ТЕОРЕТИЧНА ЕЛЕКТРОТЕХНІКА *ELECTRICAL ENGINEERING*
2010. Вип. 61. С.49-59 *2010. Is. 61. P.49-59*

УДК 004.652

ЧИСЛОВЕ МОДЕЛЮВАННЯ АЛГОРИТМУ ГРОВЕРА ДЛЯ КВАНТОВОГО ПОШУКУ ДАНИХ

Б. Павлишенко
Львівський національний університет імені Івана Франка
вул. Драгоманова, 50, 79005 Львів, Україна
pavlsh@yahoo.com

Розглянута в роботі числова модель квантового алгоритму Гровера дає змогу проаналізувати зміни амплітуд квантових станів для реалізації квантового пошуку у випадку рівномірного та довільного розподілу цих амплітуд. Проаналізовано вибір оптимальної кількості ітерацій Гровера для підсилення амплітуд шуканих квантових станів.

Ключові слова: квантовий комп'ютер, квантові обчислення, квантовий алгоритм Гровера.

Вступ. Квантові комп'ютери та алгоритми є новим перспективним напрямом сучасних інформаційних технологій. Вони дають змогу суттєво пришвидшити розв'язування деяких класів задач унаслідок реалізації квантового паралелізму та заплутаності квантових станів. Одним з відомих кванових алгоритмів є алгоритм Гровера для пошуку даних у неструктурованій базі даних [1, 2, 3]. Цей алгоритм допомагає знайти дані, які відповідають певним критеріям, за час $O(\sqrt{N})$, використовуючи $O(\log N)$ елементів пам'яті, де N – кількість елементів бази даних. Порівняно з класичним алгоритмом, у якому пошук відбувається за час $O(N)$, алгоритм Гровера дає квадратичне прискорення розв'язування, що актуальне в разі великих значень N. Особливість квантового алгоритму Гровера є та, що він є ймовірнісним алгоритмом, тобто дає правильний розв'язок із заданою ймовірністю, яку можна збільшити шляхом повторного використання алгоритму. Алгоритм Гровера може бути складовою частиною інших квантових алгоритмів, зокрема, у праці [4] його використано для еволюційного аналізу клітковых автоматів.

На сучасному етапі розвитку квантових комп'ютерів розроблені лише елементарні базові елементи та пристрої з квантовим регістром, який містить декілька кубітів. Тому паралельно з розвитком елементарної бази є необхідність розробки систем числового моделювання квантових алгоритмів на класичних комп'ютерах. Розглянемо числове моделювання алгоритму Гровера для реалізації квантового пошуку даних.

Базові елементи квантових обчислень. Проаналізуємо базові квантові принципи реалізації квантових алгоритмів [5, 6]. Основною відмінністю квантового біта – кубіта – від класичного біта є те, що кубіт, крім станів $|0\rangle$ і $|1\rangle$, може також перебувати в суперпозиції цих станів

$$|\psi\rangle = a|0\rangle + b|1\rangle. \quad (1)$$

Стани $|0\rangle$ і $|1\rangle$ є базисними векторами, які можна записати у матричному вигляді:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \quad (2)$$

Регістр з n кубітів $|x_1, x_2, ...x_n\rangle$ утворює суперпозицію з $N = 2^n$ станів, яку можна записати так:

$$|\psi\rangle = \sum_{i=0}^{N} a_i |i\rangle. \quad (3)$$

Ортонормований базис $\{ |0\rangle, |1\rangle, ...|2^n - 1\rangle \}$ називають обчислювальним базисом.

Розглянемо однокубітні квантові вентилі. Розрахунки в квантових алгоритмах виконують за допомогою унітарних перетворень, які можна трактувати як повороти комплексного векторного простору. Проаналізуємо базові операції над кубітами. Оператор тотожного перетворення не змінює значення кубітів і має вигляд

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \quad (4)$$

Операцію заперечення використовують для реалізації інверсії значень кубітів і визначають так:

$$X = |0\rangle\langle 1| + |1\rangle\langle 0|. \quad (5)$$

У спінорному зображенні оператор заперечення має вигляд матриці

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \quad (6)$$

Одним з важливих елементів є “контрольоване НІ”, яке відбувається над двома кубітами і змінює значення другого кубіта на протилежне, якщо значення першого кубіта дорівнює 1. Цей логічний елемент можна визначити як

$$U_{CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X, \quad (7)$$

а матриця оператора унітарного перетворення «контрольоване НІ» має вигляд

$$U_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \quad (8)$$

Дію вентиля “контрольоване НІ” можна зобразити так:

$$U_{CNOT} : |a, b\rangle \to |a, a \oplus b\rangle, \quad (9)$$

де $\oplus$ означає підсумування за модулем 2.

Ще одним важливим логічним елементом є вентиль Тофолі, який діє на три кубіти і змінює значення третього кубіта на протилежне, якщо значення першого та другого кубітів дорівнює 1. Від логічного елемента “контрольоване НІ”

вентиль Тофолі відрізняється наявністю ще одного додаткового керівного кубіта. Цей вентиль можна визначити так:

$$T = |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes U_{CNOT} . \quad (10)$$

Перетворення Тофолі зображають у такому вигляді:

$$T : |a,b,c\rangle \to |a,b,c \oplus ab\rangle . \quad (11)$$

Вентиль Тофолі є універсальним квантовим логічним елементом, на основі якого можна побудувати оборотну квантову машину Тюрінга.

Основні положення алгоритму Гровера. Розглянемо основні кроки реалізації алгоритму Гровера з погляду числового моделювання [1–3]. Нехай є деяка система, яка має $N = 2^n$ станів. Такою системою може бути суперпозиція станів квантового регістра *n* кубітів $|x_1, x_2, ...x_n\rangle$. Множину цих станів позначимо $\{S_1, S_2, ...S_n\}$. Нехай існує деякий стан S_q, для якого

$$f(S_q) = 1 , \quad (12)$$

а для всіх решти станів

$$f(S_i) = 0 . \quad (13)$$

Проблема пошуку в квантовій базі даних зводиться до пошуку стану S_q, який задовольняє умову (12).

В алгоритмі Гровера використано два регістри кубітів. У першому регістрі є *n* кубітів $|x_1, x_2, ...x_n\rangle$, що дає змогу записати $N = 2^n$ заданих квантових станів, а в другому регістрі – лише один кубіт, який є допоміжним і який часто називають анцилою. Введемо поняття квантового оракула. Нехай існує деяка послідовність формалізованих унітарних перетворень, які дають змогу обчислити деяку наперед задану функцію. Дію такого унітарного оператора U_f на систему двох регістрів можна описати так:

$$U_f : |x_1, x_2, ...x_n\rangle|a\rangle \to |x_1, x_2, ...x_n\rangle|a \oplus f(x_1, x_2, ...x_n)\rangle , \quad (14)$$

де $\oplus$ означає підсумовування за модулем 2. Деталізація оператора U_f не є суттєвою для розгляду алгоритму.

Розглянемо послідовні кроки реалізації алгоритму Гровера. На початковому етапі регістр *n* кубітів переведемо в нульовий стан:

$$|x_1, x_2, ..., x_n\rangle_n \to |0_1, 0_2, ..., 0_n\rangle_n . \quad (15)$$

До кожного кубіта регістра застосуємо однокубітне перетворення Адамара, яке у спінорному базисі зображають матрицею

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} . \quad (16)$$

У підсумку отримаємо

$$H^{\otimes n} |0_1, 0_2, ..., 0_n\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{x=1}^{x=2^n} |x\rangle , \quad (17)$$

де $|x\rangle$ – номер базисного стану квантового регістра $|x_1, x_2, ..., x_n\rangle_n$.

Перетворення Адамара приводить початковий стан (15) до суперпозиції всіх можливих станів з однаковою амплітудою.

Розглянемо додатковий кубіт $|a\rangle$ в стані $|1\rangle$ і подіємо на нього оператором Адамара:

$$|-\rangle = H|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right). \tag{18}$$

Подіємо оператором квантового оракула U_f на систему регістрів $|x\rangle|-\rangle$, уважаючи, що $|x\rangle = |x_1, x_2, ...x_n\rangle$, отримаємо

$$U_f : |x\rangle|-\rangle \to (-1)^{f(x)}|x\rangle|-\rangle. \tag{19}$$

Особливістю унітарної операції (19) є те, що коли кубіт $|a\rangle$ перебуває в стані $|-\rangle$, то він не змінюється під впливом оператора U_f, а в шуканих станах, для яких виконується умова $f(x)=1$, відбувається інверсія знака амплітуди стану. Унаслідок застосування унітарного перетворення U_f до суперпозиції станів (17) отримаємо

$$|\psi_R\rangle = U_f\left(|\psi_c\rangle|-\rangle\right) = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}(-1)^{f(x)}|\psi_c\rangle|-\rangle. \tag{20}$$

У суперпозиції $|\psi_R\rangle$ є всі базові стани, однак шукані стани позначені від'ємним знаком амплітуди. Цей результат ми отримали внаслідок реалізації квантового паралелізму, коли унітарне перетворення відбувається над усіма квантовими станами одночасно. Подальше завдання полягає в тому, щоб позначені від'ємним знаком амплітуди шуканих станів максимально підсилити й отримати їх під час процедури вимірювання. Введемо деякий унітарний оператор U_q, який буде порівнювати елементи бази даних $\{S_1, S_2, ...S_n\}$ згідно з деяким критерієм. Уважаємо, що він діє так:

$$U_q|q\rangle \to -|q\rangle$$
$$U_q|x\rangle \to |x\rangle \text{ для всіх } x \neq q. \tag{21}$$

Оператор U_q можна також розглянути у вигляді

$$U_q = I - 2|q\rangle\langle q|, \tag{22}$$

де I – оператор тотожного перетворення. Оператор U_q є оператором інверсії знака квантового стану і виконує в алгоритмі Гровера функції оракула U_f.

Уведемо оператор інверсії відносно середнього, який має вигляд

$$S_c = 2|\psi_c\rangle\langle\psi_c| - I, \tag{23}$$

де $|\psi_c\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}}\sum_{i=0}^{i=2^n-1}|i\rangle$.

Основою алгоритму квантового пошуку є ітерація Гровера, яка складається з двох розглянутих операторів – оператора інверсії знака та інверсії відносно середнього:

$$U_G = S_c U_q. \tag{24}$$

Застосуємо ітерацію Гровера до суперпозиції станів $|\psi_R\rangle$ k разів. Кількість ітерацій k визначена кількістю можливих розв'язків і є окремою проблемою в

алгоритмі Гровера. На наступному кроці алгоритму виконаємо вимірювання квантового регістра. З імовірністю, близькою до 1, отримаємо шуканий результат.

Розглянемо детальніше реалізацію ітерації Гровера. З погляду геометричної інтерпретації дія оператора U_q на деякий вектор еквівалентна дзеркальному відображенню цього вектора в гільбертовому просторі відносно гіперплощини, ортогональної до вектора $|q\rangle$. Дія оператора S_c на деякий вектор полягає в дзеркальному відображенні цього вектора відносно лінії, яка проходить через вектор $|\psi_c\rangle$. Отже, після застосування операторів U_q та S_c вектор суперпозиції станів $|\psi_R\rangle$ залишається в площині, утвореній векторами $|q\rangle$ і $|\psi_c\rangle$. Після кожної ітерації Гровера вектор суперпозиції $|\psi_R\rangle$ повертається на деякий кут θ в напрямі вектора шуканого стану $|q\rangle$. Важливим в алгоритмі Гровера є правильний вибір кількості необхідних ітерацій *k*, оскільки, наблизившись до стану $|q\rangle$, у разі подальших ітерацій вектор $|\psi_R\rangle$ буде від цього стану віддалятись. У працях [1, 3] з'ясовано, що оптимальна кількість ітерацій Гровера у випадку одного розв'язку

$$k \approx \frac{\pi}{4}\sqrt{N}, N = 2^n. \tag{25}$$

Якщо заданому критерію пошуку відповідає m квантових станів, то

$$k \approx \frac{\pi}{4}\sqrt{\frac{N}{m}}. \tag{26}$$

Проаналізуємо реалізацію оператора інверсії відносно середнього S_c. Оператор інверсії можна описати сукупністю однокубітних операторів Адамара та операторів інверсії стану кубіта відносно базисного вектора $|0\rangle$:

$$S_c = H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n}. \tag{27}$$

Перетворення S_c можна зобразити так:

$$S_c : \sum_i a_i |i\rangle \to \sum_i (2A - a_i)|i\rangle, \tag{28}$$

де A – середнє значення амплітуд a_i. Оператор S_c описують унітарною матрицею, елементи якої визначені правилом

$$S_{ij} = \begin{cases} \frac{2}{N}, i \neq j, \\ \frac{2}{N} - 1, i = j. \end{cases} \tag{29}$$

Як з'ясовано в [1], матрицю S_{ij} можна зобразити як добуток матриць трьох операторів

$$S = H^{\otimes n} R H^{\otimes n}, \tag{30}$$

$$\text{де } R = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & -1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & -1 \end{pmatrix}. \tag{31}$$

Отже, для реалізації ітерації Гровера достатньо однокубітних перетворень Адамара та оператора зсуву фази.

Числове моделювання ітерації Гровера. Для ефективної побудови квантових систем з елементами алгоритму Гровера необхідно виконувати кількісний числовий аналіз зміни амплітуд квантових станів у разі реалізації ітерацій Гровера U_G, яка визначена виразом (24). Також необхідно оцінити оптимальну кількість ітерацій U_G за заданих розмірів квантового регістра та очікуваної кількості шуканих станів, які відповідають критеріям пошуку. З ураховуванням розглянутих кроків алгоритму Гровера та декомпозиції ітерації U_G створено числову модель алгоритму Гровера. Для числового розрахунку розглянемо квантову систему з чотирьох кубітів, які утворюють суперпозицію 16 станів, три з яких відповідають заданим критеріям пошуку. На рис. 1 показано інверсію знаків амплітуд шуканих станів унаслідок дії оператора U_q. По осі ординат відкладено номери квантових станів $|i\rangle$. На рис. 2 зображено амплітуди станів після дії оператора інверсії відносно середнього S_c. Як випливає з наведених даних, унаслідок реалізації ітерації Гровера спостерігають суттєве підсилення амплітуд шуканих станів.

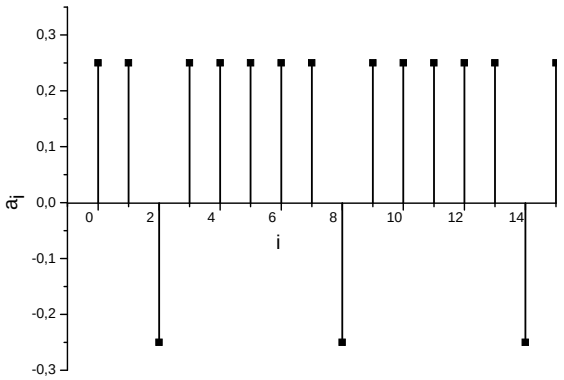

Рис. 1. Інверсія знаків амплітуд шуканих квантових станів унаслідок дії оператора U_q в разі рівномірного початкового розподілу амплітуд.

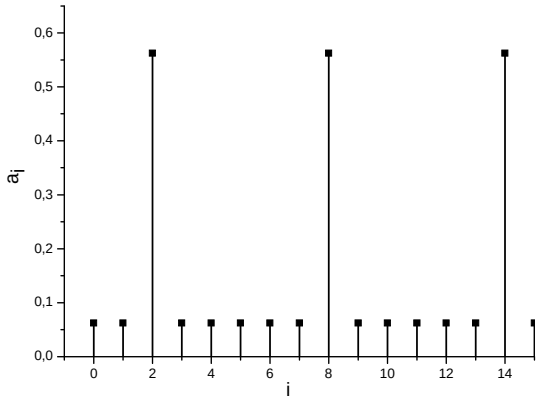

Рис. 2. Підсилення амплітуд шуканих квантових станів унаслідок дії оператора інверсії відносно середнього S_c.

У деяких квантових задачах вхідні амплітуди квантових станів можуть бути неоднакові. На рис. 3 показана числова модель нерівномірного розподілу амплітуд квантових станів, а на рис. 4, 5 – амплітуди станів після інверсії знака амплітуд шуканих станів та інверсії відносно середнього. Якщо амплітуди шуканих станів суттєво відрізняютья від амплітуд інших станів суперпозиції, то після деякої кількості ітерацій стани з великими значеннями амплітуд можуть також змінювати знак після реалізації унітарного перетворення S_c, що може спотворити результат, додавши хибні розв'язки. З рис. 5 випливає, що після дії оператора інверсії відносно середнього поряд з підсиленням шуканих амплітуд деякі амплітуди набувають від'ємного знака. На наступній ітерації Гровера в разі дії оператора інверсії амплітуд поряд із шуканими станами будуть також від'ємні амплітуди станів, які не пов'язані з розв'язком. Амплітуди цих станів також підсилюватимуться на наступних ітераціях. Отже, у випадку нерівномірного розподілу амплітуд квантових станів на вході алгоритму Гровера необхідно враховувати характер їхнього розподілу і вводити додаткові оператори корекції.

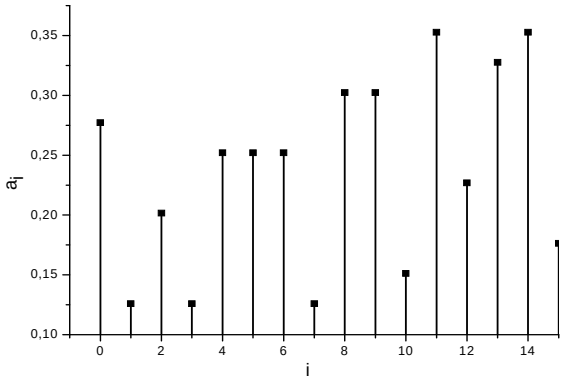

Рис. 3. Числова модель нерівномірного розподілу амплітуд квантових станів.

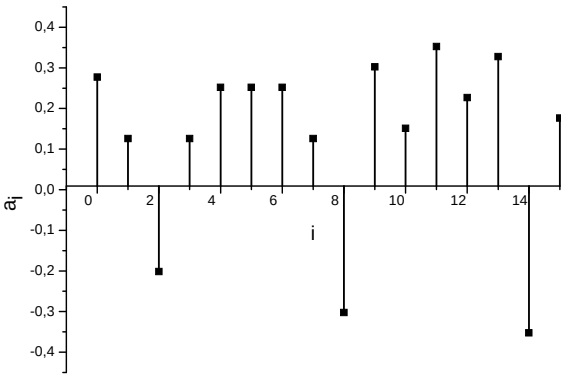

Рис. 4. Інверсія знаків амплітуд шуканих квантових станів унаслідок дії оператора U_q у разі нерівномірного початкового розподілу амплітуд.

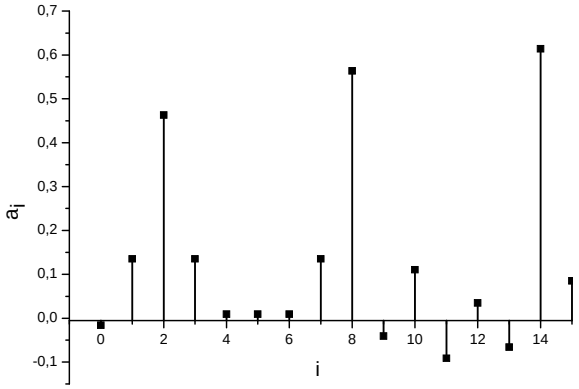

Рис. 5. Підсилення амплітуд шуканих квантових станів унаслідок дії оператора інверсії відносно середнього S_c у випадку нерівномірного початкового розподілу амплітуд.

Розглянемо як змінюється ймовірність знаходження шуканого стану в разі процедури вимірювання регістра залежно від кількості ітерацій Гровера. На рис. 6 зображено числовий розрахунок ймовірності коректного розв'язку залежно від кількості ітерацій U_G за одного та п'яти шуканих станів у випадку квантового регістра з десяти кубітів, які утворюють суперпозицію з 1024 квантових станів.

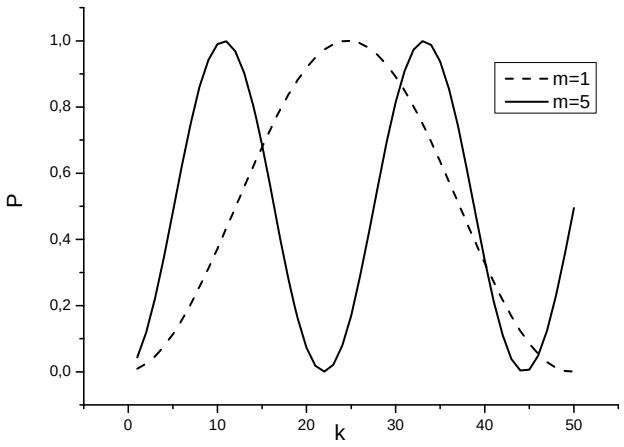

Рис. 6. Залежність ймовірності коректного розв'язку від кількості ітерацій Гровера у випадку одного та п'яти шуканих станів в суперпозиції 1024 квантових станів

Висновок. Розглянута числова модель квантового алгоритму Гровера дає змогу проаналізувати зміни амплітуд квантових станів у процесі реалізації квантового пошуку у випадку рівномірного та довільного розподілів амплітуд, що допомагає оптимізувати квантовий алгоритм пошуку для заданої квантової системи. Однією з важливих проблем у разі реалізації квантового алгоритму

пошуку є вибір оптимальної кількості ітерацій Гровера для підсилення амплітуд шуканих станів. Знайти оптимальну кількість ітерацій можна за допомогою числового аналізу залежності ймовірності знаходження коректного розв'язку від кількості ітерацій. Такий аналіз необхідно виконати для випадків різної кількості розв'язків. Це дасть змогу побудувати оптимальну серію реалізацій алгоритму з різною кількістю ітерацій Гровера, враховуючи характер поставленої задачі.

1. *Grover L.K.* Quantum Mechanics helps in searching for a needle in haystack // Phys.Rev. Lett. 1997. Vol. 79(2). P. 325–328.
2. *Zalka C.* Grover's quantum searching algorithm is optimal // Phys. Rev. A., 1999. Vol. 60(4). P. 2746–2751.
3. *Lavor C., Manssur L.R.U., Portugal R.* Grover's Algorithm: Quantum Database Search [Електронний ресурс] // arXiv:quant-ph/0301079v1. 2003.
4. *Pavlyshenko B.* Quantum Algorithm of Evolutionary Analysis of 1D Cellular Automata [Електронний ресурс] // arXiv:1001.4870v1. 2010.
5. Крохмальський Т. Квантові комп'ютери: основи й алгоритми (короткий огляд) // Журн. фіз. досліджень. 2004. Т. 8. № 4. С. 1–15.
6. *Китаев А., Шень А., Вялий М.* Классические и квантовые вычисления. М.: МЦНМО, ЧеРо, 1999. 192 с.

NUMERIC MODELING OF GROVER'S ALGORITHM FOR QUANTUM DATA SEARCH

B. Pavlyshenko

Ivan Franko Lviv National University,
Dragomanov Str. 50, Lviv, UA–79005 Ukraine
e-mail: pavlsh@yahoo.com

A numeric model of the Grover's algorithm considered in the present work enables one to analyze the changes in the amplitudes of quantum states for realization of quantum search in the cases of uniform or arbitrary distributions of those amplitudes. A choice of optimal number of the Grover's iterations needed for amplification of the quantum states under search is analyzed.

Key words: quantum computer, quantum calculations, quantum Grover's algorithm.

ЧИСЛЕННОЕ МОДЕЛИРОВАНИЕ АЛГОРИТМА ГРОВЕРА ДЛЯ КВАНТОВОГО ПОИСКА ДАННЫХ

Б. Павлишенко

Львовський национальный университет имени Івана Франка
ул. Драгоманова, 50, 79005 Львов, Украина
pavlsh@yahoo.com

Рассмотренная в работе численная модель квантового алгоритма Гровера дает возможность проанализировать изменения амплитуд квантовых состояний при реализации квантового поиска в случае равномерного и произвольного распределения этих амплитуд. Проанализировано оптимальное количество итераций Гровера для усиления амплитуд искомых квантовых состояний.

Ключевые слова: квантовый компьютер, квантовые вычисления, квантовый алгоритм Гровера.

Стаття надійшла до редколегії 28.04.2010
Прийнята до друку 26.05.2010