{ini}_x \]
\[ b^\text{fin}_x = \bar{b}^\text{fin} + (-1)^t \Delta b^\text{ini}_x , \] (26)

where the averages \( \bar{g}^\text{fin} \) and \( \bar{b}^\text{fin} \) are given as follows. Define
\[ \omega = \arccos \left( 1 - \frac{2r}{2^a N} \right) , \] (27)
\[ \alpha = \sqrt{\frac{\bar{b}^\text{ini}}{2^a N - r}} r , \] (28)
\[ \phi = \arctan \left( \frac{\bar{g}^\text{ini}}{\bar{b}^\text{ini} \sqrt{\frac{r}{2^a N - r}}} \right) . \] (29)

The averages are given by
\[ \bar{g}^\text{fin} = \sqrt{\frac{2^a N - r}{r}} \alpha \sin(\omega t + \phi) , \]
\[ \bar{b}^\text{fin} = \alpha \cos(\omega t + \phi) . \] (30)

These formulas allow us to calculate the number of Grover iterations \( t \) from the ratios \( \bar{g}^\text{ini} / \bar{b}^\text{ini} \) and \( \bar{g}^\text{fin} / \bar{b}^\text{fin} \) as follows. From Eqs. (30) we have
\[ \frac{g^\text{fin}}{b^\text{fin}} = \sqrt{\frac{2^a N - r}{r}} \tan(\omega t + \phi) , \] (31)
which, together with Eq. (29), gives
\[ \omega t = \arctan \left( \frac{\bar{g}^\text{fin}}{\bar{b}^\text{fin} \sqrt{\frac{r}{2^a N - r}}} \right) - \arctan \left( \frac{\bar{g}^\text{ini}}{\bar{b}^\text{ini} \sqrt{\frac{r}{2^a N - r}}} \right) . \] (32)

2.2 Formulas for \( t_k \)

Consider the state \( |\Psi^k\rangle \), i.e. the state that results after building the first \( k \) features using the oracles \( O_1, \ldots, O_k \). Let \( \bar{g}^\text{ini}_{k+1}, \bar{b}^\text{ini}_{k+1} \) be the average amplitudes of the “good” and “bad” states within \( |\Psi^k\rangle \) with respect to the oracle \( O_{k+1} \). By direct calculation we have
\[ \bar{g}^\text{ini}_{k+1} = \frac{\sum_{q_{1:k}} A_{q_{1:k}, q_{1:k+1}}^k N_{q_{1:k+1}}^{k+1}}{\sum_{q_{1:k}} N_{q_{1:k+1}}^{k+1}} , \]
\[ \bar{b}^\text{ini}_{k+1} = \frac{\sum_{q_{1:k}} A_{q_{1:k}, q_{1:k+1}}^k N_{q_{1:k+1}}^{k+1}}{\sum_{q_{1:k}} N_{q_{1:k+1}}^{k+1}}, \] (33)
and therefore
\[ \frac{\bar{g}^\text{ini}_{k+1}}{\bar{b}^\text{ini}_{k+1}} = \frac{(N - N_{k+1}) \sum_{q_{1:k}} A_{q_{1:k}, q_{1:k+1}}^k N_{q_{1:k+1}}^{k+1}}{N_{k+1} \sum_{q_{1:k}} A_{q_{1:k}, q_{1:k+1}}^k N_{q_{1:k+1}}^{k+1}} . \] (34)
Similarly, in the case of the final averages \( \bar{g}_{k+1}^{\text{fin}} \) and \( \bar{b}_{k+1}^{\text{fin}} \) we obtain

\[
\frac{\bar{g}_{k+1}^{\text{fin}}}{\bar{b}_{k+1}^{\text{fin}}} = \frac{(N - N_{k+1})}{N_{k+1}} \sum_{q_{1:k}} A_{q_{1:k}}^{k+1} N_{q_{1:k}}^{k+1} N_{q_{1:k}}^{k+1} \quad (35)
\]

Below we need expressions for the ratios \( \bar{g}_k^{\text{ini}}/\bar{b}_k^{\text{ini}} \) and \( \bar{g}_k^{\text{fin}}/\bar{b}_k^{\text{fin}} \), which follow by substituting \( k \) for \( k + 1 \). The number of Grover iterations, \( t_k \), required for converting the state \( |\Psi^{k-1}\rangle \) into \( |\Psi^k\rangle \) can then be obtained from Eq. \( \text{(32)} \),

\[
\omega_k t_k = \arctan \left( \frac{g_k^{\text{fin}}}{b_k^{\text{fin}}} \sqrt{\frac{N_k}{2^a N - N_k}} \right) - \arctan \left( \frac{g_k^{\text{ini}}}{b_k^{\text{ini}}} \sqrt{\frac{N_k}{2^a N - N_k}} \right), \quad (36)
\]

where

\[
\omega_k = \arccos \left( 1 - \frac{2N_k}{2^a N} \right). \quad (37)
\]

Of course these formulas for the integer times \( t_k \) are useless by themselves, because they depend on the coefficients \( A_{q_{1:k}}^{k} \), which are defined in terms of the unknown features \( h_k \) [see Eq. \( \text{(20)} \)]. The following argument leads to an explicit formula for the \( t_k \).

By construction of the sets \( \Omega_{q_{1:k}} \), the sums \( \sum_{j=1}^{k} q_j 2^{-j} / \sqrt{\eta N} \) are \( k \)-bit approximations to the target amplitudes \( \sqrt{p(x)} \) for all \( x \in \Omega_{q_{1:k}} \). We thus aim for the features \( h_j \) to be as close as possible to the values \( 2^{-j} / \sqrt{\eta N} \). This motivates the following choice for the \( t_k \).

Instead of the amplitudes \( \text{(20)} \), we define

\[
A_{q_{1:k}}^{t_k} = B^{t_k} + \sum_{j=1}^{k} q_j 2^{-j} / \sqrt{\eta N}, \quad (38)
\]

where the \( h_j \) have been replaced by \( 2^{-j} / \sqrt{\eta N} \), and where the terms \( B^{t_k} \) are determined by the normalization conditions \( \langle \Psi^{t_k} | \Psi^{t_k} \rangle = 1 \) for the states

\[
|\Psi^{t_k}\rangle = \sum_{q_{1:k}} \sum_{x \in \Omega_{q_{1:k}}} A_{q_{1:k}}^{t_k} |x\rangle. \quad (39)
\]

These states can be regarded as \( k \)-bit approximations to the intermediate states \( |\Psi^k\rangle \). We thus get the following modified expressions for the average amplitudes.

\[
\frac{\bar{g}_{k+1}^{\text{ini}}}{\bar{b}_{k+1}^{\text{ini}}} = \frac{(N - N_{k+1})}{N_{k+1}} \sum_{q_{1:k}} A_{q_{1:k}}^{t_k} N_{q_{1:k}}^{k+1} N_{q_{1:k}}^{k+1} \quad (40)
\]

and

\[
\frac{\bar{g}_{k+1}^{\text{fin}}}{\bar{b}_{k+1}^{\text{fin}}} = \frac{(N - N_{k+1})}{N_{k+1}} \sum_{q_{1:k}} A_{q_{1:k}}^{t_k+1} N_{q_{1:k}}^{k+1} N_{q_{1:k}}^{k+1}. \quad (41)
\]

The final expression for the times \( t_k \) is then

\[
t_k = \left[ \frac{1}{2} + \frac{1}{\omega_k} \left( \arctan \left( \frac{g_k^{\text{fin}}}{b_k^{\text{fin}}} \sqrt{\frac{N_k}{2^a N - N_k}} \right) - \arctan \left( \frac{g_k^{\text{ini}}}{b_k^{\text{ini}}} \sqrt{\frac{N_k}{2^a N - N_k}} \right) \right) \right], \quad (42)
\]
where the extra term 1/2 combined with the \([\ldots]\) operation amounts to a rounding to the nearest integer.

The expressions for \(t_k\) depend explicitly on the numbers \(N^{k}_{q_{1:k}}\), i.e., the numbers of points \(x\) for which the \(k\) most significant bits of \(\sqrt{\eta N p(x)}\) are given by \(q_{1:k}\). If this global information about the probabilities \(p(x)\) is available, the version of our state preparation algorithm described here will often be simpler than the original version of the algorithm described in Ref. [1]. If the numbers \(N^{k}_{q_{1:k}}\) are not available initially, they can be obtained via the quantum counting algorithm [10]. In this case, the algorithm described here loses much of its appeal. The analysis of the original algorithm in Ref. [1] includes bounds for the resources required for the initial quantum counting step.

### 2.3 Bound on the number of oracle calls

We have, by definition,

\[
\frac{2N_k}{2^a N} = 1 - \cos \omega_k = 2 \sin^2 \frac{\omega_k}{2} .
\]  
(43)

Since \(x^2 \geq \sin^2 x\) we obtain

\[
\omega_k \geq \sqrt{\frac{N_k}{2^a N}} .
\]  
(44)

Furthermore, we have

\[
\omega_k t_k \leq 2\pi ,
\]  
(45)

and hence

\[
t_k \leq \frac{2\pi}{\omega_k} \leq \pi \sqrt{\frac{2^a N}{N_k}} .
\]  
(46)

The overall number of oracle calls is therefore bounded by the expression \(T' + T \pi \sqrt{2^a N / N_k}\). A typical value for the fraction \(N_k / N\) is 1/2. The worst case for the number of oracle calls corresponds to \(N_k = 1\), which is equivalent to Grover database search [5]. The efficiency of our algorithm can be improved by ignoring very small values of \(N_k\). Bounds for the corresponding fidelity reduction have been derived in Ref. [1]. An analysis of the asymptotic number of oracle calls in the limit of large \(N\) is possible, e.g., for a sequence of states for which the parameter \(\eta\) does not depend on \(N\) and the ratios \(N_k / N\) tend to a constant \(C_k\) as \(N \to \infty\). In this case, the fidelity bound (56) does not depend on \(N\). For the right-hand side of the bound (46), we have then

\[
\pi \sqrt{\frac{2^a N}{N_k}} \to \pi \sqrt{2^a / C_k} \text{ as } N \to \infty ,
\]  
(47)

i.e., the bound for the required number of oracle calls tends to a constant for large \(N\).

### 3 Fidelity analysis

In this section we derive a lower bound for the fidelity \(|\langle \tilde{\Psi} | \Psi \rangle|\). We start by considering the fidelity between the real-amplitude target state \(|\Psi_r\rangle\) defined in Eq. (12) and the state \(|\Psi^T\rangle\) resulting from the Grover iterations, but before the \(a\) auxiliary qubits have been
measured [see Eq. (11)]. It follows from the discussion at the start of Sec. 2 that $|\Psi^T\rangle$ can be written in the form

$$|\Psi^T\rangle = \sum_{x=0}^{N-1} \left( B^T + \sum_{j=1}^{T} c_j(x) h_j \right) |x\rangle . \quad (48)$$

The first step is done in subsection 3.1 where we show that the choice Eq. (42) for the integer times $t_k$ implies that the features $h_k$, for $k = 1, \ldots, T$, satisfy the inequalities

$$|h_k - 2^{-k} \sqrt{\eta N}| < \frac{2^{1-a/2}}{\sqrt{\eta N}} . \quad (49)$$

Subsection 3.2 uses this result to derive the fidelity bound

$$|\langle \Psi_r | \Psi^T \rangle| = \sum_{x=0}^{N-1} \sqrt{p(x)} \left( B^T + \sum_{j=1}^{T} c_j(x) h_j \right)$$

$$= \sum_{x=0}^{N-1} \sqrt{p(x)} \left( B^T + \sum_{j=1}^{T} c_j(x) h_j \right)$$

$$> 1 - 3T \frac{2^{-a/2}}{\eta} , \quad (50)$$

where we have used the fact that $p(x) = 0$ for $x \geq N$, and where we have assumed that $T$ is chosen to be the smallest integer for which

$$\frac{2^{-T}}{2T^2} \leq 2^{-a} . \quad (51)$$

One can, of course, use bigger values of $T$, but this would not improve the performance of the algorithm as the fidelity of the state preparation is limited by the choice of $a$ [see Eq. (49)].

The next step of the algorithm is the measurement of the auxiliary qubits. The probability of failure, $p_{\text{fail}}$, i.e. the probability of obtaining a nonzero result, is given by

$$p_{\text{fail}} = (2^a N - N) |B^T|^2 , \quad (52)$$

where $B^T$ is the normalization term in the expression (48) for $|\Psi^T\rangle$. Subsection 3.2 derives the following bound on the failure probability.

$$p_{\text{fail}} \leq 16 T \frac{2^{-a/2}}{\eta} . \quad (53)$$

If there is no failure, i.e., if the measurement outcome is zero, the post-measurement state is given by

$$|\tilde{\Psi}_r\rangle = \frac{1}{\sqrt{1 - p_{\text{fail}}}} \sum_{x=0}^{N-1} \left( B^T + \sum_{j=1}^{T} c_j(x) h_j \right) |x\rangle . \quad (54)$$

Together with Eqs. (48) and (50) it follows directly that

$$|\langle \Psi_r | \tilde{\Psi}_r \rangle| = \frac{1}{\sqrt{1 - p_{\text{fail}}}} |\langle \Psi_r | \Psi^T \rangle| > 1 - 3T \frac{2^{-a/2}}{\eta} . \quad (55)$$
Finally, in subsection 3.3 we combine this bound with a simple analysis of the last stage in which the phases are added to the real amplitudes of the state $|\tilde{\Psi}_r\rangle$. The result is the following overall lower bound on the fidelity between the target state $|\Psi\rangle$ and the state $|\tilde{\Psi}\rangle$ prepared by the algorithm,

$$|\langle \tilde{\Psi} |\Psi \rangle| > \left(1 - 3T \frac{2^{-a/2}}{\eta} \right) \left(1 - 2^{-2T'-1} \right).$$

This bound determines the performance of the state preparation algorithm described in this paper.

### 3.1 Upper bound on $|h_k - 2^{-k}\sqrt{\eta N}|$

Consider the development of a single feature, $h$, in $t$ Grover iterations based on an oracle $O$. Let $r$ be the number of good states, or solutions, of $O$. It follows from Eqs. (30) that $h$ depends on $t$ via

$$h(t) = \alpha \sqrt{2^a N/r} \sin(\omega t - \xi),$$

where the values of $\alpha$ and $\xi$ depend on the initial average amplitudes $\bar{g}^{ini}$ and $\bar{b}^{ini}$ of the good and the bad states with respect to the oracle $O$. According to Eq. (28) we have

$$\alpha^2 = |\bar{b}^{ini}|^2 + |\bar{g}^{ini}|^2 \frac{r/N}{2^a - r/N}.$$  

(58)

The average amplitude of “bad” states is bounded as

$$\bar{b}^{ini} \leq \frac{1}{\sqrt{2^a N}},$$

and the maximum possible value of the average amplitude of “good” states is bounded as

$$\bar{g}^{ini} \leq \frac{1}{\sqrt{\eta N}}.$$  

(60)

Hence Eq. (58) implies

$$\alpha^2 \leq \frac{1}{2^a N} + \frac{r/N}{\eta N(2^a - r/N)}$$

$$\leq \frac{1}{2^a N} + \frac{1}{\eta N(2^a - 1)}$$

$$\leq \frac{1}{2^a N} + \frac{2}{\eta 2^a N}$$

$$< \frac{4}{\eta 2^a N}.$$  

(61)

Since in our algorithm the value of $t_k$ is rounded to the nearest integer, $h_k = h(t_k)$ will rarely coincide with the target value of $2^{-k}/\sqrt{\eta N}$. The mistake, however, can be bounded as

$$|h_k - 2^{-k}/\sqrt{\eta N}| \leq \max |h(t+1) - h(t)|,$$

(62)
where the maximum is taken with respect to the quantities $\alpha$, $\omega$, $\xi$, $r$ and $t$. The parameters characterizing the algorithm, $a$, $\eta$ and $N$, are being kept constant. Using (61) we obtain

$$
\left| h_k - \frac{2^{-k}}{\sqrt{\eta N}} \right| < \max \frac{2}{\sqrt{\eta N}} \left| \sin \left( (\omega t - \xi) + \omega \right) - \sin(\omega t - \xi) \right|
\leq \max \frac{2}{\sqrt{\eta N}} \sin(\omega/2),
$$

(63)

where the last inequality follows from the properties of the $\sin$ function. Since $0 \leq \omega \leq \pi$ we have

$$
\sin(\omega/2) = \sqrt{\frac{1 - \cos \omega}{2}} = \sqrt{\frac{r}{2aN}},
$$

(64)

which implies the bound

$$
\left| h_k - \frac{2^{-k}}{\sqrt{\eta N}} \right| < \frac{2^{1-a/2}}{\sqrt{\eta N}}
$$

(65)

as required.

### 3.2 Lower bound on $|\langle \Psi_r | \Psi^T \rangle|$}

Directly from the definitions we have

$$
\langle \Psi_r | \Psi^T \rangle = \sum_{x=0}^{2^aN-1} \sqrt{p(x)} \left( B^T + \sum_{j=1}^{T} c_j(x) h_j \right) 
= \sum_{x=0}^{N-1} \sqrt{p(x)} \left( B^T + \sum_{j=1}^{T} c_j(x) \frac{2^{-j}}{\sqrt{\eta N}} + \sum_{j=1}^{T} c_j(x) \left( h_j - \frac{2^{-j}}{\sqrt{\eta N}} \right) \right),
$$

(66)

where we have used the fact that $p(x) = 0$ for $x \geq N$. Let us define

$$
b(x) = \sum_{j=T+1}^{\infty} c_j(x) \frac{2^{-j}}{\sqrt{\eta N}}, \quad \delta(x) = \sum_{j=1}^{T} c_j(x) \left( h_j - \frac{2^{-j}}{\sqrt{\eta N}} \right).
$$

(67)

Since

$$
\sum_{j=1}^{T} c_j(x) \frac{2^{-j}}{\sqrt{\eta N}} = \sqrt{p(x)} - b(x),
$$

(68)

and since $\sum_{x=0}^{N-1} p(x) = 1$ we have

$$
|\langle \Psi_r | \Psi^T \rangle| \geq 1 - \left| \sum_{x=0}^{N-1} \sqrt{p(x)} \left( B^T - b(x) \right) \right| - \sum_{x=0}^{N-1} \sqrt{p(x)} \left| \delta(x) \right|.
$$

(69)

Using the bound (65), one can show that

$$
|\delta(x)| \leq 2T \frac{2^{-a/2}}{\sqrt{\eta N}},
$$

(70)
and therefore, using $\sqrt{p(x)} \leq 1/\sqrt{\eta N}$,
\[
|\langle \Psi_r | \Psi^T \rangle| \geq 1 - \left| \sum_{x=0}^{N-1} \sqrt{p(x)} \left( B^T - b(x) \right) \right| - 2 T^{2-a/2} / \eta. \tag{71}
\]

The function $b(x)$ satisfies the bounds
\[
0 \leq b(x) \leq 2^{-T} / \sqrt{\eta N}. \tag{72}
\]

In order to find the lower bound on $|\langle \Psi_r | \Psi^T \rangle|$ from Eq. (71) we need to calculate $|B^T|$. This can be done by examining the normalization condition $\langle \Psi^T | \Psi^T \rangle = 1$ which reads
\[
\sum_{x=0}^{2^a N - 1} \left( B^T + \sum_{j=1}^T c_j(x) h_j \right)^2 = 1. \tag{73}
\]

Using the definitions (67), this can be rewritten as
\[
\sum_{x=0}^{2^a N - 1} \left( B^T + \sqrt{p(x)} - b(x) + \delta(x) \right)^2 = 1. \tag{74}
\]

This leads to a quadratic equation for $B^T$:
\[
(B^T)^2 + 2 U B^T + V = 0, \tag{75}
\]

where
\[
U = \frac{1}{2^a N} \sum_{x=0}^{N-1} \left( \sqrt{p(x)} + \delta(x) - b(x) \right), \tag{76}
\]

\[
V = \frac{1}{2^a N} \sum_{x=0}^{N-1} \left( 2 \sqrt{p(x)} + \delta(x) - b(x) \right) \left( \delta(x) - b(x) \right). \tag{77}
\]

Since $\sqrt{p(x)} - b(x) \geq 0$, using the inequalities (70) and (72) together with the bound $\sqrt{p(x)} \leq 1/\sqrt{\eta N}$ we obtain
\[
-2 T^{2-3a/2} / \sqrt{\eta N} \leq U \leq \frac{2-a}{\sqrt{\eta N}} \left( 1 + 2 T 2^{-a/2} \right), \tag{78}
\]
\[
-4 T \frac{2-a}{\eta N} \left( \frac{2-T}{2T} + 2^{-a/2} \right) \leq V \leq 4 T \frac{2-3a/2}{\eta N} \left( 1 + T 2^{-a/2} \right). \tag{79}
\]

As mentioned earlier, we assume that $T$ is chosen to be the smallest integer for which
\[
\frac{2-T}{2T^2} \leq 2^{-a}. \tag{80}
\]

The above bounds can then be simplified as follows.
\[
|U| \leq \frac{2}{\sqrt{\eta N}}, \tag{81}
\]
\[
|V| \leq 8 T \frac{2^{-3a/2}}{\eta N}. \tag{82}
\]
The value of $B^T$ therefore satisfies the bound
\[
|B^T| \leq |U| + \sqrt{U^2 + |V|} \\
\leq 2 \frac{2^{-a}}{\sqrt{\eta N}} + \sqrt{9T \cdot 2^{-3a/2}}/(\eta N) \\
\leq 4 \sqrt{T} \frac{2^{-3a/4}}{\sqrt{\eta N}}. \quad (83)
\]

Using this bound together with (72) we obtain from Eq. (71) the result
\[
|\langle \Psi_r | \Psi^T \rangle| \geq \left( 1 - \frac{1}{\sqrt{\eta}} \right) \left( 4 \sqrt{T} 2^{-3a/4} + 2^{-T} + 2T 2^{-a/2} \right) \\
> 1 - 3T \frac{2^{-a/2}}{\eta}. \quad (84)
\]

Directly from Eq. (83) we obtain the upper bound on the failure probability,
\[
p_{\text{fail}} = (2^a N - N)|B^T|^2 \leq 16 \frac{2^{-a/2}}{\eta}. \quad (85)
\]

### 3.3 Adding phases

The state $|\tilde{\Psi}_r\rangle$ resulting from the measurement of the $a$ auxiliary qubits has real amplitudes, i.e., it is of the form
\[
|\tilde{\Psi}_r\rangle = \sum_x \sqrt{\tilde{p}(x)} |x\rangle. \quad (86)
\]

The final stage of the algorithm, see Eq. (13), turns $|\tilde{\Psi}_r\rangle$ into the final state $|\tilde{\Psi}\rangle$, which can be written as
\[
|\tilde{\Psi}\rangle = \sum_x \sqrt{\tilde{p}(x)} \exp[2\pi i \tilde{\phi}(x)] |x\rangle, \quad (87)
\]

where the $\tilde{\phi}(x)$ are $T'$-bit approximations to the target phases $\phi(x)$, i.e.,
\[
|\phi(x) - \tilde{\phi}(x)| \leq 2^{-T'}. \quad (88)
\]

Putting everything together, we find
\[
|\langle \tilde{\Psi} | \Psi \rangle| = \left| \sum_x \sqrt{p(x)\tilde{p}(x)} \exp[2\pi i (\phi(x) - \tilde{\phi}(x))] \right| \\
\geq \sum_x \sqrt{p(x)\tilde{p}(x)} \cos[\phi(x) - \tilde{\phi}(x)] \\
\geq \sum_x \sqrt{p(x)\tilde{p}(x)} \left( 1 - [\phi(x) - \tilde{\phi}(x)]^2 / 2 \right) \\
\geq \sum_x \sqrt{p(x)\tilde{p}(x)} \left( 1 - 2^{-2T' - 1} \right) \\
= |\langle \Psi_r | \tilde{\Psi}_r \rangle| \left( 1 - 2^{-2T' - 1} \right) \\
> \left( 1 - 3T \frac{2^{-a/2}}{\eta} \right) \left( 1 - 2^{-2T' - 1} \right), \quad (89)
\]

which is the required lower bound for the overall fidelity of the prepared state.
References

[1] A. N. Soklakov and R. Schack, e-print quant-ph/0408045

[2] S. Lloyd, Science 273, 1073 (1996).

[3] C. Zalka, Proc. R. Soc. Lond. A 454, 313 (1998).

[4] S. S. Somaroo, C.-H. Tseng, T. F. Havel, R. Laflamme, and D. G. Cory, Phys. Rev. Lett. 82, 5381 (1999).

[5] L. K. Grover, Phys. Rev. Lett. 79, 325 (1997).

[6] P. Kaye and M. Mosca, in Proceedings, International Conference on Quantum Information (Rochester, New York, 2001), e-print quant-ph/0407102.

[7] L. Grover and T. Rudolph, e-print quant-ph/0208112.

[8] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, Proc. R. Soc. Lond. A 454, 339 (1998).

[9] E. Biham, O. Biham, D. Biron, M. Grassl, and D. A. Lidar, Phys. Rev. A 60, 2742 (1999).

[10] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, Fortschr. Phys. 46, 493 (1998).