Quantum query complexity and distributed computing
Röhrig, H.P.

Citation for published version (APA):
In this chapter we present research inspired by Grover's seminal quantum search algorithm [69]. In Section 2.1 we review the basic search algorithm and its generalization to amplitude amplification. An application for computing convolution products is proposed in Section 2.2. In Section 2.3 we express the iteration of the search algorithm in terms of density matrices, so that we can analyze its performance in the presence of decoherence. Nonclassical databases are the point of departure for the considerations in Section 2.4, where we derive algorithms to compare the degeneracy of energy levels of a given Hamiltonian. Section 2.4 is based on joint work with Ozhigov [94]; Sections 2.2 and 2.3 are unpublished so far.

2.1 Quantum Amplitude Amplification

2.1.1 Grover's algorithm

Unordered search is the problem of finding a database entry matching the search criteria merely by using queries of the type "does entry $j$ match?" An example is finding a name in a telephone directory given a phone number. The telephone directory is ordered by name and the phone numbers are practically random. It is easy to see that classically, even with randomization, $\Omega(N)$ queries are required on average in an $N$-entry telephone directory.

Database query The algorithm makes use of the function $f : \{1, \ldots, N\} \rightarrow \{0, 1\}$, where $f(j) = 1$ if and only if $j$ is the index we are looking for, i.e., PhoneNumber($j$) = 736-5000. In the following we assume that $N = 2^n$ for some $n \in \mathbb{N}$ and we identify the domain of $f$ with $\{0, 1\}^n$; since the input is unordered, there is no structure to be respected. Recall that in Subsection 1.3.2
Figure 2.1: The initial state of quantum search for $N = 8$ and $f(j) = \delta_{j,3}$. The bars give the amplitudes $\alpha_j$ of the state $\sum_j \alpha_j |j\rangle |-)$. We defined a quantum query to $f$ as the unitary transformation

$$U_f : |j\rangle |b\rangle \mapsto |j\rangle |f(j) \oplus b\rangle .$$

The idea of quantum search is to start with a uniform superposition of indices

$$|\psi_0\rangle := \frac{1}{\sqrt{N}} \sum_{j \in \{0,1\}^n} |j\rangle ,$$

representing the initial knowledge about the $j$ with $f(j) = 1$ and to progressively "transfer" amplitude from basis states $|j'\rangle$ with $f(j') = 0$ to basis states $|j\rangle$ with $f(j) = 1$. The operations have to be unitary and what counts is how often the query gate $U_f$ is invoked. In $|\psi_0\rangle$ and throughout the quantum-search algorithm, the amplitudes of the basis vectors are real and therefore we can represent them as a bar chart like the example in Figure 2.1. We saw in Subsection 1.3.2 that by initializing the last qubit to $|-> := (|0\rangle - |1\rangle)/\sqrt{2}$ we can realize the mapping

$$|j\rangle |-> \mapsto (-1)^{f(j)} |j\rangle |->$$

using one invocation of $U_f$. This flips the amplitude of the $|j\rangle$ with $f(j) = 1$ from $1/\sqrt{N}$ to $-1/\sqrt{N}$.

**Reflection about the average** This substantial change in phase can be translated to a change in absolute value by performing a reflection about the average operation as outlined in the step from Figure 2.2(a) to Figure 2.2(b). On input $|\psi\rangle = \sum_j \alpha_j |j\rangle$, it maps each individual amplitude $\alpha_j$ to $\bar{\alpha} - (\alpha_j - \bar{\alpha}) = 2\bar{\alpha} - \alpha_j$ where $\bar{\alpha} := (1/N) \sum_j \alpha_j$ is the average of the $\alpha_j$ and $(\alpha_j - \bar{\alpha})$ is the deviation of $\alpha_j$ from the average. It turns out that this operation is unitary and can be implemented efficiently without any $U_f$ gate;

$$T_0 := -WS_0W$$
2.1. Quantum amplitude amplification

Figure 2.2: The first iterations of quantum search ($N = 8$ and $f(j) = \delta_{j,3}$). The bars give the amplitudes $\alpha_j$ of the state $\sum_j \alpha_j |j\rangle |\rangle$; the dashed line indicates the average.
achieves the desired result. Here $W := H^\otimes n$ denotes a Hadamard transform on all $n$ qubits individually and

$$S_0 := 1 - 2|0\rangle\langle 0| = \begin{pmatrix} -1 & 1 & \cdots & 1 \\ & 1 & & \\ & & & \ddots \\ & & & & 1 \end{pmatrix}$$

changes the phase of the $|0^n\rangle$ basis state by a factor of $-1$, leaving all other basis states unchanged. To see that $T_0$ implements the reflection about the average, note that

$$T_0|\psi\rangle = -(1 + 2W|0\rangle\langle 0|W)|\psi\rangle$$

$$= -\sum_j \alpha_j|j\rangle + 2 \left( \frac{1}{\sqrt{N}} \sum_k |k\rangle \right) \left( \frac{1}{\sqrt{N}} \sum_\ell \langle \ell | \right) \sum_m \alpha_m|m\rangle.$$

$$= \sum_j \left( \frac{2N}{N} \left( \sum_m \alpha_m \right) - \alpha_j \right)|j\rangle = \sum_j (2\alpha - \alpha_j)|j\rangle. \quad (2.1)$$

What is the gain in amplitude? For a single $j$ with $f(j) = 1$, the amplitude $\alpha_j = -1/\sqrt{N}$ is mapped to

$$\frac{2}{N} \left( (N - 1) \frac{1}{\sqrt{N}} - \frac{1}{\sqrt{N}} \right) - \left( -\frac{1}{\sqrt{N}} \right) > \frac{2}{\sqrt{N}}.$$ 

Hence, the amplitude of basis state $|j\rangle$ increased by an additive term of more than $1/\sqrt{N}$.

So far, we prepared the uniform superposition, performed one query and the “reflection about the average” operation; this corresponds to the unitary operator

$$G := (T_0 \otimes 1) U_f$$

applied to the initial state

$$|\psi_0\rangle := (W \otimes H)|0^n1\rangle = \frac{1}{\sqrt{N}} \sum_j |j\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle). \quad (2.2)$$

One application of $G$ improves our success probability. It is natural to ask whether repeating $G$ is helpful; an oblivious phase-flip followed by the reflection operation should boost the amplitude of the states $|j\rangle$ with $f(j) = 1$. Indeed, these iterations are at the heart of Grover’s algorithm. It remains to determine a judicious number of repetitions $r$ so that when measuring $G^r|\psi_0\rangle$ the probability of observing $j$ with $f(j) = 1$ is large.
2.1. Quantum amplitude amplification

Two-dimensional evolution The observation that an iteration of the algorithm treats basis states $|j\rangle$ with the same value of $f$ the same leads to an elegant way to analyze the behavior of the algorithm [24]. Let $M := |\{j : f(j) = 1\}|$ denote the number of solutions and

$$|\chi\rangle := \frac{1}{\sqrt{M}} \sum_{j : f(j) = 1} |j\rangle H|1\rangle \quad \text{and} \quad |\chi^+\rangle := \frac{1}{\sqrt{N-M}} \sum_{j : f(j) = 0} |j\rangle H|1\rangle \quad (2.3)$$

the uniform superposition of “good” and “bad” basis states, respectively. The initial state from Equation (2.2) is a superposition of those states:

$$|\psi_0\rangle = \sqrt{\frac{M}{N}} |\chi\rangle + \sqrt{\frac{N-M}{N}} |\chi^+\rangle \quad . \quad (2.4)$$

From Equation (2.1) we obtain

$$G|\chi\rangle = -T_0|\chi\rangle = \left(1 - \frac{2M}{N}\right) |\chi\rangle - \frac{2\sqrt{M(N-M)}}{N} |\chi^+\rangle$$

and

$$G|\chi^+\rangle = T_0|\chi^+\rangle = \frac{2\sqrt{M(N-M)}}{N} |\chi\rangle + \left(-1 + \frac{2N-M}{N}\right) |\chi^+\rangle \quad .$$

Hence, one iteration $G$ can be expressed as a mapping in the two-dimensional subspace spanned by $|\chi\rangle$ and $|\chi^+\rangle$. For $|\psi\rangle = \alpha|\chi\rangle + \beta|\chi^+\rangle$, $\alpha, \beta \in \mathbb{C}$, we get

$$G|\psi\rangle = (|\chi\rangle \ |\chi^+\rangle) \hat{G} \left(\begin{array}{c} \alpha \\ \beta \end{array}\right)$$

where the first matrix product on the right-hand side is to be interpreted formally as $(|\chi\rangle \ |\chi^+\rangle) (\alpha' \ \beta')^T = \alpha'|\chi\rangle + \beta'|\chi^+\rangle$ and $\hat{G}$ is the two-dimensional version of $G$,

$$\hat{G} = \frac{1}{N} \begin{pmatrix} N-2M & 2\sqrt{M(N-M)} \\ -2\sqrt{M(N-M)} & N-2M \end{pmatrix}$$

We are interested in $\hat{G}^r$, which describes the effect of $r$ iterations of $G$ in the two-dimensional subspace spanned by $|\chi\rangle$ and $|\chi^+\rangle$. $\hat{G}$ is a real unitary matrix, therefore it is a rotation in the real plane, possibly combined with a reflection. Choosing the smallest $\vartheta \geq 0$ such that $\cos \vartheta = (N - 2M)/N$,

$$\hat{G} = \begin{pmatrix} \cos \vartheta & \sin \vartheta \\ -\sin \vartheta & \cos \vartheta \end{pmatrix} \quad \text{and therefore} \quad \hat{G}^r = \begin{pmatrix} \cos(r\vartheta) & \sin(r\vartheta) \\ -\sin(r\vartheta) & \cos(r\vartheta) \end{pmatrix}$$
Using the same substitution and the observation that \( 1 + \cos^2(\theta/2) = 2 \cos \theta \), the initial state from Equation (2.4) becomes

\[
|\psi_0\rangle = \sin(\theta/2)|\chi\rangle + \cos(\theta/2)|\chi^\perp\rangle = (|\chi\rangle \quad |\chi^\perp\rangle) \begin{pmatrix} \sin(\theta/2) \\ \cos(\theta/2) \end{pmatrix}
\]  

(2.5)

The probability of obtaining a measurement outcome \( j \) with \( f(j) = 1 \) after \( r \) iterations is

\[
\left| \sum_{j: f(j) = 1} |j\rangle \langle j^*|G^r|\psi_0\rangle \right|^2 = \left| \begin{pmatrix} 1 & 0 \\ 0 & \hat{G}^r \end{pmatrix} \begin{pmatrix} \sin(\theta/2) \\ \cos(\theta/2) \end{pmatrix} \right|^2
\]

\[
= |\cos(r\theta) \sin(\theta/2) + \sin(r\theta) \cos(\theta/2)|^2
\]

\[
= \sin^2 \left( \left( r + \frac{1}{2} \right) \theta \right). \tag{2.6}
\]

The last transformation uses the trigonometric identity

\[
\sin(\alpha + \beta) = \cos \alpha \sin \beta + \sin \alpha \cos \beta.
\]

**Success probability**  From Equation (2.6) it follows that the success probability of quantum search is periodic in \( r \); when \((r + 1/2)\theta \approx \pi/2\), we have a high probability of obtaining a good measurement outcome. The first maximum is at \( r_{\text{opt}} = \pi/(2\theta) - 1/2 + \Delta \) for \( \Delta \in \mathbb{R} \) with \(|\Delta| \leq 1/2 \) that ascertains that \( r_{\text{opt}} \) is an integer. For \( \theta \leq \pi/2 \), we can bound the success probability as follows:

\[
\sin^2 \left( \left( r_{\text{opt}} + \frac{1}{2} \right) \theta \right) = \sin^2 \left( \frac{\pi}{2} + \Delta \theta \right) = 1 - \sin^2 (\Delta \theta) \geq 1 - \frac{\theta^2}{4} \geq \frac{1}{3}
\]

whereas \( \theta > \pi/2 \) implies \( 2M > N \) and \( r_{\text{opt}} = 0 \). Since in this case, measuring the initial state gives success probability greater than 1/2, we have constant success probability in all cases.

To obtain an asymptotic bound on \( r \) in terms of \( N \) and \( M \), let \( \theta' := 2\sqrt{M/N} \). Since \( x \geq \sin x \) for \( x \geq 0 \), we have

\[
\frac{\theta}{2} \geq \sin \left( \frac{\theta}{2} \right) = \sqrt{\frac{M}{N}} = \theta'
\]

where the first equality is as in Equation (2.5). Hence, \( \theta \geq \theta' \) and

\[
r_{\text{opt}} \leq \left\lfloor \frac{\pi}{4} \sqrt{\frac{N}{M}} \right\rfloor.
\]

For our telephone-directory example, this implies that using quantum queries we can find the single matching entry with high probability using \( O(\sqrt{N}) \) quantum queries.
2.1. Quantum amplitude amplification

<table>
<thead>
<tr>
<th>“mixing” operator</th>
<th>Grover’s algorithm</th>
<th>amplitude amplification</th>
</tr>
</thead>
<tbody>
<tr>
<td>initial state</td>
<td>$W \otimes \mathbb{1}$</td>
<td>arbitrary unitary operator $A$</td>
</tr>
<tr>
<td>first phase flip</td>
<td>query $U_f$</td>
<td>$A</td>
</tr>
<tr>
<td>second phase flip</td>
<td>$1 - 2</td>
<td>0\rangle\langle 0</td>
</tr>
</tbody>
</table>

Table 2.1: From Grover’s algorithm to amplitude amplification

Tuning  So far, we need to know the number of solutions $M$ in order to determine the sufficient number of iterations. For $M$ unknown, there are ways using doubling techniques [24] to find a solution with an expected number of queries $O(\sqrt{N/M})$. If $M$ is known, the success probability of the quantum-search algorithm can be improved to 1, e.g., by changing the $\theta$ for the last iteration [26, 28]. With regard to lower bounds, Grover’s algorithm and its extensions have been shown to be optimal in many respects [20, 120, 30].

2.1.2 Amplitude amplification

The preceding analysis of the quantum-search algorithm hinged on the fact that iterations of the quantum-search algorithm can be expressed as rotations in a plane spanned by “good” and “bad” states. “Amplitude amplification” is a general framework [27, 70] for increasing the amplitude of “good” states when those can be recognized efficiently.

The framework  The generalization from Grover’s algorithm to amplitude amplification is outlined in Table 2.1. The only operator that is genuinely quantum in Grover’s algorithm is the Hadamard transform. Let us investigate what happens if we replace it by an arbitrary unitary operator $A$, start on an arbitrary quantum state $|\psi_0\rangle$, and use an arbitrary orthonormal family $F := \{|\varphi_x\rangle : x \in X\}$ as the set of “good” states. The iteration of Grover’s algorithm began with a database query $U_f$, which effectively flipped the sign of the good states. So now we just perform an analogous step, namely applying the operator

$$S_F := 1 - 2 \sum_{x \in X} |\varphi_x\rangle\langle \varphi_x| .$$

The next step in the iteration was to reflect the amplitudes about their average, realized by a phase-flip in the $W$-basis. We mimic the property that the “reflection about the average” flips the phase of the initial state and leaves all orthogonal states invariant by defining the new

$$T_{\psi_0} := -A(1 - 2|\psi_0\rangle\langle \psi_0|)A^{-1} .$$
What properties does our new iteration operator $Q := T_{\psi_0} S_T$ have when applied repeatedly to the initial state $A|\psi_0\rangle$? Our definitions are validated insofar as we can repeat the analysis in two-dimensions: in analogy to (2.3) define the “good” and “bad” portions of $A|\psi_0\rangle$ as

$$|\bar{\chi}\rangle := \sum_{x \in X} |\varphi_x\rangle\langle\varphi_x|A|\psi_0\rangle \quad \text{and} \quad |\bar{\chi}^\perp\rangle := \left(1 - \sum_{x \in X} |\varphi_x\rangle\langle\varphi_x|\right)A|\psi_0\rangle$$

and with $a := \sqrt{\langle\bar{\chi}|\bar{\chi}\rangle}$ normalize to

$$|\chi\rangle := \frac{1}{a}|\bar{\chi}\rangle \quad \text{and} \quad |\chi^\perp\rangle := \frac{1}{\sqrt{1 - a^2}}|\bar{\chi}^\perp\rangle.$$

Then by simple arithmetic we obtain

$$A|\psi_0\rangle = |\bar{\chi}\rangle + |\bar{\chi}^\perp\rangle = a|\chi\rangle + \sqrt{1 - a^2}|\chi^\perp\rangle,$$

$$Q|\chi\rangle = \frac{1}{a} \left(A(1 - 2|\psi_0\rangle\langle\psi_0|)A^{-1} \sum_{x \in X} |\varphi_x\rangle\langle\varphi_x|A|\psi_0\rangle\right)$$

$$= |\chi\rangle - 2aA|\psi_0\rangle = (1 - 2a^2)|\chi\rangle - 2a\sqrt{1 - a^2}|\chi^\perp\rangle,$$

and

$$Q|\chi^\perp\rangle = \frac{1}{\sqrt{1 - a^2}} \left(-A(1 - 2|\psi_0\rangle\langle\psi_0|)A^{-1} \left(1 - \sum_{x \in X} |\varphi_x\rangle\langle\varphi_x|\right)A|\psi_0\rangle\right)$$

$$= -|\chi^\perp\rangle + 2\sqrt{1 - a^2}A|\psi_0\rangle = 2a\sqrt{1 - a^2}|\chi\rangle + (1 - 2a^2)|\chi^\perp\rangle,$$

so that we can again define a two-dimensional rotation

$$Q := \begin{pmatrix} 1 - 2a^2 & 2a\sqrt{1 - a^2} \\ -2a\sqrt{1 - a^2} & 1 - 2a^2 \end{pmatrix}$$

with

$$Q(\alpha|\chi\rangle + \beta|\chi^\perp\rangle) = (|\chi\rangle \quad |\chi^\perp\rangle)Q \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

Hence, with the smallest $\theta \geq 0$ such that $a = \sin(\theta/2)$, $Q$ is a rotation by $\theta$ and after at most $[\pi/4\alpha]$ iterations we are close to the good states in the sense that measuring the observable $\sum_{x \in X} |\varphi_x\rangle\langle\varphi_x|$ will yield outcome 1 with constant probability and in this case project the state into the subspace spanned by the $\{|\varphi_x\rangle : x \in X\}$. 


2.1. Quantum amplitude amplification

Applications So what is amplitude amplification good for? Clearly, it generalizes quantum search. Furthermore, we can amplify the success probability of an arbitrary quantum algorithm if the following conditions are met:

1. the initial state of the algorithm is a pure state $|\psi_0\rangle$ and we have a transformation $S_{\psi_0} = 1 - 2|\psi_0\rangle\langle\psi_0|;$

2. the algorithm only uses unitary gates and in particular does not make any measurements;

3. there is a projective measurement $\{P_{\text{success}}, 1 - P_{\text{success}}\}$ that determines for an output whether the run was successful or not, and we have the corresponding unitary transform $S_F = 1 - 2P_{\text{success}}.$

By Condition 2, the algorithm corresponds to an overall unitary operator $A.$ On initial state $|\psi_0\rangle,$ the success probability is $p_{\text{success}} := \|P_{\text{success}}A|\psi_0\rangle\|^2$ according to Condition 3. We fit this into the amplitude-amplification framework by letting the set of good states $F = \{|\varphi_x\rangle : x \in X\}$ be a basis of the range of $P_{\text{success}}.$ Then $P_{\text{success}} = \sum_{x \in X} |\varphi_x\rangle\langle\varphi_x|,$ $S_F = 1 - 2\sum_{x \in X} |\varphi_x\rangle\langle\varphi_x|,$ and $a = \|P_{\text{success}}A|\psi_0\rangle\| = \sqrt{p_{\text{success}}}.\,$ Hence, applying amplitude amplification we can boost a small $p_{\text{success}}$ to constant in $O(1/\sqrt{p_{\text{success}}})$ iterations, whereas classically, boosting the success probability of algorithms that indicate whether they were successful takes

$$1 - (1 - p_{\text{success}})^r \geq c \quad \Rightarrow \quad r = \Omega\left(\frac{1}{p}\right)$$

repetitions.

For a concrete example, consider the following instance of the claw-finding problem, derived as a special case from [32]: given two functions $f$ and $g$ with domain $[N] = \{1, \ldots, N\},$ find $x$ and $y \in [N]$ with $f(x) = g(y).$ Our quantum algorithm $A$ selects uniformly at random a set $I \subseteq [N]$ of size $|I| = \sqrt{N}.$ It queries $f$ on all $x \in I$ and uses this to construct an oracle $h : [N] \rightarrow \{0, 1\}$ for quantum search on $g$ by defining for $h(y) = 1 \Leftrightarrow \exists x \in I : f(x) = g(y).$ Evaluating $h$ takes one query to $g$ and no query to $f.$ $A$ then performs quantum search for $h(y) = 1.$ This takes $|I| = \sqrt{N}$ queries to $f$ and $O(\sqrt{N})$ queries to $h$ and thus to $g.$ $A$ finds a claw $f(x) = f(y)$ if it chose $I$ such that $x \in I$ and if the quantum search was successful. This happens with probability $(|I|/N) \cdot \text{const} = \Omega(1/\sqrt{N}).$ Now we use amplitude amplification on $A$ to boost the success probability to constant in $O(N^{1/4})$ iterations, performing in total $O(N^{1/4 + 1/2}) = O(N^{3/4})$ queries. Since this is a special case of quantum search, classically $\Omega(N)$ queries are necessary in the worst case. The best known quantum upper bound to date is $O(N^{2/3})$ [9].
2.2 Convolution Products

Can a quantum computer speed up multiplication or applications relying on multiplication? This question, the efficient quantum Fourier transform [46, 108, 50, 44], and the utility of convolution products, e.g., for pattern matching, were our motivations for examining computing convolution products on a quantum computer.

Convolution and the discrete Fourier transform For two vectors \( a = (a_0 \cdots a_{N-1}) \) and \( b = (b_0 \cdots b_{N-1}) \), the convolution product is

\[
a \ast b = (c_0 \cdots c_{N-1})
\]

with

\[
c_j = \sum_{k, k': k + k' = j} a_k b_{k'} \quad \text{(2.7)}
\]

Evidently, \( c \) is just the vector of coefficients of the polynomial

\[
\left( \sum_{k=0}^{N-1} a_k x^k \right) \left( \sum_{k'=0}^{N-1} b_{k'} x^{k'} \right).
\]

Computing \( c \) directly via Equation (2.7) requires \( \Omega(N^2) \) arithmetic operations. This can be reduced to \( O(N \log N) \) operations using the discrete Fourier transform and its inverse. Let \( \omega \) denote the \( N \)th root of unity \( \omega = e^{2\pi i/N} \). The discrete Fourier transform is the mapping

\[
\text{DFT} : a \mapsto \hat{a} := (\hat{a}_0 \cdots \hat{a}_{N-1}) \quad \text{with} \quad \hat{a}_\ell = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} a_k \omega^{k\ell} \quad \text{(2.8)}
\]

and its inverse is

\[
\text{DFT}^{-1} : \hat{a} \mapsto a := (a_0 \cdots a_{N-1}) \quad \text{with} \quad a_\ell = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \hat{a}_k \omega^{-k\ell} \quad \text{(2.9)}
\]

First, we compute \( \hat{a} \) and \( \hat{b} \). Then we compute the product of \( \hat{a} \) and \( \hat{b} \) component by component, i.e.,

\[
\hat{c} = (\hat{a}_0 \hat{b}_0 \cdots \hat{a}_{N-1} \hat{b}_{N-1})
\]

and use the inverse Fourier transform to obtain \( c \) with

\[
c_\ell = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \hat{a}_k \hat{b}_k \omega^{-k\ell}
\]
2.2. Convolution products

\[
\begin{align*}
&\quad = \frac{1}{N^{3/2}} \sum_{k', k''=0}^{N-1} a_{k'} b_{k''} \sum_{k=0}^{N-1} \omega^{k(k'+k''-t)} \\
&\quad = \frac{1}{\sqrt{N}} \sum_{(k', k'') \in \Sigma(t)} a_{k'} b_{k''},
\end{align*}
\]

with \( \Sigma(t) = \Sigma_2(t) \) and \( \Sigma_t(\ell) := \{(i_1, \ldots, i_N) : 0 \leq i_j < N \text{ for all } j \text{ and } \sum i_j = \ell \text{ mod } N\} \); we drop the subscript from \( \Sigma_t(\ell) \) whenever \( t \) is evident from the context.

Hence, if \( a_k = b_k = 0 \) for \( k > N/2 \), then \( \sqrt{N}c = a \ast b \). The fast Fourier transform algorithm [45] computes the discrete Fourier transform or its inverse in \( O(N \log N) \) steps, therefore we can compute the convolution product with \( O(N \log N) \) steps as well.

Quantum Fourier transform In the setting of quantum circuits, the vectors \( a, b, c \), etc. from the preceding paragraphs map in a natural way to quantum states, e.g.,

\[
|\psi_a\rangle := \sum_{k=0}^{N-1} a_k |k\rangle.
\]

Moreover, as defined in Equation (2.8) the discrete Fourier transform is a unitary transformation. The corresponding quantum operation

\[
\text{QFT} : |j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{kj} |k\rangle
\]

is called the quantum Fourier transform. That it can be approximated efficiently with \( O(\log N \log \log N) \) operations [46, 108, 50] is the foundation of many quantum algorithms.

Keeping this in mind, it is straightforward to compute convolution products on a quantum computer by transforming the input state

\[
|\psi_{\text{input}}\rangle := \left( \sum_{k=0}^{N-1} a_k |k\rangle \right) \otimes \left( \sum_{k'=0}^{N-1} b_{k'} |k'\rangle \right)
\]

into

\[
|\psi_{\text{output}}\rangle := \left( \sum_{j=0}^{N-1} \left( \sum_{(k, k') \in \Sigma(j)} a_k b_{k'} \right) |j\rangle \right) \otimes |\text{rest}\rangle,
\]

where \( N = 2^n \) and \( |k\rangle, |k'\rangle, |j\rangle, \) and \( |\text{rest}\rangle \) are \( n \)-bit quantum registers. These vectors are not necessarily normalized; note, however, that we need to require
that \(a \neq 0\) and \(b \neq 0\). A straightforward approach is to perform a QFT gate on the first \(N\) qubits and the last \(N\) qubits, leading to state

\[
|\psi_1\rangle = \left(\sum_{\ell=0}^{N-1} \hat{a}_\ell |\ell\rangle \right) \otimes \left(\sum_{\ell'=0}^{N-1} \hat{b}_{\ell'} |\ell'\rangle \right) = \sum_{\ell, \ell'=0}^{N-1} \hat{a}_\ell \hat{b}_{\ell'} |\ell\rangle |\ell'\rangle.
\]

We then permute the basis states to map \(|\ell\rangle |\ell\rangle\) to \(|\ell\rangle |0\rangle\) for each \(\ell\); call this state \(|\psi_2\rangle\). Now we measure the second register. If the outcome is not \(|0\rangle\), then the algorithm fails, otherwise the system is projected to

\[
|\psi_3\rangle = \sum_{\ell=0}^{N-1} \hat{a}_\ell \hat{b}_{\ell} |\ell\rangle |0\rangle = \frac{1}{N} \sum_{\ell=0}^{N-1} \left( \sum_{k,k'=0}^{N-1} a_k b_{k'} \omega^{(k+k')\ell} \right) |\ell\rangle |0\rangle
\]

and we apply the inverse QFT\(^{-1}\) on the first register. Hence, we obtain

\[
\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \left( \sum_{\ell=0}^{N-1} \hat{a}_\ell \hat{b}_{\ell} \omega^{-\ell j} \right) |j\rangle |0\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \sum_{(k,k') \in \Sigma(j)} a_k b_{k'} |j\rangle |0\rangle,
\]

which is the desired output state \(|\psi_{\text{output}}\rangle\).

**Amplification** Unfortunately, the success probability of this algorithm is not constant and, moreover, is dependent on the inputs \(a\) and \(b\). Therefore we resort to amplitude amplification. The price to pay will be the need to repeatedly execute the steps we outlined before and the input \(|\psi_{\text{input}}\rangle\) must be given by means of an operator \(V\) preparing \(|\psi_{\text{input}}\rangle\) from the initial state of amplitude amplification \(|0\rangle\), i.e., \(V |0\rangle = |\psi_{\text{input}}\rangle\).

To define the algorithm \(A\) formally, let \(R\) be the permutation that maps \(|\ell_0\ldots \ell_{n-1}\ell_0' \ldots \ell_{n-1}'\rangle\) to \(|\ell_0\ell_0' \ldots \ell_{n-1}\ell_{n-1}'\rangle\). Since \(R^{-1}\text{CNOT}^\otimes n R\) maps \(|\ell\rangle |\ell\rangle\) to \(|\ell\rangle |0\rangle\), we can express the operations up to the measurement by

\[
A := R^{-1} \text{CNOT}^\otimes n R (\text{QFT} \otimes \text{QFT}) V.
\]

Thus \(A |0\rangle = |\psi_2\rangle\). We would like to amplify the basis states \(F := \{|\ell\rangle |0\rangle : 0 \leq \ell < N\}\). Let \(a := \|\| |\psi_2\rangle\|/\|\| |\psi_2\rangle\||\|,\) i.e., \(a^2\) is the success probability when \(A\) is applied exactly once. This is the initial success probability that we boost by amplitude amplification using \(\Theta(1/a)\) applications of \(A\). We derive a lower bound on \(a^2\) under the additional assumption that all \(a_k\) and \(b_k\) are nonnegative:

\[
a^2 = \frac{1}{\|\| |\psi_2\rangle\|/\|\| |\psi_3\rangle\|} \frac{1}{\|\| |\psi_{\text{input}}\rangle\|/\|\| |\psi_3\rangle\|} = \frac{1}{\|a\|^2/\|b\|^2} \sum_{\ell=0}^{N-1} \|\hat{a}_\ell \hat{b}_{\ell}\|^2
\]
2.2. Convolution products

\[
\begin{align*}
&= \frac{1}{\|a\|^2\|b\|^2N^2} \sum_{\ell=0}^{N-1} \sum_{k,k'=0}^{N-1} a_k b_{k'} \omega^{(k+k')\ell} \\
&= \frac{1}{\|a\|^2\|b\|^2N^2} \sum_{\ell=0}^{N-1} \sum_{k,k',k'',k'''}=0}^{N-1} a_k b_{k'} \omega^{(k+k'-k''-k'''\ell)} \\
&= \frac{1}{\|a\|^2\|b\|^2N^2} \sum_{(k,k',N-k'',N-k''')\in\Sigma(0)} a_k b_{k'} \omega^{N} \\
&\geq \frac{1}{\|a\|^2\|b\|^2N} \sum_{k,k'=0}^{N-1} |a_k|^2 |b_{k'}|^2 = \frac{1}{N}
\end{align*}
\]

The inequality holds because we impose the restriction of summing only over those \((k, k', N-k'', N-k''') \in \Sigma(0)\) where \(k = k''\) and \(k' = k'''\). It follows that \(O(\sqrt{N})\) repetitions of the amplitude-amplification procedure are sufficient in all cases.

How expensive is one iteration? The iteration operator is

\[
Q = -AS_0A^{-1}S_F,
\]

where \(A\) is as defined above, \(S_0\) is the phase rotation by \(-1\) conditional on the input being \(|0\rangle\), i.e., \(S_0 = \mathbb{I} - 2|0\rangle\langle 0|\), and

\[
S_F = \mathbb{I} - 2 \sum_{\ell=0}^{N-1} |\ell\rangle\langle \ell| \otimes |0\rangle\langle 0|
\]

rotates the phase of basis vectors \(|\ell\rangle|0\rangle\) by \(-1\) and leaves all other basis vectors invariant. Preskill [99] shows that \(S_0\) can be implemented with \(O(\log N)\) gates; similarly, \(S_F\) can be realized using \(O(\log N)\) gates and three auxiliary qubits. QFT takes \(O(\log N \log \log N)\) operations [50] and \(R\) can be implemented by \(O(\log N)\) swaps of adjacent qubits, which in turn can be constructed from three CNOT gates. If \(v\) is the number of gates needed for implementing \(V\), we get a bound of \(O(v + (\log N)^2)\). Thus, if we measure the observable \(\sum_{\ell=0}^{N-1} |\ell\rangle\langle \ell| \otimes |0\rangle\langle 0|\) after

\[
O \left( \sqrt{N} \left( v + (\log N)^2 \right) \right)
\]

operations, we have constant success probability for projecting the system into state \(|\psi_3\rangle\). Since we only have a lower bound on the success probability, it will in general be necessary to apply the techniques of quantum search with unknown number of solutions. Finally, we can convert \(|\psi_3\rangle\) by an inverse QFT on the first register with \(O(\log N \log \log N)\) operations into \(|\psi_{\text{output}}\rangle\).
**An application** Suppose we want to implement the preparation $V$ using an oracle for the amplitudes $(a_0 \cdots a_{N-1})$ and $(b_0 \cdots b_{N-1})$ by using the technique from [72]. We assume that $N = 2^n$, that the components of $a$ and $b$ are nonnegative multiples of $2^{-m}$ for some $m \in \mathbb{N}$, and that $\sum_{0 \leq k < N} a_k^2 = \sum_{0 \leq k < N} b_k^2 = 1$. Using oracles for the $m$ bits of precision of the components, we can implement transformations for putting the components in the amplitudes,

$$U_a : |k\rangle|b\rangle \mapsto a_k |k\rangle|b\rangle + (-1)^b \sqrt{1 - |a_k|^2} |b\rangle \oplus 1 \rangle$$

$$U_b : |k\rangle|b\rangle \mapsto b_k |k\rangle|b\rangle + (-1)^b \sqrt{1 - |b_k|^2} |b\rangle \oplus 1 \rangle$$

and their inverses

$$U_a^{-1} : |k\rangle|b\rangle \mapsto a_k |k\rangle|b\rangle - (-1)^b \sqrt{1 - |a_k|^2} |b\rangle \oplus 1 \rangle$$

$$U_b^{-1} : |k\rangle|b\rangle \mapsto b_k |k\rangle|b\rangle - (-1)^b \sqrt{1 - |b_k|^2} |b\rangle \oplus 1 \rangle$$

where $0 \leq k < N$ and $b \in \{0,1\}$. These operators are weak in the sense that, e.g., for most $a$, the $a_k$ are going to be small and therefore the states $U_a |k\rangle|b\rangle$ close to $|k\rangle|b\rangle$; however, this construction has the advantage of uniformly operating on the table of amplitudes without preprocessing.

Amplitude amplification on $U_a H^\otimes n$ lets us map $|0^{n+1}\rangle$ exactly to

$$\sum_{0 \leq k < N} a_k |k\rangle|0\rangle$$

in $\Theta(\sqrt{N})$ iterations; from this we get the input preparation operator $V$. Applying the result of the previous paragraph we can thus produce

$$\sum_{j=0}^{N-1} \sum_{(k,k') \in \Sigma(j)} a_k b_{k'} |j\rangle$$

with high probability using $O(\sqrt{N} (m \sqrt{N} + (\log N)^2)) = O(mN)$ oracle queries and operations.

An efficient method to produce the state (2.10) may be of interest, e.g., for approximate pattern matching. However, our result is disappointing in this respect; the present algorithm requires reading a constant fraction of the input. Moreover, a very similar classical problem has an efficient solution: reading the entire input allows us to sample efficiently from the distribution $\Pr[j] = \sum_{(k,k') \in \Sigma(j)} a_k^2 b_{k'}^2$, simply by choosing $k$ with probability $a_k^2$ and $k'$ with probability $b_{k'}^2$, and outputting $k + k'$. One way to improve the quantum complexity would be to realize the reflection about the input state, $1 - 2 |\psi_{\text{input}}\rangle \langle \psi_{\text{input}}|$, directly using $U_a$ and $U_b$ instead of relying on
2.3. Search in the density-matrix formalism

1 - 2|ψ_{input}\rangle\langle ψ_{input}| = V(1 - 2|0\rangle\langle 0|)V^\dagger. This operation requires Θ(\sqrt{N}) invocations of U_a and U_b, since obtaining V from U_a and U_b is a generalization of quantum search, which has a lower bound of Ω(\sqrt{N}) queries [20, 71, 15]. Similarly, implementing V using the reflection operator 1 - 2|ψ_{input}\rangle\langle ψ_{input}| requires in general Ω(\sqrt{N}) iterations of amplitude amplification, hence, one might hope that implementing the “weak” reflection operator by means of the “weak” amplitude queries U_a and U_b should be efficiently feasible, but alas we did not find a way to achieve this.

2.3 Search in the Density-Matrix Formalism

In the real world, a quantum computer will be subject to noise and imperfections. For instance, it is hard to implement quantum gates exactly and the approximation error will accumulate over the course of a computation. An altogether different error source arises from the difficulty of isolating a quantum mechanical system from its environment; unintended interaction with the environment is called decoherence and manifests itself in uncontrolled measurements that “collapse” the current quantum state. These problems have attracted much attention and were in part solved by quantum error correction: by computing on encoded states, interleaving the computation with error-correction stages, and recursively applying these techniques, fault-tolerant quantum computing was shown to be possible whenever the errors are sufficiently local and uncorrelated, there is a supply of “fresh” qubits or sufficient parallelism, and the individual error probability is below a model-specific threshold [106, 112, 107, 2, 78].

However, the generic transformations for making a quantum circuit fault-tolerant are quite expensive and may be prohibitive for simple quantum computers. Therefore it is of interest to study the behavior of fundamental quantum algorithms when subjected to typical errors—with or without minimal fault detection and correction. In this section, we generalize the elegant analysis of Grover’s algorithm as a rotation in a two-dimensional vector space spanned by two pure quantum states: now the current state of the algorithm is a mixed state, and to accommodate the decoherence operator, we have to analyze the algorithm as a linear transformation in a four-dimensional space spanned by four density matrices.

Evolution in density matrices Consider Grover’s algorithm for database search [69] with one target state. Let N = 2^n be the size of the database, |t⟩ ∈ ℋ_N the target state, S_k = 1 - 2|k\rangle\langle k| the reflection conditional on k, and W the N-dimensional Hadamard transform. As before, one iteration WS_0WS_1 of the algorithm can be seen as a unitary mapping in the two-dimensional
subspace spanned by $|t\rangle$ and $|t^\perp\rangle := \sum_{k \neq t} |k\rangle = \sqrt{N}(1 - |t\rangle\langle t|)W|0\rangle$:

$$WS_0WS_t(\alpha|t\rangle + \beta|t^\perp\rangle) = (|t\rangle \langle t^\perp|) \frac{1}{N} \begin{pmatrix} N-2 & 2(N-1) \\ -2 & N-2 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

In order to investigate the effects of decoherence on the algorithm, we express this evolution in the language of density matrices. For $\alpha, \beta \in \mathbb{R}$, we write the undisturbed iteration

$$WS_0WS_t(\alpha|t\rangle + \beta|t^\perp\rangle) (\alpha\langle t| + \beta\langle t^\perp|) S_t^* W^* S_0^* W^*$$

$$= WS_0WS_t(\alpha^2|t\rangle\langle t| + \beta^2|t^\perp\rangle\langle t^\perp| + \alpha\beta \langle |t\rangle\langle t| + |t\rangle\langle t^\perp|) S_t W S_0 W$$

as a linear mapping in the subspace of matrices spanned by

$$\rho_t := |t\rangle\langle t| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \leftarrow t$$

$$\rho_{t^\perp} := |t^\perp\rangle\langle t^\perp| = \sum_{j, k \neq t} |j\rangle\langle k| = \begin{pmatrix} 1 \cdots 1 \\ \vdots \\ 1 \cdots 1 \\ 0 \cdots 0 \\ 0 \cdots 0 \\ 1 \cdots 1 \\ \vdots \\ 1 \cdots 1 \end{pmatrix} \leftarrow t$$, and

$$\rho_\times := |t^\perp\rangle\langle t| + |t\rangle\langle t^\perp| = \begin{pmatrix} 1 \cdots 1 \\ 0 \cdots 0 \\ 1 \cdots 1 \\ 0 \cdots 0 \end{pmatrix} \leftarrow t$$.
For $\rho_t$,

\[
WS_0WS_t\rho_tS_tWS_0W = (WS_0WS_t|t\rangle) (\langle t|WS_tWS_0W)
= (\frac{N-2}{N}|t\rangle - \frac{2}{N}|t^\perp\rangle) \left( \frac{N-2}{N} \langle t| - \frac{2}{N} \langle t^\perp| \right)
= \left( \frac{N-2}{N} \right)^2 \rho_t + \frac{4}{N^2} \rho_{t^\perp} - \frac{2(N-2)}{N^2} \rho_x .
\]

For $\rho_{t^\perp}$,

\[
WS_0WS_t\rho_{t^\perp}S_tWS_0W = (WS_0WS_t|t^\perp\rangle) (\langle t^\perp|WS_tWS_0W)
= \left( \frac{2(N-1)}{N}|t\rangle + \frac{N-2}{N}|t^\perp\rangle \right) \left( \frac{2(N-1)}{N} \langle t| + \frac{N-2}{N} \langle t^\perp| \right)
= 4 \left( \frac{N-1}{N} \right)^2 \rho_t + \left( \frac{N-2}{N} \right)^2 \rho_{t^\perp} + \frac{2(N-1)(N-2)}{N^2} \rho_x .
\]

For $\rho_x$,

\[
WS_0WS_t\rho_xS_tWS_0W = (WS_0WS_t|t^\perp\rangle) (\langle t|WS_tWS_0W) + (WS_0WS_t|t\rangle) (\langle t^\perp|WS_tWS_0W)
= \left( \frac{2(N-1)}{N}|t\rangle + \frac{N-2}{N}|t^\perp\rangle \right) \left( \frac{N-2}{N} \langle t| - \frac{2}{N} \langle t^\perp| \right) + \left( \frac{N-2}{N}|t\rangle - \frac{2}{N}|t^\perp\rangle \right) \left( \frac{2(N-1)}{N} \langle t| + \frac{N-2}{N} \langle t^\perp| \right)
= \frac{4(N-1)(N-2)}{N^2} \rho_t - \frac{4(N-2)}{N^2} \rho_{t^\perp} + \frac{N^2-8N+8}{N^2} \rho_x .
\]

Thus, one iteration of database search acts as

\[
a \rho_t + b \rho_{t^\perp} + c \rho_x \mapsto (\rho_t \quad \rho_{t^\perp} \quad \rho_x ) R \begin{pmatrix} a \\ b \\ c \end{pmatrix},
\]

where

\[
R = \frac{1}{N^2} \begin{pmatrix}
(N-2)^2 & 4(N-1)^2 & 4(N-1)(N-2) \\
4 & (N-2)^2 & -4(N-2) \\
-2(N-2) & 2(N-1)(N-2) & N^2-8N+8
\end{pmatrix} .
\]
Chapter 2. Quantum search

The initial state \( W|0\rangle \) has density matrix

\[ W|0\rangle\langle 0| W = \frac{1}{N} (\rho_t + \rho_{t\perp} + \rho_x) \]

and is represented by the 3-vector

\[ \frac{1}{N} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \]

Decoherence processes We considered two decoherence processes that are motivated by NMR [39]:

\[ D_1 : \rho \mapsto (1 - \lambda_1)\rho + \lambda_1 \sum_k |k\rangle\langle k| \rho |k\rangle\langle k| \]

corresponds to performing a measurement in the basis \( \{|k\rangle\} \) with probability \( \lambda_1 \). Note that \( D_1 \) pushes the system towards a "preferred" basis, which we assume to coincide with the computational basis. On the other hand, a usually weaker but more devastating decoherence effect is

\[ D_2 : \rho \mapsto (1 - \lambda_2)\rho + \lambda_2 \frac{1}{N} \mathbb{1}, \]

which models relaxation to the totally mixed state \( \mathbb{1}/N \) with probability \( \lambda_2 \). Since the action of \( D_2 \) commutes with every other linear transformation, we restrict our attention to \( D_1 \). We compute how \( D_1 \) acts on the four-dimensional subspace spanned by \( \rho_t, \rho_{t\perp}, \rho_x, \) and \( \mathbb{1} \):

\[ D_1 \rho_t = \rho_t \]
\[ D_1 \rho_{t\perp} = (1 - \lambda_1)\rho_{t\perp} + \lambda_1 \mathbb{1} - \lambda_1 \rho_t \]
\[ D_1 \rho_x = (1 - \lambda_1)\rho_x \]
\[ D_1 \mathbb{1} = \mathbb{1} . \]

Thus \( D_1 \) acts as

\[ a \rho_t + b \rho_{t\perp} + c \rho_x + d \mathbb{1} \mapsto (\rho_t \quad \rho_{t\perp} \quad \rho_x \quad \mathbb{1}) D_1 \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \]

with

\[ D_1 = \begin{pmatrix} 1 & -\lambda_1 & 0 & 0 \\ 0 & 1 - \lambda_1 & 0 & 0 \\ 0 & 0 & 1 - \lambda_1 & 0 \\ 0 & \lambda_1 & 0 & 1 \end{pmatrix} . \]
2.3. Search in the density-matrix formalism

We investigate the behavior of search when the state of the system is disturbed by $D_1$ before each rotation. One iteration then corresponds to the linear mapping

$$a \rho_t + b \rho_{t\perp} + c \rho_x + d \mathbb{1} \mapsto (\rho_t \quad \rho_{t\perp} \quad \rho_x \quad \mathbb{1}) R_1 D_1 \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$$

with

$$R_1 = \begin{pmatrix} R & 0 \\ 0 & 1 \end{pmatrix}.$$ 

The initial state is represented by the 4-vector

$$s = \frac{1}{N} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$ 

The probability of successfully measuring $|t\rangle$ after $\ell$ iterations is

$$p_{N,\lambda_1,\ell} = (t|(WS_0WS_tD_1)^\ell W|0\rangle\langle 0|W(D_1^\ast S_tDW)_\ell |t\rangle$$

$$= (1 \quad 0 \quad 0 \quad 1) (R_1 D_1)^\ell s.$$ 

**Numerical simulations** Figure 2.3 gives an example of the undisturbed evolution in the four-dimensional subspace; Figure 2.4 shows the same evolution when subjected to decoherence via $D_1$. Figure 2.5 indicates that for constant success probability, smaller and smaller $\lambda_1$ can be tolerated with growing $N$ and it suggests that constant success probability can be achieved with $\lambda_1 = \omega(1/\sqrt{N})$—this would mean that the decoherence process $D_1$ is somewhat less destructive to quantum search than $D_2$, which in each iteration replaces the state of the computation with the completely mixed state with probability $\lambda_2$ and which clearly can tolerate error probability $\lambda_2 = O(1/\sqrt{N})$ only. The susceptibility of quantum search to other kinds of errors has been studied before both numerically and analytically [85, 95, 105].
Chapter 2. Quantum search

Figure 2.3: Example of undisturbed database search ($N = 128$)

Figure 2.4: Example of database search disturbed by $D_1$ before each iteration ($N = 128$, $\lambda_1 = 0.1$)
2.3. Search in the density-matrix formalism

Figure 2.5: For the case of database search disturbed by $D_1$ before each iteration, plot of success probability after $(\pi/4)\sqrt{N}$ iterations against database size for several $\lambda_1$. 
2.4 Energy Levels of a Hamiltonian

In this section we study an application of quantum search to physics. Recall from Subsection 1.2.2 that a time-independent Hamiltonian is a self-adjoint operator $H$ that describes the evolution of a quantum system via $|\psi_t\rangle = e^{iHt}|\psi_0\rangle$. The eigenvalues of $H$ are real and describe the "energy levels" of the system; the energy is a preserved quantity for every state. If an eigenspace of $H$ has dimension greater than 1, we call it degenerate; the dimension of the eigenspace we call the degeneracy degree of the given energy level.

We study the following problem: suppose in an $N$-dimensional Hilbert space $\mathcal{H}$ we are given a Hamiltonian $H$ with three energy levels, 0, $E$, and $E + d$. By $k$ and $\ell$ we denote the degeneracy degree of $E$ and $E + d$, respectively; we assume that they are much less than $N$, i.e., $k + \ell = o(N)$. The goal is to sample states from level $E$ (or from level $E + d$) and to determine which degree is larger as efficiently as possible for large $N$, $E = \pi$ fixed, and $d$ fixed or a decreasing function of $N$. In unit time, an eigenstate of the Hamiltonian is unchanged at energy 0, acquires a phase of $-1$ at energy $E = \pi$, and a phase of $-e^{i\ell}$ at energy $E = \pi + d$. Taking this evolution as a query operator, sampling amounts to quantum search with a phase error. Thus we extend quantum search beyond perfect phase flips; our case study is of different scope to the robustness construction of Høyer, Mosca, and de Wolf [75] since here our goal is to distinguish between the different phases.

<table>
<thead>
<tr>
<th>Method 1</th>
<th>sampling</th>
<th>comparing</th>
</tr>
</thead>
<tbody>
<tr>
<td>$d = O\left(\sqrt{\frac{k}{N}}\right)$</td>
<td>$d = O\left(\frac{</td>
<td>k-\ell</td>
</tr>
<tr>
<td>time $O\left(\frac{N}{k}\right)$</td>
<td>time $O\left(\frac{N}{</td>
<td>k-\ell</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Method 2</th>
<th>sampling</th>
<th>comparing</th>
</tr>
</thead>
<tbody>
<tr>
<td>$d = \Omega\left(\sqrt{\frac{k+\ell}{N}}\right)$</td>
<td>$d = \Omega\left(\frac{k+\ell}{N}\right)$</td>
<td></td>
</tr>
<tr>
<td>time $O\left(\frac{N}{k}\right)$</td>
<td>time $\approx O\left(\frac{N}{\min(k,\ell)}\right)$</td>
<td></td>
</tr>
</tbody>
</table>

Table 2.2: Summary of results for Hamiltonian energy levels; the conditions on $d$ indicate in what regime the corresponding time bounds hold.

We derive quantum algorithms for this problem based on Grover's search technique. Our results are summarized in Table 2.2; we used different approaches depending on whether $d$ is small or large; for $\ell = o(k)$, the full range of possible $d$ is covered.
2.4. Energy levels of a Hamiltonian

We use the following notation. Let $U := e^{-iH}$ be the evolution operator of the system in unit time and let $U' := e^{-iH_\pi/(\pi+d)}$ be the evolution in time $\pi/(\pi+d)$. Let $\{|m\rangle: 0 \leq m < N\}$ be an orthonormal basis of the eigenstates of $H$, $U$, and $U'$. Let $M_\vartheta$ be the indices of the eigenstates with energy $\vartheta$. Thus $U$ multiplies $|m\rangle$ by $e^{i\pi} = -1$ if $m \in M_\pi$, by $e^{i(\pi+d)}$ if $m \in M_{\pi+d}$, and leaves it unchanged if $m \in M_0$. With $d' = -d + d^2/(\pi + d) = -d + O(d^2)$, $U'$ phase-shifts $|m\rangle$ by $e^{i(\pi+d')}$ if $m \in M_\pi$, by $-1$ if $m \in M_{\pi+d}$, and leaves it unchanged otherwise.

2.4.1 Sampling from the energy levels

Sampling using Grover’s search technique Building on Grover’s search technique, we discuss in this subsection how to approximately generate a uniform superposition of the states $|m\rangle$ with $m \in M_\pi$ if $k$ and $\ell$ are known. Uniformly sampling an $|m\rangle$ with $m \in M_\pi$ then amounts to measuring this superposition in the basis $\{|m\rangle: 0 \leq m < N\}$.

Grover’s search algorithm consists of a number of repeated applications of the operator $G = T_0 S_t$ to the start state $W|0\rangle$. Here $W := H_{\otimes n}$ denotes again the Hadamard transformation applied to all log $N$ qubits; $S_t$ denotes the conditional phase-shift operator that acts on the computational basis by multiplying the phase of certain “marked” basis states by $-1$ and leaving the remaining basis states unchanged; $T_0$ is again the reflection about the average in the computational basis. In Section 2.1 we saw that with $O(\sqrt{N})$ applications of $G$ to $W|0\rangle$ it is possible to approximate the uniform superposition of the marked basis states.

In our setting, we do not have an operator $S_t$; $U$ acts like $S_t$ on the $M_\pi$ and $M_0$ states but deviates on the $M_{\pi+d}$ states. We present ways to recover the properties of Grover’s search algorithm when $S_t$ is replaced by $U$. Note that using $U'$ in place of $U$ will yield essentially the same results with the role of $M_\pi$ and $M_{\pi+d}$ interchanged.

Small energy difference First, we quickly discuss the case

$$d \leq \frac{\pi}{40} \sqrt{\frac{k}{N}}.$$  

For $q \in \mathbb{N}$, the operator $U^{2q+1}$ phase-shifts the $M_\pi$-states by $-1$, the $M_{\pi+d}$ states by $e^{i(\pi+(2q+1)d)}$, and leaves the remaining states unchanged. So we can select a $q$ that minimizes the impact of the $M_{\pi+d}$ states: with $q$ the integer closest to $(\pi/d-1)/2$, the $M_{\pi+d}$ states get phase-shifted by $e^{i\delta_0}$ with $|\delta_0| \leq d$. Hence in the operator norm, $\|U^{2q+1} - S_t\| \leq d$. Applying Grover search for $(\pi/4)\sqrt{N/k}$ steps with $U^{2q+1}$ in place of $S_t$ thus causes a total deviation
from the ideal evolution of quantum search of $O(d\sqrt{N/k}) < 1/3$ with high probability.

We now turn our attention to the case $d = \Omega(\sqrt{(k+\ell)/N})$, for which a much more efficient algorithm can be derived by showing that the $M_{\pi+d}$-states do not cause any noticeable disturbance.

**Evolution in a three-dimensional subspace** In Section 2.1 we derived that the evolution of the system under subsequent applications of $G$ is confined to the two-dimensional subspace spanned by the uniform superposition of marked and unmarked states. In our setting, $G = T_0 U$; we derive the evolution of $W|0\rangle$ under repeated applications of $G$ as a transformation in a three-dimensional subspace. Let

$$|\bar{0}\rangle := \frac{1}{\sqrt{N-k-\ell}} \sum_{m \in M_0} |m\rangle$$

$$|\bar{k}\rangle := \frac{1}{\sqrt{k}} \sum_{m \in M_k} |m\rangle$$

and

$$|\bar{\ell}\rangle := \frac{1}{\sqrt{\ell}} \sum_{m \in M_{\pi+d}} |m\rangle.$$

For every $M \subseteq \{0, \ldots, N - 1\}$, the reflection about the average $T_0$ acts as

$$T_0 : \sum_{m \in M} |m\rangle \mapsto \left(\frac{2|M|}{N} - 1\right) \sum_{m \in M} |m\rangle + \frac{2|M|}{N} \sum_{m \notin M} |m\rangle,$$

hence,

$$G|\bar{\ell}\rangle = T_0 U|\bar{\ell}\rangle = -e^{i d T_0}|\bar{\ell}\rangle$$

$$= e^{i d} \left(\left(1 - \frac{2\ell}{N}\right)|\bar{\ell}\rangle - \frac{2\ell}{N} \left(\frac{\sqrt{N-k-\ell}}{\sqrt{\ell}}|\bar{0}\rangle + \frac{\sqrt{k}}{\sqrt{\ell}}|\bar{k}\rangle\right)\right)$$

$$= -2e^{i d} \frac{\ell(N-k-\ell)}{N} |\bar{0}\rangle - 2e^{i d} \frac{\sqrt{k\ell}}{N} |\bar{k}\rangle + e^{i d} \left(1 - \frac{2\ell}{N}\right)|\bar{\ell}\rangle.$$

Similar calculations give rise to a matrix

$$R = \begin{pmatrix}
1 - \frac{2(k+\ell)}{N} & -2\frac{\sqrt{k(N-k-\ell)}}{N} & -2e^{i d} \frac{\sqrt{k(N-k-\ell)}}{N} \\
2\frac{\sqrt{k(N-k-\ell)}}{N} & 1 - \frac{2k}{N} & -2e^{i d} \frac{\sqrt{k\ell}}{N} \\
2\frac{\sqrt{\ell(N-k-\ell)}}{N} & -2\frac{\sqrt{k\ell}}{N} & e^{i d} \left(1 - \frac{2\ell}{N}\right)
\end{pmatrix}.$$
so that the evolution of the system starting in state

\[ W|0\rangle = \sqrt{\frac{N-k-\ell}{N}}|\tilde{0}\rangle + \frac{k}{N}|\tilde{k}\rangle + \frac{\ell}{N}|\tilde{\ell}\rangle \]

to which \( G \) is applied repeatedly can be expressed as a transformation in the 3-dimensional subspace of \( \mathcal{H}_N \) spanned by \( |\tilde{0}\rangle, |\tilde{k}\rangle, \) and \( |\tilde{\ell}\rangle \):

\[ G(a|\tilde{0}\rangle + b|\tilde{k}\rangle + c|\tilde{\ell}\rangle) = (|\tilde{0}\rangle \ |\tilde{k}\rangle \ |\tilde{\ell}\rangle) R \begin{pmatrix} a \\ b \\ c \end{pmatrix} \]

Discarding in \( R \) terms that are \( O((k+\ell)/N) \) and substituting \( x := 2\sqrt{k/N} \), \( y := 2\sqrt{\ell/N} \), and \( v := e^{id} \), we get \( R = \tilde{R} + O((k+\ell)/N) \) with

\[ \tilde{R} = \begin{pmatrix} 1 & -x & -vy \\ x & 1 & 0 \\ y & 0 & v \end{pmatrix} . \]

Here \( R = \tilde{R} + O((k+\ell)/N) \) is shorthand for \( \| R - \tilde{R} \| = O((k+\ell)/N) \) in the operator norm.

**Finding the eigenvalues** To find the eigenvalues of \( \tilde{R} \) we consider its characteristic polynomial \( p(\lambda) = \det(\tilde{R} - \lambda I) \). It has the form

\[ p(\lambda) = (\lambda - 1 + ix)(\lambda - 1 - ix)(\lambda - v) + vy^2(\lambda - 1) . \]  

(2.11)

We show that \( \tilde{\lambda}_1 = 1 - ix, \tilde{\lambda}_2 = 1 + ix \) and \( \tilde{\lambda}_3 = v \) are the zeroes of \( p(\lambda) \) up to order \( 1/(dN) \), i.e., there exist roots \( \lambda_1, \lambda_2, \lambda_3 \) of \( p(\lambda) \) such that \( \lambda_k = \tilde{\lambda}_k + O(1/(dN)) \).

By the definition of the derivative and the inverse-function theorem from elementary calculus,

\[ p^{-1}(0) = p^{-1}(h) - (p^{-1})'(h) \cdot h + o(h) \]

\[ = p^{-1}(h) - \frac{h}{p'(p^{-1}(h))} + o(h) , \]

that is, for \( h = p(\tilde{\lambda}_k) \),

\[ \lambda_k = \tilde{\lambda}_k - \frac{p(\tilde{\lambda}_k)}{p'(\tilde{\lambda}_k)} + o(p(\tilde{\lambda}_k)) . \]
From Eq. (2.11) we have \( p(\tilde{\lambda}_k) = vy^2(\tilde{\lambda}_k - 1) \), thus \( p(\tilde{\lambda}_{1,2}) = O(1/N^{3/2}) \) and \( p(\tilde{\lambda}_3) = O(d/N) \). Moreover,

\[
p'(\tilde{\lambda}_{1,2}) = \pm 2i(v - 1)x - 2x^2 + vy^2 = \Omega \left( \frac{d}{\sqrt{N}} \right) \quad \text{and} \quad p'(\tilde{\lambda}_3) = 1 + v^2 + x^2 + v(y^2 - 2) = \Omega(1) .
\]

Altogether, \( \tilde{\lambda}_{1,2} = \tilde{\lambda}_{1,2} + O(1/(dN)) \) and \( \lambda_3 = \tilde{\lambda}_3 + O(d/N) = \tilde{\lambda}_3 + O(1/(dN)) \).

### Finding the eigenvectors

Let \( \gamma := (k + \ell)/N \) and denote eigenvectors of \( \tilde{R} \) by \( \tilde{a} = (a, b, w) \). We assume that they are of unit length: \( a^2 + b^2 + w^2 = 1 \). The system of linear equations \( \tilde{a}(\tilde{R} - \lambda I) = 0 \) for finding approximate eigenvectors up to \( O(\gamma) \) has for \( \tilde{\lambda}_1 \) the form

\[
\begin{bmatrix}
ixa & +xb & +yw \\
dxa & +ixb & = O(\gamma) \\
dvy & +w & = O(\gamma)
\end{bmatrix} = 0(\gamma)
\]

It has the solution \( a = -1 + o(1), b = i + o(1), w = o(1) \). For the second root, \( \tilde{\lambda}_2 \), the corresponding equations yield \( a = 1 + o(1), b = i + o(1), w = o(1) \). For the third root, \( \tilde{\lambda}_3 \), we obtain \( a = o(1), b = o(1), w = 1 + o(1) \).

Comparing this with the two-dimensional quantum-search iteration,

\[
G = \frac{1}{N} \begin{pmatrix}
N - 2M \\
-2\sqrt{M(N - M)} \\
N - 2M
\end{pmatrix} \begin{pmatrix}
2\sqrt{M(N - M)} \\
N - 2M \\
0
\end{pmatrix} = \begin{pmatrix}
i & -i & 1 \\
1 & 1 & 1
\end{pmatrix} \begin{pmatrix}
i & 1 \\
0 & 1
\end{pmatrix}
\]

we see that the eigenvalues are up to \( O(\gamma) \) the same and the eigenvectors coincide up to terms of \( o(1) \). This means that for up to \( o(1/\gamma) \) iterations, the behavior of our algorithm can be approximated by the behavior of Grover’s algorithm.

### 2.4.2 Comparing degeneracy degrees

In this subsection we apply the quantum approximate counting technique by Brassard, Høyer, and Tapp [28] to our setting:

**Lemma (Theorem 5 of [28]):** Let \( F : [N] \to \{0, 1\} \) be a Boolean function, \( t = |F^{-1}(1)| < N/2 \), and \( P \in \mathbb{N} \) with \( 0 < P \leq N \). There is a quantum algorithm \( \text{Count}(F, P) \) whose output \( \hat{t} \) satisfies

\[
|t - \hat{t}| \leq \frac{2\pi}{P} \sqrt{tN} + \frac{\pi^2}{P^2} N .
\]
2.4. Energy levels of a Hamiltonian

Furthermore, Count\((F,P)\) makes \(P\) quantum queries to \(F\).

As before, we study two cases, namely that \(d\) is small enough to construct a good approximation of \(S_t\) for the \(M_\pi\) states and that \(d\) is so large that it does not influence

**Small energy difference** The same construction as for sampling gives us an approximation \(U^{2q+1}\) of \(S_t\) with \(\| U^{2q+1} - S_t \| \leq d\). Hence, with \(P = O(1/d)\) the algorithm Count\((F,P)\) with \(U^{2q+1}\) in place of \(S_t\) will still work with constant probability. To compare the degeneracy degrees \(\ell = |M_\pi|\) and \(\ell = |M_\pi + d|\), we obtain an approximate count \(\ell\) and, with \(U'\) in place of \(U\), an approximation \(k\). Sufficient conditions for the comparison to succeed with constant probability are

\[
|\ell - \ell| < \frac{1}{2} |k - \ell| \quad \text{and} \quad |k - \ell| < \frac{1}{2} |k - \ell| .
\]

These are satisfied if we choose \(P\) so that

\[
\frac{2\pi}{P} \sqrt{(k + \ell)N} + \frac{\pi^2}{P^2} N < \frac{1}{2} |k - \ell| ,
\]

or

\[
P = \Theta \left( \frac{\sqrt{(k + \ell)N}}{|k - \ell|} \right) .
\]

**Large energy difference** If \(d\) is large enough to allow \(P\) iterations of search with only constant total deviation, then we can just use \(U\) and \(U'\) in place of \(S_t\). In the previous subsection we showed that for \(d = \Omega(\sqrt{(k + \ell)N})\) we can execute as many as \(o(N/(k + \ell))\) iterations of search with \(U\) and \(U'\). With \(P_k = \omega(\sqrt{N/k})\) and \(P_\ell = \omega(\sqrt{N/\ell})\), respectively, we obtain approximations \(\hat{k}\) and \(\hat{\ell}\) with

\[
|k - \hat{k}| + |\ell - \hat{\ell}| = o(1)
\]

so that asymptotically we can detect any difference between \(k\) and \(\ell\). This takes time \(O(\sqrt{N/\min(k, \ell)} r(N))\) where \(r(N) = \omega(1)\) is an unbounded and arbitrarily slow growing function.

### 2.4.3 Numerical simulations

To complement our theoretical results, we simulated the sampling algorithms from Subsection 2.4.1 with one state that is rotated by \(e^{i\pi}\) and one state that
is rotated by $e^{i(\pi+d)}$. Figures 2.6 and 2.7 show the probability of finding the state rotated by $e^{i\pi}$ as a function of the dimension of the state space. In Figure 2.6, $d$ is chosen independently of $N$. Observe that for small $d$ and small $N$, the success probability is about 1/2. This is because in this regime, the system evolves as search with two target states that are rotated by $e^{i\pi}$: the probability that we hit the desired of the two target states is 1/2. With growing $N$, the success probability converges to 1, as theoretically predicted—the state rotated by $e^{i(\pi+d)}$ causes negligible distortion. The graph suggests that the “speed” of convergence depends linearly on $d$: given $\varepsilon > 0$, the smallest $N$ for which the success probability is greater than $1 - \varepsilon$ appears to be a linear function of $d$. Figure 2.7 illustrates the case that $d$ is a function of $N$. Our analysis that for $d = \omega(1/\sqrt{N})$ the success probability will converge to 1, is mirrored by the curves for $a < 1/2$ appearing to converge to 1. We do not have an analytical result for $d = \Theta(1/\sqrt{N})$ or $a = 1/2$, but the graph suggests that the success probability does not rise above 1/2.
2.4. Energy levels of a Hamiltonian

Figure 2.6: Success probability for finding one of the $|k\rangle$ states for $d$ constant: Plot of success probability against dimension $N = 2^n$ for $n = 2, \ldots, 40$ and $d = 2^{-2}, 2^{-6}, 2^{-10}, 2^{-14}$.

Figure 2.7: Success probability for finding one of the $|k\rangle$ states for $d$ a function of $N$: Plot of success probability against dimension $N = 2^n$ for $n = 2, \ldots, 40$ and $d = 2^{-2-an}$ where $a = 0, 1/6, 1/3, \text{ and } 1/2$. 