Grover Algorithm

Ivan Murashko

Contents

Introduction

Let us consider the following problem. Suppose that we have a large set of data consisting of N elements, and we have to find an element that satisfies some condition. Schematically this problem is shown in Figure 1.

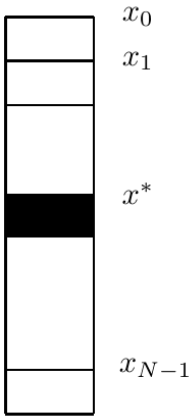

Figure 1: Search in an unstructured data set.

If the data are sorted, then algorithms of the "divide and conquer" type can find the required element in time of order $O(\log N)$. In many cases the initial data set cannot be prepared for such a fast search. In this case the classical search is performed in time of order $O(N)$.

One example is a symmetric encryption algorithm where the task is to determine the key from a known ciphertext and the corresponding plaintext. In this case preliminary preparation of the data is not available, and the direct solution of the problem is a simple search over all possible values.

Grover's algorithm [2] solves the problem of unstructured search in time of order $O(\sqrt{N})$.

1 The Oracle

Suppose that we have a quantum circuit which computes the value of a function $f(x)$. This function can take only two values, 0 and 1. The value 1 corresponds only to the element that we are looking for:

$$\begin{aligned} f(x)|_{x=x^*} &= 1, \\ f(x)|_{x\neq x^*} &= 0. \end{aligned} \tag{1}$$

Here and below we assume that there is one marked element x^*.

Figure 2 shows a circuit that computes this function. At the output we have a state of the form

$$|out\rangle = \frac{1}{\sqrt{N}} \left(\sum_{x\neq x^*} |x\rangle \otimes |0\rangle + |x^*\rangle \otimes |1\rangle \right), \tag{2}$$

where N is the total number of elements in the sequence where the search is performed.

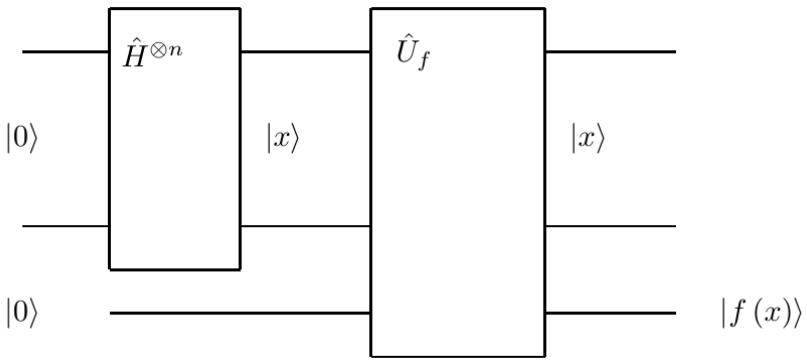

Figure 2: Computing the function $f(x)$.

If we look at (2), we can see that this scheme computes the function at the required point, but it still does not allow us to choose the required element. All elements in the resulting sequence are equally probable. In other words, each element can be selected by measurement with probability $1/N$.

Grover proposed an algorithm which increases the probability of detecting the required element in the resulting superposition.

2 Grover Iteration

The circuit that implements Grover's algorithm consists of a block described by an operator $\hat{U}_G$. This block is repeated a certain number of times, as shown in Figure 3. At each iteration the probability of detecting the required element increases.

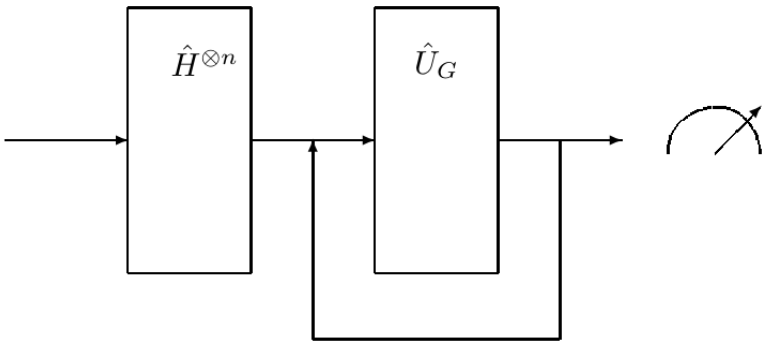

Figure 3: Grover's algorithm.

The basic element $\hat{U}_G$ is the sequential action of two operators, as shown in Figure 4:

$$\hat{U}_G = \hat{U}_s \hat{U}_{x^*}, \tag{3}$$

where $\hat{U}_{x^*}$ is the phase inversion operator, and $\hat{U}_s$ is the operator of inversion about the mean.

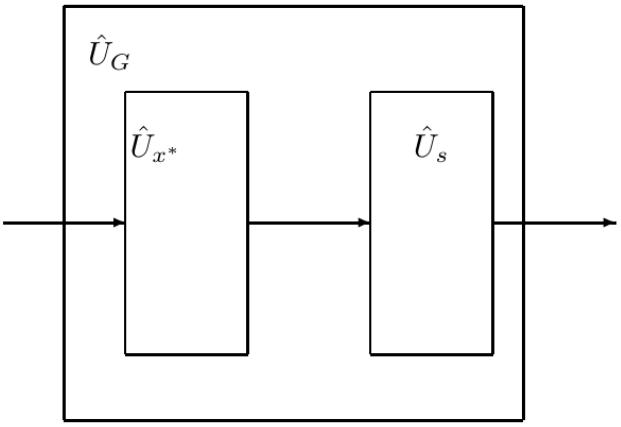

Figure 4: Grover's algorithm. The basic element.

The most important point is that the two operators in (3) do not directly reveal x^*. Instead, they change the amplitudes so that the amplitude of $|x^*\rangle$ becomes larger than the amplitudes of the other basis states.

3 Phase Inversion

The action of the operator $\hat{U}_{x^*}$ is described by the following relation:

$$\hat{U}_{x^*}\left(\sum_x \alpha_x |x\rangle\right) = \sum_x \alpha_x (-1)^{f(x)} |x\rangle . \tag{4}$$

Thus the marked state changes its sign, while all other basis states remain unchanged. Figure 5 shows this operation schematically.

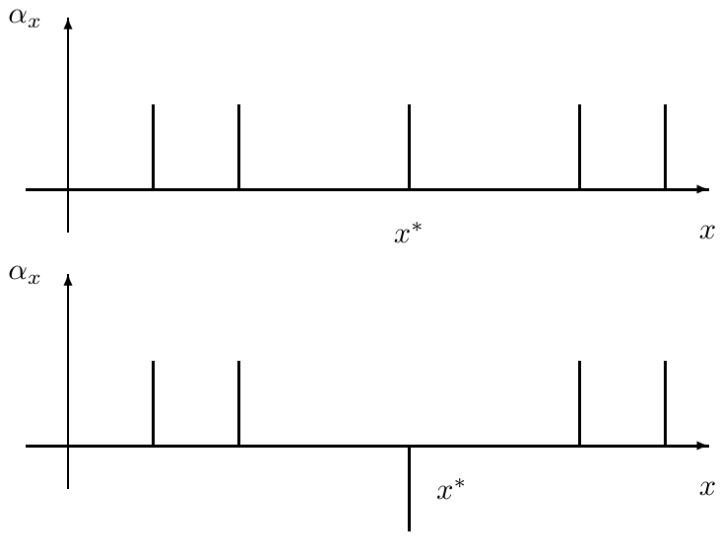

Figure 5: Grover's algorithm. Phase inversion.

The operator $\hat{U}_{x^*}$ can be rewritten as follows:

$$\hat{U}_{x^*} = \hat{I} - 2 |x^*\rangle \langle x^*| . \tag{5}$$

Indeed, we have

$$\begin{aligned}
&\left(\hat{I} - 2 |x^*\rangle \langle x^*|\right)\left(\sum_x \alpha_x |x\rangle\right) \\
&= \sum_x \alpha_x |x\rangle - 2\alpha_{x^*} |x^*\rangle \\
&= \sum_{x \neq x^*} \alpha_x |x\rangle - \alpha_{x^*} |x^*\rangle \\
&= \sum_x \alpha_x (-1)^{f(x)} |x\rangle ,
\end{aligned} \tag{6}$$

which coincides with (4).

Now let us discuss how this phase inversion can be implemented. In other words, we have to understand how the value $f(x)$ can be sent into the phase.

Consider the circuit shown in Figure 6. It performs the transformation

$$|x\rangle \otimes |b\rangle \longrightarrow |x\rangle \otimes |b \oplus f(x)\rangle\,, \tag{7}$$

where

$$a \oplus b = a + b \mod 2.$$

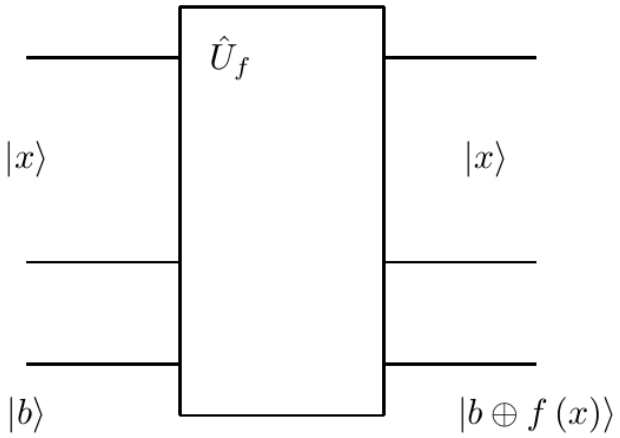

Figure 6: Implementation of phase inversion by the oracle $\hat{U}_f$.

For the case

$$|b\rangle = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

we obtain two cases. If $x \neq x^*$, then $f(x) = 0$, and

$$\begin{aligned} |x\rangle \otimes |-\rangle &\longrightarrow |x\rangle \otimes \left(\frac{|0 \oplus 0\rangle - |1 \oplus 0\rangle}{\sqrt{2}}\right) \\ &= |x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ &= |x\rangle \otimes |-\rangle\,. \end{aligned} \tag{8}$$

If $x = x^*$, then $f(x) = 1$, and

$$\begin{aligned} |x\rangle \otimes |-\rangle &\longrightarrow |x\rangle \otimes \left(\frac{|0 \oplus 1\rangle - |1 \oplus 1\rangle}{\sqrt{2}} \right) \\ &= |x\rangle \otimes \left(\frac{|1\rangle - |0\rangle}{\sqrt{2}} \right) \\ &= - |x\rangle \otimes |-\rangle . \end{aligned} \tag{9}$$

Therefore we have the transformation

$$|x\rangle \otimes |-\rangle \longrightarrow (-1)^{f(x)} |x\rangle \otimes |-\rangle . \tag{10}$$

This is exactly the phase inversion from (4); the auxiliary qubit remains in the state $|-\rangle$.

4 Inversion About the Mean

The action of the operator $\hat{U}_s$ is described by the following relation:

$$\hat{U}_s \left(\sum_x \alpha_x |x\rangle \right) = \sum_x (2\mathcal{M} - \alpha_x) |x\rangle , \tag{11}$$

where

$$\mathcal{M} = \frac{1}{N} \sum_x \alpha_x .$$

This operation is shown schematically in Figure 7.

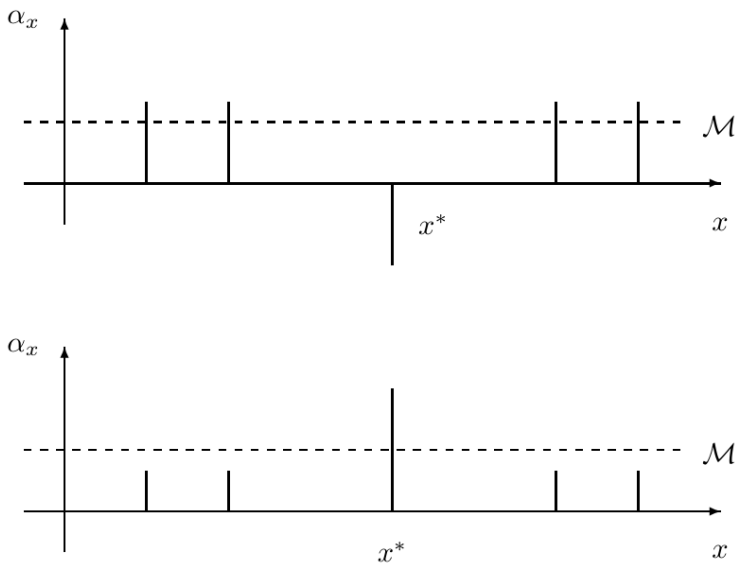

Figure 7: Grover's algorithm. Inversion about the mean.

The operator $\hat{U}_s$ can be rewritten in the following form:

$$\hat{U}_s = 2\,|s\rangle\,\langle s| - \hat{I}, \tag{12}$$

where

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$$

is the initial state in Grover's algorithm. Indeed,

$$\begin{aligned}
&\left(2\,|s\rangle\,\langle s| - \hat{I}\right)\left(\sum_x \alpha_x\,|x\rangle\right) \\
&\quad = 2\sum_x \alpha_x\,\langle s|x\rangle\,|s\rangle - \sum_x \alpha_x\,|x\rangle \\
&\quad = \frac{2}{N}\sum_x \alpha_x \sum_x |x\rangle - \sum_x \alpha_x\,|x\rangle \\
&\quad = \sum_x (2\mathcal{M} - \alpha_x)\,|x\rangle\,,
\end{aligned} \tag{13}$$

which coincides with (11).

It remains to show how this operator can be realized. Consider the circuit shown in Figure 8. The element $\hat{U}_{x\neq 0}$ performs a transformation analogous

to (10), but now the function is defined by

$$f(x=0)=0, \qquad f(x\neq 0)=1.$$

Thus

$$\begin{aligned} \hat{U}_{x\neq 0}\left|x\right\rangle \otimes \left|-\right\rangle &= \left|x\right\rangle \otimes \left|-\right\rangle, && x=0, \\ \hat{U}_{x\neq 0}\left|x\right\rangle \otimes \left|-\right\rangle &= -\left|x\right\rangle \otimes \left|-\right\rangle, && x\neq 0. \end{aligned} \tag{14}$$

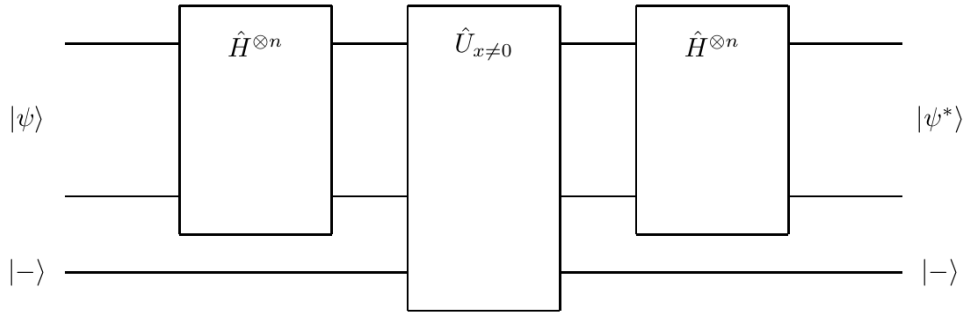

Figure 8: Implementation of inversion about the mean.

If we omit the unchanged auxiliary state $|-\rangle$, the matrix of this transformation on the search register has the form

$$\begin{aligned} \hat{U}_{x\neq 0} &= \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}. \end{aligned} \tag{15}$$

Combining this result with two Hadamard transformations, and using

$$\hat{H}^{\otimes n}\left|0\right\rangle = \frac{1}{\sqrt{N}}\sum_x \left|x\right\rangle = \left|s\right\rangle, \qquad N=2^n,$$

we obtain

$$\begin{aligned}
&\hat{H}^{\otimes n}\left\{\begin{pmatrix} 2 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} - \hat{I}\right\}\hat{H}^{\otimes n} \\
&= \left\{\begin{pmatrix} \frac{2}{N} & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \end{pmatrix} - \hat{I}\right\} \\
&= \begin{pmatrix} \frac{2}{N}-1 & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N}-1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N}-1 & \cdots & \frac{2}{N} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N}-1 \end{pmatrix}. \qquad (16)
\end{aligned}$$

If we act by the operator $\hat{H}^{\otimes n}\hat{U}_{x\neq 0}\hat{H}^{\otimes n}$, then from (16) we obtain

$$\begin{aligned}
&\hat{H}^{\otimes n}\hat{U}_{x\neq 0}\hat{H}^{\otimes n}\sum_x \alpha_x |x\rangle \\
&= \begin{pmatrix} \frac{2}{N}-1 & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N}-1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N}-1 & \cdots & \frac{2}{N} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N}-1 \end{pmatrix}\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} \\
&= \begin{pmatrix} \frac{2}{N}\sum_x \alpha_x - \alpha_0 \\ \frac{2}{N}\sum_x \alpha_x - \alpha_1 \\ \frac{2}{N}\sum_x \alpha_x - \alpha_2 \\ \vdots \\ \frac{2}{N}\sum_x \alpha_x - \alpha_{N-1} \end{pmatrix} \\
&= \sum_x (2\mathcal{M} - \alpha_x)|x\rangle\,. \qquad (17)
\end{aligned}$$

Therefore the circuit from Figure 8 does implement inversion about the mean.

5 Number of Iterations

The schematic form of Grover's algorithm can be written as follows.

1. Prepare the initial state
$$|\psi\rangle_0 \Leftarrow \frac{1}{\sqrt{N}} \sum_x |x\rangle .$$
2. Repeat
$$|\psi\rangle_t \Leftarrow \hat{U}_s \hat{U}_{x^*} |\psi\rangle_{t-1}$$
until t reaches approximately
$$\frac{\pi}{4}\sqrt{N}.$$
3. Measure the state $|\psi\rangle_t$.

We are interested in two questions. What is the algorithmic complexity of Grover's algorithm? And do there exist algorithms that can perform the search in an unstructured volume of data more efficiently than Grover's algorithm?

The criterion of efficiency is the following fact: a good algorithm has to find the required value with the minimal number of calls to the function (1).

Let us consider the first iteration. The initial state $|\psi\rangle_0$ has the following form:

$$|\psi\rangle_0 = \sum_x \alpha_x |x\rangle = |s\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle = \frac{1}{\sqrt{N}} \sum_{x \neq x^*} |x\rangle + \frac{1}{\sqrt{N}} |x^*\rangle . \qquad (18)$$

Thus the coefficient before the required element is

$$\alpha_{x^*} = \frac{1}{\sqrt{N}}.$$

After applying the phase inversion operator $\hat{U}_{x^*}$ from (4), we obtain

$$\hat{U}_{x^*} |\psi\rangle_0 = \frac{1}{\sqrt{N}} \sum_{x \neq x^*} |x\rangle - \frac{1}{\sqrt{N}} |x^*\rangle = \sum_x \beta_x |x\rangle , \qquad (19)$$

where

$$\beta_{x^*} = -\frac{1}{\sqrt{N}}, \qquad \beta_{x \neq x^*} = \frac{1}{\sqrt{N}}.$$

After applying the inversion-about-the-mean operator $\hat{U}_s$ from (11), we obtain

$$\begin{aligned}\hat{U}_G |\psi\rangle_0 &= \hat{U}_s \hat{U}_{x^*} |\psi\rangle_0 = \hat{U}_s \sum_x \beta_x |x\rangle \\ &= \sum_x (2\mathcal{M} - \beta_x) |x\rangle \\ &\approx \sum_{x \neq x^*} \left(2\frac{1}{\sqrt{N}} - \frac{1}{\sqrt{N}}\right) |x\rangle + \left(2\frac{1}{\sqrt{N}} + \frac{1}{\sqrt{N}}\right) |x^*\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{x \neq x^*} |x\rangle + \frac{3}{\sqrt{N}} |x^*\rangle . \end{aligned} \tag{20}$$

In the derivation of (20) we used the approximation

$$\mathcal{M} = \frac{1}{N} \sum_x \beta_x = \frac{N-2}{N\sqrt{N}} \approx \frac{1}{\sqrt{N}}.$$

Therefore, after the first iteration of Grover's algorithm, the amplitude α_{x^*} has increased by approximately $2/\sqrt{N}$. If we extrapolate this result to an arbitrary iteration, then we obtain that 50% probability of detecting $|x^*\rangle$ is reached after the following number of iterations:

$$\frac{1}{\sqrt{2}} \Big/ \frac{2}{\sqrt{N}} = \frac{\sqrt{N}}{2\sqrt{2}} = O(\sqrt{N}).$$

More accurate calculations [3] give

$$\frac{\pi}{4}\sqrt{N}$$

iterations.

One can ask about the optimality of Grover's algorithm: does there exist a quantum algorithm that searches an unstructured volume of data faster than $O(\sqrt{N})$ calls to the function (1)? In the oracle model, this square-root order cannot be improved in general [1].

References

[1] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997.

[2] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 212–219. Association for Computing Machinery, 1996.

[3] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.