

УДК 53.087/.088; 53.072; 53:004;
53.08:004; 002.6:004.65; 002.6:004.62/.63

^{1,2}A.S. Kussainov*, ³S.G. Kussainov, ¹G.B. Turmaganbet

¹Physics and Technology Department, al-Farabi Kazakh National University, Kazakhstan, Almaty

²National Nanotechnology Open Laboratory, al-Farabi Kazakh National University, Kazakhstan, Almaty

³K.I. Satpaev Kazakh National Technical University, Kazakhstan, Almaty

*E-mail: arman.kussainov@gmail.com;

Computer model of the Grover's algorithm

We have implemented and tested the basic steps of the computer model of the Grover's algorithm for searching an unsorted database using Matlab software. The quantum, probabilistic algorithm of Lov Grover achieves this using $O(N^{1/2})$ queries. The algorithm starts from the simulated quantum states superposition that is treated later with the Grover's diffusion operator and its modification known as the quantum oracle, representing together the Grover's iteration. The freedom of choice for the initial superposition of states is provided. Projection operator and measurement procedures are implemented using the basic Dirac bra-ket notation in the separate Matlab functions. The existence of an optimal time for a near-optimal measurement as a function of the number's of the Grover's iteration is demonstrated. Extension to the space with multiple targets is available.

Key words: Quantum algorithm, Grover's algorithm, oracle, computer model, Grover's iteration.

А.С. Құсаинов, С.Г. Құсаинов, Г.Б. Тұрмағанбет
Гровер алгоритмінің компьютерлік моделі

Матлаб бағдарламалық қамсыздандыруын пайдалана отырып, реттелмеген мәліметтер базасындағы жазбаны іздеуге арналған кванттық Гровер алгоритмінің компьютерлік моделі жасап шығарылды және тексерілді. Лов Гровердің ықтималды табиғатқа ие кванттық алгоритмі $O(N^{1/2})$ амал ішінде нәтижеге дұрыс шешім алудың ең үлкен ықтималдығымен қол жеткізеді. Алгоритм өз жұмысын таза күйлердің суперпозициясын инициализациялаумен бастайды, кейіннен ол Гровердің диффузиялық операторының және оның кванттық оракул деген атаумен танымал модификациясының әсеріне ұшырайды, бұлардың жиынтығы Гровер итерациясын құрайды. Кванттық күй векторының бастапқы комбинациясын еркін таңдап алу мүмкіндігі бар. Таңдап алынған базистың проекциясы операторы мен кванттық жүйеге өлшеу жүргізу рәсімі Дирак формализмінің бра және кет векторларының көмегімен жүзеге асырылды. Ізделініп отырған шаманың амплитудасын Гровер итерациялары санының функциясы ретінде максимизациялау үшін ең ұтымды уақыт $\sim O(N^{1/2})$ екендігі көрсетілді. Сондай-ақ алгоритмнің бір уақытта бірнеше жазбаны іздестіруге арналған нұсқасына да қол жеткізілді.

Түйін сөздер: кванттық алгоритм; Гровер алгоритмі, оракул, компьютерлік модель, Гровер итерациясы.

А.С. Құсаинов, С.Г. Құсаинов, Г.Б. Турмағанбет
Компьютерная модель алгоритма Гровера

Используя программное обеспечение Матлаб, была написана и протестирована компьютерная модель квантового алгоритма Гровера для поиска записи в неупорядоченной базе данных. Квантовый, вероятностный по своей природе алгоритм Лова Гровера достигает результата, с максимально возможной вероятностью правильного ответа, за $O(N^{1/2})$ операции. Алгоритм начинает работу с инициализации суперпозиции чистых состояний, которая в дальнейшем подвергается воздействию диффузионного оператора Гровера и его модификации, известной как квантовый оракул, в совокупности представляя итерацию Гровера. Предоставлена свобода выбора первоначальной комбинации квантового вектора состояния. Оператор проекции на выбранный базис и процедура проведения измерения над квантовой системой были реализованы с использованием бра и кет формализма Дирака. Продемонстрирован факт наличия оптимального времени $\sim O(N^{1/2})$ для максимизации амплитуды искомой величины как функции числа итераций Гровера. Доступна версия алгоритма с одновременным поиском нескольких записей.

Ключевые слова: квантовый алгоритм, алгоритм Гровера, оракул, компьютерная модель, итерация Гровера.

Introduction

Within the broad range of existing quantum algorithms there is a set of procedures unified by the use of so-called oracular algorithms. The later ones are referring to the quantum computation realization of the oracle machine [1]. Oracle is an entity from the complexity theory and computability theory that is designed and exists to make a decision based on some input. There are up to 30 oracular algorithms listed at [2] with the range of speed up from a constant multiplier and up to superpolynomial and exponential.

Here we are presenting the simple computer model of the Grover's algorithm [3] whose oracle is assisting to find the target entry in the questioned database. We have demonstrated the simple software version of the oracle algorithm within the set of procedures altering the expectation probability of the states' superposition.

Methods

Assuming the N dimensional space could be provided by $n=\log_2 N$ number of qubits, we construct the initial superposition of states as follows

$$\begin{aligned} U_w |w\rangle &= -|w\rangle \\ U_w |x\rangle &= |x\rangle \quad \text{for all } x \neq w \\ &\text{or} \\ U_w &= I - 2|w\rangle\langle w| \end{aligned} \quad (2)$$

where the purpose of the oracle operator U_w is to flip the sign of the target state $|w\rangle$, see again [3]. Matlab's $Uw.m$ function providing the desired effect will look like this

```
1 function y = Uw(a,b,w)
2 % assuming that both a and b are the raw
vectors...
3 a=rot90(a,-1); b=conj(b);
4 y=a*b(1);
5 for i=2:length(b)
6 y=[y a*b(i)];
7 end
8 y=eye(length(a),length(b))-2*y;
9 y=w*y;
```

Scalar, or dot product, is defined to follow the regular Dirac bra-ket notation

$$\langle s|w\rangle = \langle w|s\rangle = 1/\sqrt{N} \quad (3)$$

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^N |x\rangle, \quad (1)$$

where Hadamard transform may be used to put each qubit in the equal probability superposition state. This could be easily achieved in the following few lines

```
1 clear all; close all; clc;
2 s=[1 1 1 1 1 1 1 1 1 1 1];
3 % normalize
4 N=length(s); s=s/sqrt(N);
5 w=[0 0 0 0 0 0 0 0 0 1 0];
6 disp('Amplitudes of initial pure states
uniform superpositon |s>')
7 disp(s.^2)
```

where the index of a target entry w is marked as a nonzero raw vector's entry at line 5 and the superposition of the pure states is a simple one row matrix with the entries corresponding to the initial probability amplitudes distribution.

Quantum oracle will be described by function f which maps each database entries to 0 or to 1, where $f(\omega)=1$ if and only if ω satisfies the search criterion. In terms of unitary operator U_w it could be written as

with Matlab's $braket.m$ function performing the entry wise multiplication taken the form

```
1 function y = braket(s,w)
2 % assuming that both a and b are the raw
vectors...
3 s=conj(s); w=rot90(w,-1);
4 y=s*w;
```

Our Grover's diffusion operator is a combination of a projection operator and a unity operator I

$$U_s = 2|s\rangle\langle s| - I \quad (4)$$

with Matlab $Us.m$ function which looks like this

```
1 function y = Us(a,b,s)
2 % assuming that both a and b are the raw
vectors...
3 a=rot90(a,-1); b=conj(b);
```

```

4  y=a*b(1);
5  for i=2:length(b)
6    y=[y a*b(i)];
7  end
8  y=2*y-eye(length(a),length(b));
9  y=s*y;

```

Here, from line 3 till line 7 we can clearly see a projection operator $|s\rangle\langle s|$.

Consecutive application of U_s and U_w operators preceded by the initial mixture of pure states initialization, see Eq.1, leads to the increase of the amplitude of the search-for element after one iteration as big as

$$|\langle w|s\rangle|^2 = 1/N \text{ to } |\langle w|U_s U_w s\rangle|^2 \approx 9/N \quad (4)$$

Altogether, the main Matlab *Grover.m* function will take a form

```

1  clear all;closeall;clc;
2  s=[1 1 1 1 1 1 1 1 1 1 1 1];
3  % normalize
4  N=length(s); s=s/sqrt(N);
5  w=[0 0 0 0 0 0 0 0 0 0 1 0];
6  disp('Amplitudes of initial pure states
uniform superpositon |s>')
7  disp(s)
8  %disp('Initialize operator Us=2|s><s|-I')
>Columns 1 through 13
>0.27740.27740.27740.27740.27740.27740.27740.27740.27740.27740.27740.2774
>sp =
>Columns 1 through 13
>0.27740.27740.27740.27740.27740.27740.27740.27740.27740.2774-0.2774
>sp =
>Columns 1 through 13
>0.1920 0.19200.19200.19200.19200.19200.19200.19200.19200.19200.19200.74670.1920

```

This increase in amplitude has a cyclic nature given by the following expression

$$\sin^2((r + 1/2)\theta) \quad (5)$$

meaning that the earliest time when we get the maximum achievable amplitude is

$$r \approx \pi\sqrt{N}/4 \quad (6)$$

Discussion

As we can see, the basic elements of the Grover's algorithm are straightforward in

```

9  sp=Uw(w,w,s) % (w,w,s)!! not (w,w,sp)
yet!!!

```

```

10 sp=Us(s,s,sp)

```

```

11 sp.^2

```

Results

Algorithm described above leads to the consecutive changes in amplitudes of the initial equiprobable state superposition, see the analytical expression provided by Eq.4, as following

>Amplitudes of initial pure states uniform superposition $|s\rangle$

implementation as a program code. Besides numerical output on the screen and to the data file we can supplement our results by the graphical representation of an effect caused by a consecutive application of the operators U_s and U_w leading to the cyclic change of the amplitude of the searched element w as plotted along the y axis on Figure 1.

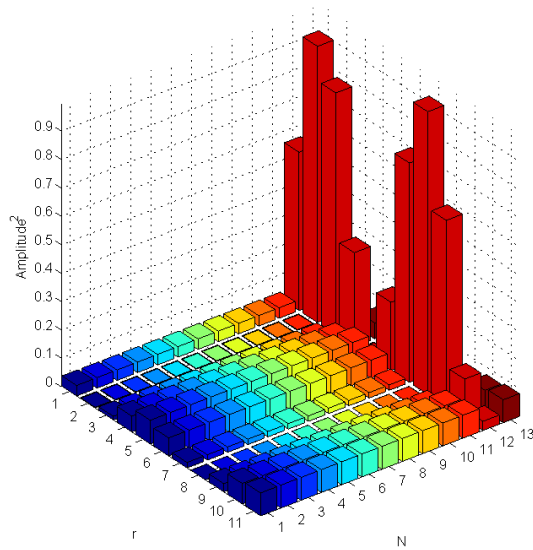


Figure 1 – Bar diagram displaying the squared amplitude distribution for the N states superposition after $r=11$ iterations of the Grover's algorithm.

Conclusions

We have shown the basics of the quantum Grover's computation algorithm implementation using Matlab software. The generalization of the Grover's algorithm is known as the amplitude estimation and is now an essential part of practically every quantum algorithm. The algorithm has a substantial individual value as well as indispensable role within the structures of the other algorithms. The program is written as an educational and research software.

Acknowledgements

This research was supported by a research grant №2532/ГФЗ provided by the Science Committee at the Ministry of Science and Education of Republic of Kazakhstan to the principal investigator at the National Nanotechnology Open Laboratory.

Работа выполнена при финансовой поддержке гранта Комитета Науки МОН РК №2532/ГФЗ в ДГП на ПХВ "Национальная нанотехнологическая лаборатория открытого типа" РГП на ПХВ "КазНУ им. аль-Фараби" Министерства образования и науки РК.

References

1. Nielsen M.A., Chuang I.L. Quantum computation and quantum information/ Cambridge University Press.- 2000.-Ch.6.- P.248.
2. Quantum algorithm zoo.-<http://math.nist.gov/quantum/zoo>
3. Grover's algorithm.-http://en.wikipedia.org/wiki/Grover's_algorithm