УДК 004.421.2:537.611

Г.П. Горський, магістр,
В.Г. Дейбук, д-р. фіз.-мат. наук, проф.,
Чернівец. нац. ун-т ім. Ю. Федьковича

АЛЬТЕРНАТИВНИЙ КВАНТОВИЙ АЛГОРИТМ ПОШУКУ В БАЗІ ДАНИХ

Г.П. Горський, В.Г. Дейбук. **Альтернативний квантовий алгоритм пошуку в базі даних.** В програмному середовищі емулятора QCE розроблено і апробовано альтернативний до алгоритма Гровера квантовий алгоритм пошуку в базі даних, який на відміну від алгоритма Гровера має не експоненціальну, а лінійну складність.

Г.П. Горский, В.Г. Дейбук. **Альтернативный квантовый алгоритм поиска в базе данных.** В программной среде эмулятора QCE разработан и апробирован альтернативный алгоритму Гровера квантовый алгоритм поиска в базе данных, который в отличие от алгоритма Гровера обладает не экспоненциальной, а линейнойю сложностью.

G.P. Gorskiy, V.G. Deibuk. **Alternative quantum search algorithm in a database.** By QCE emulator alternative quantum search algorithm has been designed and probed. It differs from Grover's algorithm by linear difficulty. Grover's algorithm in contrast has exponent difficulty.

Надії науковців і практиків на квантовий комп'ютер (КК) головно пов'язані з явищем так званого квантового паралелізму, яке не притаманне класичним комп'ютерам [1]. Суть явища полягає в тому, що в квантовому комп'ютері кожен квантовий біт (КвБ) рівноймовірно з імовірністю 0,5 може перебувати як в стані логічного нуля (0), так і в стані логічної одиниці (1). Таким чином, у квантовому регістрі довжини n може рівноймовірно і одночасно зберігатись і оброблятись 2^n n-розрядних двійкових чисел (слів). Це дозволяє істотно підвищити продуктивність обробки інформації. КвБ можуть репрезентуватись різноманітними квантово тотожними фізичними об'єктами, головною вимогою до яких є наявність у кожного чітко виражених двох станів, які відрізняються енергією. Такими об'єктами можуть бути, наприклад, окремі електрони, або ж так звані ферміонні атомні ядра. Кожний з таких електронів або ядер має власний механічний момент кількості руху, або ж спін (від англійського слова "spin" – дзиґа). Цей момент, наприклад, для електронів може мати значення $\pm h/4\pi$, де h — стала Планка, верхній знак відповідає орієнтації "вгору", а нижній — орієнтації "вниз". Таке наочне уявлення є, звичайно, дуже спрощеним, оскільки, ні електрон ні атомне ядро не можна уявити, наприклад, кулькою, яка обертається навколо якої-небудь осі.

Маючи власнийм механічний момент кількості руху, електрони або атомні ядра, будучи зарядженими частинками, з необхідністю мають і власний магнітний момент, а, отже, і здатність переважно орієнтуватись вздовж або проти напрямку зовнішнього магнітного поля (в залежності від знаку заряду). Якщо КвБ репрезентуються електронами, то внаслідок від'ємного знаку їх заряду переважним напрямком орієнтації електронів є напрямок зовнішнього статичного магнітного поля. Це відповідає основному станові, в якому всі КвБ знаходяться у стані 0 (орієнтовані "вгору"). При зміні напрямку поля на протилежний в ідеальному випадку або при дії радіочастотної (РЧ) складової в реальному випадку відбувається переорієнтація всіх або частини КвБ "униз", тобто перехід їх у стан 1. Таким чином будь-який квантовий алгоритм (КА) — це сукупність таких переходів. Надалі з метою лаконічності викладу будемо, як це умовно прийнято для даного і ряду інших випадків в теоретичній фізиці, замість понять "електрон, якому притаманний спін", "ядро, якому притаманний спін", "система електронів (ядер), які мають спіни", вживати поняття "спін", "система спінів", ототожнюючи (звичайно, суто умовно) *характеристику об'єкта* і власне *об'єкт.*

З викладеного випливає основна відмінність КА від алгоритмів в звичайному розумінні слова (класичних алгоритмів). Класичний алгоритм можна розглядати сам по собі, абстрагуючись від тих апаратних засобів, в межах можливостей яких він реалізується, якщо, звичайно, не йдеться про тонкощі його оптимізації. З КА цього робити не можна, оскільки там "апаратні засоби" і "алгоритм" нероздільні. Таким чином в даному випадку алгоритм невіддільний від законів магнетизму, яким підкоряється функціонування системи спінів як одного з специфічних квантових апаратних засобів. Розроблено два ефективних квантових алгоритми: алгоритм Шора розкладання

великих цілих чисел на прості множники і алгоритм Гровера пошуку в повністю невпорядкованій базі даних (БД) [1].

Рекурсивний КА Гровера полягає у послідовному застосуванні квантової операції "інверсії відносно середнього", внаслідок якої в міру зростання кількості кроків рекурсії ймовірність реалізації шуканого запису поступово наближається до 1. Кількість кроків рекурсії в цьому алгоритмі порядку $\pi\sqrt{N_{rec}}/4$, де N_{rec} — кількість записів у БД. Але при врахуванні явища квантового паралелізму у квантовому регістрі (КР) довжини n вміщується 2^n n-бітових слів, кожне з яких і повинно розглядатись як запис. Отже, кількість операцій в алгоритмі Гровера $N_{op} = 2^{n/2}\,\pi/4$, тобто експоненціально залежить від довжини регістра.

Альтернативний алгоритм пошуку в БД ґрунтується на тому, що коли існує оператор B, який переводить стан $|0...00\rangle$ у повністю невпорядкований, то у відповідності із загальними принципами квантової механіки з необхідністю існує і обернений до нього оператор B^{-1}, який здійснює повернення до початкового стану і який, отже, може бути оператором опитування БД [2]. Таким чином, достатньо кожну одиницю в зображенні шуканого n-бітового слова помітити оператором інверсії, а кожен нуль — тотожним оператором. Тому загальна форма алгоритму пошуку, альтернативного до алгоритма Гровера,

$$f_i = B^{-1}\prod_{l\in M_i} inv_l B|0...00\rangle, \qquad (1)$$

де inv_l — оператор інверсії КвБ з номером l з множини M_i бітів, які в шуканому слові (записі) з номером i повинні бути зайняті одиницями.

Інвертування полягає в повороті спіну, що репрезентує квантовий біт (КвБ), на кут π.

Розглянемо більш детально структуру цього алгоритма, використовуючи залежний від часу гамільтоніан моделі Ізінга, який має вигляд [3]

$$H(t) = -\sum_{i,\mu}(h_{0i}^{\mu} + h_{1i}^{\mu}\sin(2\pi f_i^{\mu}t + \varphi_i^{\mu}))S_i^{\mu} - \sum_{i,j\neq i,\mu} J_{ij}^{\mu}S_i^{\mu}S_j^{\mu}\,, \qquad (2)$$

де h_{0i}^{μ} — статична складова магнітного поля, яка діє на спін i вздовж осі μ;

μ — (x,y,z);

h_{1i}^{μ} — амплітуда РЧ складової магнітного поля, яка діє на спін i вздовж осі μ;

f_i^{μ} — кругова частота РЧ складової магнітного поля, яка діє на спін i вздовж осі μ;

t — час;

φ_i^{μ} — початкова фаза РЧ складової магнітного поля, яка діє на спін i вздовж осі μ;

S_i^{μ} — проекція i-го спіну на вісь μ;

J_{ij}^{μ} — стала обмінної взаємодії між i-м та j-м спінами вздовж осі μ.

КА в середовищі QCE являють собою набори мікроінструкцій (МІ) [3]. Кожна МІ являє собою своєрідний "електронний бланк", в який в інтерактивному режимі вставляються масштабовані параметри гамільтоніану і час його дії. При цьому час зручно вимірювати в безрозмірних одиницях повної фази, тобто 2π. Емулятор розв'язує нестаціонарне рівняння Шредінгера для гамільтоніану (2) із заданими користувачем параметрами методом добутку Сузукі [4]. Результати розв'язання з допомогою спеціального графічно-числового інтерфейсу виводяться на екран і дають можливість визначити ймовірність орієнтації кожного зі спінів у негативному напрямку будь якої з координатних осей. Саме ці результати і використовуються для оцінки коректності роботи КА.

Даний КА розглянемо для випадку ідеального квантового комп'ютера (КК), тобто такого, коли на спіни, що репрезентують квантові біти (КвБ), діють лише статичне магнітне поле та обмінна взаємодія.

Розглянемо спочатку структуру оператора B для двох випадків: парної і непарної кількості розрядів квантового регістра (КР). Найпростішу структуру цей оператор має для парної кількості розрядів. Її можна відобразити операторним рівнянням

$$B_{2n} = W_1W_2g_{12}W_3W_4g_{34}...W_{2n-1}W_{2n}g_{2n-1,2n}\,, \qquad (3)$$

де W_i — оператор Адамара, який переводить i-й КвБ у суперпозиційний стан по проекціях спіну на осі y та z;

g_{ij} — операція обмінної взаємодії між i-м та j-м КвБ з параметрами $J_{ij}^z = -1;\ \tau = 0,5$ (час τ вимірюється в одиницях 2π), яка переводить пару КвБ у суперпозиційний стан по всіх компонентах.

Дію оператора Адамара на k-й КвБ можна відобразити операторним рівнянням

$$W_k = \overline{Y}_k \overline{X}_k^2, \tag{4}$$

де $\overline{Y}_k$ — операція повороту КвБ на кут $-\pi/2$ навколо осі y, параметри якої $h_{0k}^y = -1;\ \tau = 0,25$;

$\overline{X}_k$ — операція повороту КвБ на кут $-\pi/2$ навколо осі x, параметри якої $h_{0k}^x = -1;\ \tau = 0,25$.

Оператор B_{2n}^{-1} відрізняється від оператора B_{2n} оберненим порядком операцій.

Операція інверсії inv_l КвБ з номером l має параметри $h_{0l}^z = 1;\ \tau = 0,5$.

Розглянемо тепер структуру пропонованого КА для випадку непарної кількості розрядів КР виду $2n+3$. Структура оператора B_{2n+3} підготовки абсолютно невпорядкованої БД зі стану $|00...0\rangle$

$$B_{2n+3} = D_3 B_{2n}. \tag{5}$$

де D_3 — оператор підготовки бази для КвБ 1, 2, 3.

Структура оператора D_3

$$D_3 = W_1 W_2 W_3 g_{123}, \tag{6}$$

де g_{123} — операція з параметрами $J_{12}^z = J_{23}^z = J_{13}^z = -1;\ \tau = 0,5.$

Але якщо застосувати, наприклад, до стану $|00000\rangle$ спочатку оператор B_5 зі структурою (5) при врахуванні (6), а потім оператор B_5^{-1}, який отримується з оператора B_5 виконанням всіх операцій в оберненому порядку, то отримаємо

$$B_5^{-1} B_5 |00000\rangle = |00111\rangle. \tag{7}$$

Це співвідношення є вірним при будь якому n. Тому для непарної кількості розрядів виду $2n+3$ будь якому алгоритм пошуку в базі даних можна записати у вигляді

$$f_i = inv_1 inv_2 inv_3 \prod_{l \in M_i} inv_l B_{2n+3}^{-1} B_{2n+3} |0...00\rangle. \tag{8}$$

Емуляція даних алгоритмів в середовищі QCE показала, що вони працюють так. При дії оператора підготовки БД (у відповідності до кількості розрядів або КвБ) з основного стану $|00...0\rangle$, в якому всі КвБ знаходяться у стані логічної одиниці (спіни орієнтовані “вгору”), одержується такий суперпозиційний стан, в якому всі орієнтації спінів рівноймовірні. Виконана після цього інверсія КвБ, які в шуканому n- бітовому слові (записі) повинні бути зайняті одиницями, не змінює стану БД. Однак при цьому шуканий запис отримує унікальну ознаку або мітку. Після цього застосування оператора опитування бази веде до того, що спіни, які в шуканому слові репрезентують КвБ у стані логічного 0, з імовірністю 1 орієнтуються вздовж позитивного напрямку вісі z (угору), а спіни, які репрезентують КвБ у стані логічної 1, з імовірністю 1 орієнтуються вздовж негативного напрямку вісі z (униз). Таким чином, шуканий запис у повністю невпорядкованій БД знаходиться з імовірністю 1, що свідчить про коректну роботу алгоритма.

Розрахуємо кількість операцій (мікроінструкцій) в операторі опитування. Якщо розрядів парна кількість, тобто $2n$, то їх стільки ж, скільки в операторі підготовки бази, тобто $6n + n = 7n$. У відповідності з наведеним означенням БД $2n = \log_2 N$, тому остаточно для парної кількості розрядів кількість операцій

$$N_{op} = 3,5 \log_2 N, \tag{9}$$

де N — кількість записів в базі.

Якщо ж розрядів непарна кількість тобто $2n+3$, то цих операцій є $3(2n+3)+n+1+6=7n+16$. Отже для непарної кількості розрядів кількість операцій

$$N_{op}=3{,}5\log_2 N+5{,}5. \qquad (10)$$

З (9) і (10) видно, що при великій кількості записів кількість операцій пошуку залежить від кількості записів в базі за логарифмічним законом, а не за кореневим, як в алгоритмі Гровера. При кількості записів у базі більшій за 2048 даний алгоритм є істотно більш економічним.

Таким чином, основний результат роботи полягає в тому, що запропонований алгоритм пошуку у повністю невпорядкованій БД, на відміну від існуючого алгоритма Гровера, має не експоненціальну, а лінійну складність в залежності від довжини регістру. Відповідно до цього кількість операцій в пропонованому алгоритмі, на відміну від алгоритму Гровера, залежить від кількості записів не за кореневим, а за логарифмічним законом.

Література

1. Nilsen, M.A. Quantum Computation and Quantum Information / M.A. Nilsen, I.L. Chuang. — N.Y.: Cambridge University Press, 2001. — 822 p.
2. Давыдов, А.С. Квантовая механика / А.С. Давыдов — М.: Наука, 1973. — 704с.
3. Michielsen, K. QCE — quantum computer emulator / K. Michielsen, H. De Raedt // Turk. J. Phys. — 2003. — Vol. 27. — P. 1 — 29.
4. Suzuki, M. Product method for TDSE solving / M. Suzuki, S. Miyashita, A. Kuroda // Progress of Theor. Phys. — 1977. — Vol. 58. — P. 1377 — 1387.

Рецензент д-р фіз.-мат. наук. Чернівец. нац. ун-ту ім. Ю. Федьковича Остапов С.Е.

Надійшла до редакції 1 липня 2009 р.