Introduction to quantum information and quantum cryptography: Lecture 6

WANTED

DEAD **&** ALIVE

Schrödinger's cat

$$\frac{1}{\sqrt{2}}(|\mathrm{DEAD}\rangle + |\mathrm{ALIVE}\rangle)$$

Quantum search: the Grover algorithm

Quantum search: the Grover algorithm

The Grover algorithm answers the question how to find a needle in a haystack in a way which is more effective than any of the known classical methods.

What is it all about? Let us supppose we have a list of phone numbers sorted by names and we would like to know whose phone number has been given to us.

Quantum search: the Grover algorithm

In the reverse case when we have to find a phone number for a given name, we can use the following *efficient* (classical) algorithm:

We look at the middle of the list of N names and find out if the sought name is before or after the middle of the list.

Quantum search: the Grover algorithm

In case it can be found before the middle point, we will look at the middle of the first halfe of the list (at the end point of the quarter of the whole list).

Comparing the name found here with the name we seek, we can split the list again to get a new (and smaller) part list to be looked through.

Quantum search: the Grover algorithm

In this way, at the nth step, the length of the part list we have to look through yet is $\frac{N}{2^n}$.

That is after approximately $\log_2 N$ steps we find the sought name and the phone number belonging to it. This is an algorithm with a $Poly(\log N)$ complexity which is said to be easy.

Quantum search: the Grover algorithm

However, in the reverse case, it is hard to handle the problem, because the phone numbers are not ordered.

If we want to find the name which belongs to the known phone number with a probability of $1/2$, we have to look through $N/2$ names (with their phone numbers), that is we have to take $2^{\log_2(N/2)}$ steps. In other words, in this case, the task is exponential in $\log N$.

Quantum search: the Grover algorithm

Using the Grover algorithm, the number of steps will be proportional to $\sqrt{N}$ instead of $N/2$. (Though, this effect is not as significant as the accelerator effect of Shor algorithm in the case of prime factorization, but this is an interesting result.)

It is natural to ask how this algorithm works. The mathematical task is the following:

Quantum search: the Grover algorithm

Let the list of the names be considered as a set of $Z_N^0 = \{0, 1, \ldots N-1\}$ and - on this set - let us have the following function $x \in Z_N^0$, $x \to g(x)$, which gives the related phone number $g(x)$.

Let us suppose we have been given a phone number $g(\omega)$ and we want to find $\omega \in Z_N^0$, whose image is $g(\omega)$. We define another function $f(x)$ with the following properties:

$$f_\omega(x) = 1, \quad \text{if} \quad x = \omega$$

$$f_\omega(x) = 0, \quad \text{if} \quad x \neq \omega \tag{1}$$

Quantum search: the Grover algorithm

This is the so called oracle, where x is the input and $f(x)$ is the output. Physically, this can be the phone book itself.

The essence is the following: for a given x, f can be calculated rapidly, but in the reverse case (where we want to find $x = \omega$ for which $f_\omega(x) = 1$) we face a hard solvable problem.

Quantum search: the Grover algorithm

The real question is that how many times do we need to ask the oracle until we find ω? Let us define the following two-register operation (or "quantum machine"):

$$U_\omega \; : \; |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f_\omega(x)\rangle, \tag{2}$$

where, on the first register N different numbers can be imaged, that is the first register is an L-qubit register, where L is the smallest number for which $N < 2^L$ and $|x\rangle$ is imaged as the binary form of number x.

Quantum search: the Grover algorithm

The second register is a two-qubit register. Learning of Deutsch algorithm, we saw that if the initial state of the second qubit is $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, then

$$U_\omega \; : \; |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow \frac{1}{\sqrt{2}}|x\rangle(|0 \oplus f_\omega(x)\rangle - |1 \oplus f_\omega(x)\rangle) =$$

$$= \begin{cases} \frac{1}{\sqrt{2}}|x\rangle(|0\rangle - |1\rangle) & \text{if} \quad f_\omega(x) = 0 \\ \frac{1}{\sqrt{2}}|x\rangle(|1\rangle - |0\rangle) & \text{if} \quad f_\omega(x) = 1. \end{cases} \tag{3}$$

Quantum search: the Grover algorithm

This means that

$$U_\omega \; : \; |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow (-1)^{f_\omega(x)}|x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \qquad (4)$$

Quantum search: the Grover algorithm

Now the second register (whose state remains the same) can be omitted and we examine the first one only.

Being one of the elements of the special computational base, the sought $|\omega\rangle$ is orthogonal to all the other elements of the base. Thus in case the state of the second register is held unchanged, the effect of operator U_ω can be expressed by the following formula:

Quantum search: the Grover algorithm

$$U_\omega|x\rangle \to (-1)^{f_\omega(x)}|x\rangle = (1 - 2|\omega\rangle\langle\omega|)|x\rangle, \tag{5}$$

because $\langle\omega|x\rangle = 0$, if $\omega \neq x$.

Quantum search: the Grover algorithm

Being true for the base vectors, due to the linearity, it has to hold true for the cases of any other vectors.

That is operator U_ω has the following shape:

$$U_\omega = 1 - 2|\omega\rangle\langle\omega|$$

$$U_\omega|\psi\rangle = |\psi\rangle - 2|\omega\rangle\langle\omega|\psi\rangle. \tag{6}$$

Quantum search: the Grover algorithm

Now we show how the effect of the unitary operator U_ω can be imagined geometrically.

In this (geometrical) picture this effect is actually a mirroring to a hyperplane which is perpendicular to $|\omega\rangle$. What does it mean exactly?

Quantum search: the Grover algorithm

Let us have the two component vectors of an arbitrary state $|\psi\rangle$. One of them lies in the direction of $|\omega\rangle$ and the other one is perpendicular to this direction.

In this case, due to the effect of U_ω the sign of the vector which is parallel with $|\omega\rangle$ will be changed while the other component vector (which is othogonal to $|\omega\rangle$) will be untouched.

Quantum search: the Grover algorithm

In case of an arbitrary vector $|\psi\rangle$, a decomposition like this can be seen below:

$$|\psi\rangle = |\omega\rangle\langle\omega|\psi\rangle + (|\psi\rangle - |\omega\rangle\langle\omega|\psi\rangle), \tag{7}$$

where the first member is the component which is parallel with $|\omega\rangle$ and the second one is the orthogonal component.

Quantum search: the Grover algorithm

Indeed, if the sign of the first member is changed to its reverse (in other words it is mirrored to the plane which is perpendicular to $|\omega\rangle$), the resulted state is

$$|\varphi\rangle = |\psi\rangle - 2|\omega\rangle\langle\omega|\psi\rangle = U_\omega|\psi\rangle, \tag{8}$$

which is exactly $U_\omega|\psi\rangle$ (as it can be seen above).

Quantum search: the Grover algorithm

Now let us introduce a state which is the symmetric linear combination of all computational base state:

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle. \tag{9}$$

Quantum search: the Grover algorithm

We know also $|\omega\rangle$ is one of the elements of the computational base, but we do not know which element is it. Hence, in case of making a measurement in the computational base, the measurement will result $|\omega\rangle$ with a probability of $|\langle\omega|s\rangle|^2 = 1/N$.

This probability value is equal to the one which can be obtained in case of seeking $|\omega\rangle$ in a classical random way.

Quantum search: the Grover algorithm

However, Grover algorithm is an iteration, which increases the probability of finding ω step by step.

Let us consider the following unitary operator

$$U_s = 2|s\rangle\langle s| - 1. \tag{10}$$

Quantum search: the Grover algorithm

Using this operator, its operation preserves the component which lies in the direction of the symmetric average of all base states, that is the component along the direction of $|s\rangle$ will be untuched, while the other component which is orthogonal to $|s\rangle$ will be mirrored.

Quantum search: the Grover algorithm

Now let us consider the Grover operator $G = U_s U_\omega$. Applying it on $|s\rangle$ and again on the resulted state, and so on, after enough number of iterations, we get the proper ω. Indeed, let us consider

$$\langle \omega | s \rangle = \frac{1}{\sqrt{N}} = \sin\theta, \tag{11}$$

where the equation defines θ, which is the angle between the symmetric vector and the plane which is orthogonal to the sought $|\omega\rangle$.

Quantum search: the Grover algorithm

Let us have two orthogonal components of $|s\rangle$, where one of them is in the direction of $|\omega\rangle$ (and naturally the other one is orthogonal to it). In this way we get the following expression:

$$|s\rangle = |\omega\rangle \sin\theta + |\omega_\perp\rangle \cos\theta, \tag{12}$$

where $|\omega_\perp\rangle$ is a unit vector which lies in the direction of $|s_\perp\rangle = |s\rangle - |\omega\rangle\langle\omega|s\rangle$, that is $|\omega_\perp\rangle = |s_\perp\rangle/|s_\perp|$.

Quantum search: the Grover algorithm

Applying U_ω on $|s_\perp\rangle$, we get the following result: $|s'\rangle = -|\omega\rangle \sin\theta + |\omega_\perp\rangle \cos\theta$. If we apply U_s on the previous result, overall we achieve the following operation: $G|s\rangle$, or

$$G|s\rangle = |s_1\rangle = |\omega\rangle \sin 3\theta + |\omega_\perp\rangle \cos 3\theta. \tag{13}$$

(This result can be seen geometrically, but also can be deducted from the formulae above.) From this, it directly follows that vector $|s\rangle$ turns towards $|\omega\rangle$ from $|\omega_\perp\rangle$.

Quantum search: the Grover algorithm

It can be seen easily that if we apply G again, the resulted state will be

$$G^2|s\rangle = G|s_1\rangle = |s_2\rangle = |\omega\rangle \sin 5\theta + |\omega_\perp\rangle \cos 5\theta \qquad (14)$$

and in general

$$G^n|s\rangle = |s_n\rangle = |\omega\rangle \sin(2n+1)\theta + |\omega_\perp\rangle \cos(2n+1)\theta. \qquad (15)$$

Quantum search: the Grover algorithm

If we stop iterating in the proper moment, then $|s_n\rangle$ will be close to $|\omega\rangle$, that is $\langle s_n|\omega\rangle \approx 1$.

This means if we make a measurement in the computational base we will get $|\omega\rangle$ with a big probability. This can happen, if the angle of the turning is about $\pi/2$.

Quantum search: the Grover algorithm

If N is big, then $\sin\theta = 1/\sqrt{N} \ll 1$ so $\theta \approx \sin\theta = 1/\sqrt{N}$.

Thus at the Tth step the angle is $(2T+1)\,\theta \approx (2T+1)/\sqrt{N}$ and this value is close to $\pi/2$, that is $(2T+1)/\sqrt{N} \approx \pi/2$.

Quantum search: the Grover algorithm

From this it follows that the number of the steps we need to take is about the following value:

$$T = \frac{\pi}{4}\sqrt{N} - \frac{1}{2}, \tag{16}$$

which is proportional to $\sqrt{N}$.

Quantum search: the Grover algorithm

However, T has to be an integer number so the following formula is righter: $T = \frac{\pi}{4}\sqrt{N}(1 - O(1/\sqrt{N}))$. After taking these steps the probability of finding ω is

$$P(\omega) = |\langle s_n|\omega\rangle|^2 = \sin^2(2T + 1)\,\theta = 1 - O(1/N). \qquad (17)$$

Quantum search: the Grover algorithm

Operator U_ω has to be applied once in every step, hence also function f has to be examined once in every step.

The previous result means that our search is $\sqrt{N}$ times shorter than in a classical case. However, we have to be careful, because in case we do not stop iterating in time, we will move away from ω.

Quantum search: the Grover algorithm

Let us consider a simple case, where $N = 4$. Though, in this situation θ is not small, but our method works well, because $\sin\theta = 1/2$ and from this it directly follows $\theta = \pi/6$, that is after one rotation the value of the angle $3\theta = \pi/2$.

This means that the result is equal to ω exactly.

Quantum search: the Grover algorithm

If we wanted to solve this problem using classical search, the expectation value of the number of tryings would be

$$1 \cdot \frac{1}{4} + 2 \cdot \frac{1}{4} + 3 \cdot \frac{1}{4} + 4 \cdot \frac{1}{4} = 2.5.$$