Общероссийский математический портал

Д. Ли, К. Ли, Х. Хуанг, Фазовое условие для алгоритма Гровера, *ТМФ*, 2005, том 144, номер 3, 472–483

DOI: <https://doi.org/10.4213/tmf1871>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.224.135.184

26 апреля 2023 г., 05:51:08

© 2005 г.

Д.-Ф. Ли*, К.-К. Ли†, Х.-Т. Хуанг‡

ФАЗОВОЕ УСЛОВИЕ ДЛЯ АЛГОРИТМА ГРОВЕРА

В рамках алгоритма Гровера выведена точная формула для нормы амплитуды в отмеченном состоянии в виде функции синуса. С помощью этой формулы выведено необходимое и достаточное фазовое условие $\sin \Delta \leq |\beta|$ для алгоритма Гровера с произвольными фазовыми вращениями. Показано, что условие совпадающих углов поворота, представляющее собой частный случай общего условия, есть достаточное, но не необходимое фазовое условие.

Ключевые слова: алгоритм Гровера, алгоритм квантового поиска, фазовое условие.

1. ВВЕДЕНИЕ

В квантовых алгоритмах обычно используются два метода: преобразование Фурье [1] и амплитудное умножение. На последнем основан алгоритм Гровера, с помощью которого решается проблема поиска отмеченного члена (или *цели* в терминологии работы [2]) в неупорядоченной базе данных размера N . При использовании этого алгоритма цель достигается квантовым компьютером с помощью $O(\sqrt{N})$ вопросов [3]. В оригинальной версии Гровера [3] алгоритм представляет собой последовательность унитарных операций над исходным чистым состоянием, т.е. алгоритм имеет вид $Q = -I_0^{(\pi)} W I_\tau^{(\pi)} W$, где W есть преобразование Уолша–Адамара, и оператор $I_x^{(\pi)} = I - 2|x\rangle\langle x|$ инвертирует амплитуду состояния $|x\rangle$. При этом $I_0^{(\pi)}$ и $I_\tau^{(\pi)}$ инвертируют амплитуды соответственно начального и отмеченного базисных состояний $|0\rangle$ и $|\tau\rangle$. Гровер предложил расширение своего исходного алгоритма в работе [2], где заменил преобразование Уолша–Адамара на произвольную квантово-механическую операцию, получив таким образом алгоритм квантового поиска $Q = -I_\gamma^{(\pi)} U^{-1} I_\tau^{(\pi)} U$, где U – унитарная операция, а U^{-1} – ее сопряженная (комплексно-сопряженная и транспонированная). Боуер и др. нашли аналитические выражения для амплитуды состояний в исходном гроверовском алгоритме

*Department of Mathematical Sciences National Laboratory for Artificial Intellect at Tsinghua University Tsinghua University, Beijing, China. E-mail: dli@math.tsinghua.edu.cn

†Department of Computer Science, Wayne State University, Detroit, MI, USA

‡Electrical Engineering and Computer Science Department University of Michigan, Ann Arbor, MI, USA

с преобразованием Уолша–Адамара и инвертированием амплитуд при довольно жестких ограничениях на алгоритм квантового поиска [4]. Чтобы обобщить алгоритм Гровера, надо допустить не просто инвертированные амплитуды, а амплитуды, повернутые на произвольные фазы. Примером такого обобщения является квантовый алгоритм $Q = -I_{\gamma}^{(\theta)} U^{-1} I_{\tau}^{(\phi)} U$, где θ и ϕ – углы поворотов фаз амплитуд в исходном базисном состоянии $|\gamma\rangle$ и в отмеченном базисном состоянии $|\tau\rangle$, соответственно. В последнее время целый ряд авторов занимался построением подобных алгоритмов квантового поиска с произвольными унитарными операциями и произвольными фазовыми вращениями [5]–[10].

Следующие проблемы должны быть решены для общего алгоритма квантового поиска.

1. Какова амплитуда отмеченного состояния после k применений алгоритма Q ?
2. Какими должны быть углы вращения в исходном и в отмеченном базисных состояниях, чтобы можно было достичь отмеченного состояния, начиная с исходного (*фазовое условие*)?
3. Каково оптимальное число шагов итерации, необходимое для достижения отмеченного состояния?
4. Какой из общих алгоритмов наиболее эффективен?

Основная мотивация данной работы состоит в следующем.

С тех пор как Гровер предложил фазовое условие, оно обсуждалось целым рядом авторов. Чтобы с достоверностью найти отмеченное состояние, Лонг и др. предложили рассматривать условие согласования углов поворота $\theta = \phi$ [5]. Далее, Хойер предложил фазовое условие вида $\text{tg}(\theta/2) = \text{tg}(\phi/2)(1 - 2a)$ [7]. Затем Бихам и др. использовали рекуррентное уравнение для исследования алгоритма квантового поиска и сообщили, что при несовпадающих углах поворота $\theta \neq \phi$ алгоритм не способен увеличить вероятность измерения отмеченного состояния, и для того чтобы применить этот алгоритм, два угла поворота должны совпасть [9]. Таким образом, по мнению этих авторов, совпадение углов поворота $\theta = \phi$ есть необходимое и достаточное фазовое условие. По крайней мере в четырех работах [5], [8], [9] условие совпадающих углов поворота было заявлено как фазовое. Таким образом, открытый вопрос состоит в нахождении необходимого и достаточного фазового условия для алгоритма Гровера с произвольными вращениями фаз. В данной работе предлагается фазовое условие вида $\sin \Delta \leq |\beta|$, которое необходимо и достаточно для достижения отмеченного состояния, и таким образом, решена проблема, поставленная Гровером в работе [2]. Также показано, что условие совпадения углов вращения $\theta = \phi$, представляющее собой частный случай нашего условия, достаточно, но не необходимо для нахождения отмеченного состояния. С помощью точного фазового условия можно строить квантовые алгоритмы с произвольными вращениями, которые достигают успеха с вероятностью единица.

Работа организована следующим образом. В разделе 3 выводится точное выражение для нормы амплитуды отмеченного состояния. В разделе 4 с помощью этой формулы находится необходимое и достаточное фазовое условие для алгоритма Гровера с

произвольными углами поворота. В разделе 5 показано, что условие совпадения углов вращения $\theta = \phi$ представляет собой достаточное, но не необходимое фазовое условие для нахождения отмеченного состояния.

2. АЛГОРИТМ ГРОВЕРА С ПРОИЗВОЛЬНЫМИ ФАЗОВЫМИ ВРАЩЕНИЯМИ

Исходный алгоритм поиска, введенный Гровером [3], использовался для решения следующей задачи: найти в неупорядоченной базе данных, содержащей N элементов, единственный элемент, удовлетворяющий известному свойству (отмеченный элемент). Чтобы выделить отмеченный элемент среди N прочих элементов, алгоритм Гровера производит следующие чередующиеся унитарные преобразования: фазовое вращение R_1 и обращение относительно среднего D . Более того, Гровер показал, что обращение относительно среднего имеет вид $D = W R_2 W$, где R_2 – матрица фазового вращения. В работе [2] Гровер исследовал алгоритм квантового поиска $Q = -I_\gamma^{(\pi)} U^{-1} I_\tau^{(\pi)} U$, где U – унитарный оператор, U^{-1} совпадает с сопряженным (комплексно-сопряженным от транспонированного) оператором для U , а $I_x^{(\pi)} = I - 2|x\rangle\langle x|$ – оператор, инвертирующий амплитуду в состоянии $|x\rangle$. При $U^{-1} = U = W$ и $|\gamma\rangle = |0\rangle$ этот алгоритм сводится к исходному. Гровер обнаружил следующее свойство:

$$Q \begin{pmatrix} |\gamma\rangle \\ U^{-1}|\tau\rangle \end{pmatrix} = \begin{pmatrix} 1 - 4|U_{\tau\gamma}|^2 & 2U_{\tau\gamma} \\ -2U_{\tau\gamma}^* & 1 \end{pmatrix} \begin{pmatrix} |\gamma\rangle \\ U^{-1}|\tau\rangle \end{pmatrix},$$

где $U_{\tau\gamma} = \langle \tau | U | \gamma \rangle$ и $U_{\tau\gamma}^* = \langle \gamma | U | \tau \rangle$ – оператор, комплексно сопряженный $U_{\tau\gamma}$ (см. выражение (6) в работе [2]). Он интерпретировал это свойство таким образом: оператор Q оставляет инвариантным двумерное векторное пространство, натянутое на векторы $|\gamma\rangle$ и $U^{-1}|\tau\rangle$.

Алгоритм Гровера находит отмеченное состояние $|\tau\rangle$ среди N прочих состояний с помощью метода усиления амплитуды. Начав поиск с исходного базисного состояния $|\gamma\rangle$, алгоритм производит $O(\sqrt{N})$ применений оператора Q , после чего исходное базисное состояние $|\gamma\rangle$ переходит в $U^{-1}|\tau\rangle$. Последующее применение U к $U^{-1}|\tau\rangle$ приводит к отмеченному состоянию $|\tau\rangle$. Чтобы вычислить $Q^k|\gamma\rangle$, необходимо учесть, что Q сохраняет инвариантным двумерное векторное пространство, натянутое на векторы $|\gamma\rangle$ и $U^{-1}|\tau\rangle$. Из этого свойства, например, следует, что $Q|\gamma\rangle = (1 - 4|U_{\tau\gamma}|^2)|\gamma\rangle + 2U_{\tau\gamma}(U^{-1}|\tau\rangle)$. Предположим, что $Q^k|\gamma\rangle = a_k|\gamma\rangle + b_k(U^{-1}|\tau\rangle)$. Тогда можно получить, что $Q^{k+1}|\gamma\rangle = Q(Q^k|\gamma\rangle) = a_k Q|\gamma\rangle + b_k Q(U^{-1}|\tau\rangle)$, если снова учесть то, что оператор Q сохраняет двумерное векторное пространство, натянутое на векторы $|\gamma\rangle$ и $U^{-1}|\tau\rangle$. Это свойство оператора Q обеспечивает успех алгоритма поиска.

В 1999 г. Лонг предложил следующий алгоритм поиска [5]:

$$Q = -I_\gamma U^{-1} I_\tau U, \quad I_\gamma = I - (-e^{i\theta} + 1)|\gamma\rangle\langle\gamma|, \quad I_\tau = I - (-e^{i\phi} + 1)|\tau\rangle\langle\tau|.$$

В случае $\theta = \phi = \pi$, $U^{-1} = U = W$, $|\gamma\rangle = |0\rangle$ этот алгоритм сводится к алгоритму Гровера. Лонг показал, что такой оператор Q также сохраняет векторное пространство, натянутое на векторы $|\gamma\rangle$ и $U^{-1}|\tau\rangle$ (см. формулу (4) работы [5]). В 2000 г. Хойер ввел алгоритм поиска $Q = -AS_0(\phi)A^{-1}S_\chi(\varphi)$ и доказал, что данный оператор Q оставляет инвариантным двумерное векторное пространство, натянутое на векторы $1/\sqrt{a}|\psi_1\rangle$ и $1/\sqrt{b}|\psi_0\rangle$ (см. уравнение (3) в работе [7]).

В работе [6] приведен алгоритм поиска

$$Q = -I_\gamma U^{-1} I_\tau U, \quad I_\gamma = I - 2 \cos \theta e^{i\theta} |\gamma\rangle \langle \gamma|, \quad I_\tau = I - 2 \cos \phi e^{i\phi} |\tau\rangle \langle \tau|,$$

где константы θ и ϕ — вещественные числа. При $\theta = \phi = 0$ этот алгоритм переходит в алгоритм Гровера [2]. Показано, что оператор Q оставляет инвариантным векторное пространство, натянутое на векторы $|\gamma\rangle$ и $U^{-1}|\tau\rangle$:

$$Q \begin{pmatrix} |\gamma\rangle \\ U^{-1}|\tau\rangle \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \lambda & \delta \end{pmatrix} \begin{pmatrix} |\gamma\rangle \\ U^{-1}|\tau\rangle \end{pmatrix},$$

где

$$\begin{aligned} \alpha &= -1 + 2 \cos \theta e^{i\theta} - 4 \cos \theta e^{i\theta} \cos \phi e^{i\phi} |U_{\tau\gamma}|^2, & \beta &= 2U_{\tau\gamma} \cos \phi e^{i\phi}, \\ \lambda &= 2 \cos \theta e^{i\theta} (1 - 2 \cos \phi e^{i\phi}) U_{\tau\gamma}^*, & \delta &= 2 \cos \phi e^{i\phi} - 1. \end{aligned} \quad (1)$$

В этом алгоритме после k применений оператора Q , как только достигнуто состояние $U^{-1}|\tau\rangle$, следующее применение U переводит состояние квантового компьютера в состояние $|\tau\rangle$, т.е. в отмеченное состояние.

В данной работе все рассуждения и вычисления основаны на этом алгоритме. Результаты настоящей работы также остаются справедливыми в рамках алгоритмов Гровера, Хойера, Лонга и др., равно как и для любого алгоритма квантового поиска, у которого имеется инвариантное двумерное векторное пространство, при условии, что результат может зависеть лишь от переменных α , β , λ и δ .

3. ТОЧНАЯ ФОРМУЛА ДЛЯ АМПЛИТУДЫ

Ключевая проблема алгоритма квантового поиска Q состоит в определении амплитуды отмеченного состояния после k применений Q . В этом разделе выводится точная формула для амплитуды в виде функции типа синуса. Пусть $Q|\gamma\rangle = \alpha|\gamma\rangle + \beta(U^{-1}|\tau\rangle)$, $Q(U^{-1}|\tau\rangle) = \lambda|\gamma\rangle + \delta(U^{-1}|\tau\rangle)$ и $Q^k|\gamma\rangle = a_k|\gamma\rangle + b_k(U^{-1}|\tau\rangle)$, где a_k и b_k суть амплитуды в начальном состоянии $|\gamma\rangle$ и в отмеченном состоянии $U^{-1}|\tau\rangle$, соответственно.

В работе [6] показано, что $b_k = \beta r_k$. При $\beta = 0$ ($\cos \phi = 0$) мы получаем $|b_k| = 0$, и квантовый алгоритм становится неприменимым. Поэтому следует предполагать, что $\beta \neq 0$ ($\cos \phi \neq 0$).

3.1. Более простая рекуррентная формула для амплитуды b_k . Рекуррентные формулы для a_k и b_k имеют вид $a_{k+1} = (\alpha a_k + \lambda b_k)$ и $b_{k+1} = (\beta a_k + \delta b_k)$ [6]. Заметим, что рекуррентные формулы для b_{k+1} и a_{k+1} содержат члены a_k и b_k . Можно предложить более простую рекуррентную формулу $b_{k+1} = \beta(\alpha a_{k-1} + \lambda b_{k-1}) + \delta b_k = (\alpha + \delta)b_k + (\beta\lambda - \alpha\delta)b_{k-1}$, которая не содержит члена a_k . Можно также вывести более простую рекуррентную формулу для амплитуды a_k : $a_{k+1} = (\alpha + \delta)a_k + (\beta\lambda - \alpha\delta)a_{k-1}$. При этом $a_k = r_{k+1} - \delta r_k$, так как $b_{k+1} = \beta r_{k+1}$.

Поскольку $b_k = \beta r_k$, β не зависит от k , достаточно вывести точную формулу для r_k в виде функции типа синуса. Выведем сначала рекуррентную формулу для r_k . Вычислив $b_1 = \beta$ и $b_2 = \beta(\alpha + \delta)$, получим $r_1 = 1$, $r_2 = \alpha + \delta$ и $r_{k+1} = (\alpha + \delta)r_k + (\beta\lambda - \alpha\delta)r_{k-1}$. Для алгоритма Гровера $r_1 = 1$, $r_2 = \alpha + 1$ и $r_{k+1} = (\alpha + 1)r_k - r_{k-1}$.

3.2. Выражение для r_k . Очевидно, что $z^2 - (\alpha + \delta)z + (\alpha\delta - \beta\lambda)$ — характеристический многочлен алгоритма Q по отношению к базису. Тогда $\det Q = \alpha\delta - \beta\lambda = \det(-I_\gamma^{(x)} U^{-1} I_\tau^{(y)} U) = e^{i(x+y)}$, где x и y — вещественные углы вращения.

Пусть $r_{k+1} = (z_1 + z_2)r_k - z_1 z_2 r_{k-1}$, где $z_1 + z_2 = \alpha + \delta$, $z_1 z_2 = \alpha\delta - \beta\lambda$, т.е. z_1 и z_2 — собственные значения Q . Тогда $(z_1 - z_2)r_{k+1} = z_1^{k+1} - z_2^{k+1}$. Детали вычисления см. в приложении А. Из результата 6 приложения Б следует, что $z_1 \neq z_2$, если $\cos \phi \neq 0$. Таким образом, $r_{k+1} = (z_1^{k+1} - z_2^{k+1}) / (z_1 - z_2)$.

Пусть $z_1 = \rho_1 e^{i\psi_1}$ и $z_2 = \rho_2 e^{i\psi_2}$, где $\rho_1 > 0$ и $\rho_2 > 0$. Так как $|z_1 z_2| = 1$, имеем $\rho_1 \rho_2 = 1$. Пусть далее $\rho_1 = \rho$. Тогда $\rho_2 = 1/\rho$, $z_1 + z_2 = 2(\cos(\theta - \phi) - 2|U_{\tau\gamma}|^2 \cos \theta \cos \phi) e^{i(\theta + \phi)}$, $(\rho^2 - 1) \sin(\psi_1 - (\theta + \phi)) = 0$. Заметим, что $\psi_1 + \psi_2 = 2(\theta + \phi)$.

Имеют место два случая.

Пусть $\rho \neq 1$. Тогда $\sin(\psi_1 - (\theta + \phi)) = 0$, и потому $\psi_1 = \psi_2$. Пусть $z_1 = \rho e^{i\psi}$. Тогда $z_2 = e^{i\psi}/\rho$, $z_1 + z_2 = (\rho + 1/\rho)e^{i\psi}$, и из результатов 4 и 5 приложения Б следует, что $2 < \rho + 1/\rho = |\alpha + \delta| \leq 2$. Таким образом, условие $\rho \neq 1$ невозможно.

Пусть $\rho = 1$, $z_1 = e^{i\psi_1}$ и $z_2 = e^{i\psi_2}$. Тогда $r_k = \sin(k\Delta) e^{i(k-1)(\theta + \phi)} / \sin \Delta$, где $\Delta = (\psi_1 - \psi_2)/2$. Найдем Δ . Очевидно, что

$$z_1 + z_2 = 2 \cos \frac{\psi_1 - \psi_2}{2} e^{i(\psi_1 + \psi_2)/2}.$$

Пусть $p = |U_{\tau\gamma}|$. Тогда $\Delta = \arccos(\cos(\theta - \phi) - 2p^2 \cos \theta \cos \phi) = \arccos(e^{-i(\theta + \phi)} \text{tr } Q)$, где $\text{tr } Q$ — след матрицы Q (см. результат 2 приложения Б). Так как $\cos \phi \neq 0$, можно заключить, что $\psi_1 \neq \psi_2$. Без потери общности положим $\psi_1 > \psi_2$. Тогда

$$\sin \Delta = \sqrt{1 - \frac{|\alpha + \delta|^2}{4}} = \sqrt{1 - (\cos(\theta - \phi) - 2p^2 \cos \theta \cos \phi)^2} > 0.$$

3.3. Точная формула для амплитуды b_k . Очевидно, что $b_k = \beta r_k = 2p \cos \phi e^{i((k-1)(\theta + \phi) + \phi)} \sin(k\Delta) / \sin \Delta$, и при каждом применении алгоритма Гровера фаза амплитуды отмеченного состояния растет как $(\theta + \phi)$. Тогда из приведенного выше выражения для Δ имеем $|b_k| = |\beta| |\sin(k\Delta)| / \sin \Delta$, где $|\beta| = 2p |\cos \phi|$.

ЗАМЕЧАНИЕ 1. Формула для b_k справедлива для алгоритмов Гровера, Лонга и др. и Хойера, равно как и для любого другого алгоритма квантового поиска, сохраняющего двумерное векторное пространство.

Выражение для b_k можно упростить при совпадающих углах вращения и в случае алгоритма Гровера. Пусть $\theta = \phi$, тогда $|b_k| = |\beta| |\sin(k\Delta)| / \sin \Delta$, где

$$\Delta = \frac{\psi_1 - \psi_2}{2}, \quad \psi_1 - \psi_2 = \arccos\{2(1 - 2p^2 \cos^2 \phi)^2 - 1\},$$

$$\sin \Delta = 2p |\cos \phi| \sqrt{1 - p^2 \cos^2 \phi}.$$

В работе [5] с применением многочисленных преобразований была выведена аппроксимирующая формула для амплитуды в отмеченном состоянии.

Рассмотрим алгоритм Гровера $Q = -I_\gamma^{(\pi)} U^{-1} I_\tau^{(\pi)} U$. В этом случае легко видеть, что $\alpha = 1 - 4|U_{\tau\gamma}|^2$, $\beta = 2U_{\tau\gamma}$, $\lambda = -2U_{\tau\gamma}^*$ и $\delta = 1$. Характеристическое уравнение из п. 3.2 принимает вид $z^2 - (\alpha + 1)z + 1 = 0$. Положим корни характеристического многочлена равными $z_1 = e^{i\xi}$ и $z_2 = e^{-i\xi}$. Тогда

$$\cos \xi = 1 - 2p^2, \quad z_1^k - z_2^k = 2i \sin(k\xi), \quad r_k = \frac{\sin(k\xi)}{\sin \xi},$$

что также можно было бы получить с помощью формул п. 3.2, положив $\psi_1 = \xi$ и $\psi_2 = -\xi$. Окончательно получим, что

$$b_k = \beta \frac{\sin(k\xi)}{\sin \xi}, \quad |b_k| = 2p \frac{|\sin(k\xi)|}{|\sin \xi|}.$$

4. НЕОБХОДИМОЕ И ДОСТАТОЧНОЕ ФАЗОВОЕ УСЛОВИЕ

Выведем необходимое и достаточное фазовое условие, которое следует наложить на произвольные фазовые вращения, чтобы достичь отмеченного состояния с вероятностью единица.

4.1. Необходимое и достаточное фазовое условие $\sin \Delta \leq |\beta|$.

ТЕОРЕМА. Алгоритм достоверно находит отмеченное состояние, т.е. существует число шагов k такое, что $|b_k| = 1$, тогда и только тогда, когда

$$\sin \Delta = \sqrt{1 - \frac{|\alpha + \delta|^2}{4}} = \sqrt{1 - (\cos(\theta - \phi) - 2p^2 \cos \theta \cos \phi)^2} \leq |\beta|.$$

ДОКАЗАТЕЛЬСТВО. Если $b_k = 1$, т.е. $|b_k| = |\beta| |\sin(k\Delta)| / \sin \Delta = 1$ для некоторого k , то $|\sin(k\Delta)| = \sin \Delta / |\beta|$. Очевидно, что $\sin \Delta / |\beta| \leq 1$. Таким образом, $\sin \Delta \leq |\beta|$. Пусть k_o – оптимальное число шагов итераций, необходимое для достоверного нахождения отмеченного состояния. Тогда

$$k_o = \frac{1}{\Delta} \arcsin \frac{\sin \Delta}{|\beta|}, \quad (2)$$

при этом $|b_{k_o}| = 1$.

Обратно, если $\sin \Delta \leq |\beta|$ и k_o имеет вид (2), то $|b_{k_o}| = |\beta| |\sin k_o \Delta| / \sin \Delta = 1$. Доказательство завершено.

Фазовое условие можно также представить в виде $2\sqrt{1 - |\beta|^2} \leq |\operatorname{tr} Q|$. Оно выполнено для алгоритмов Лонга и др., для алгоритма Хойера, равно как и для любого другого алгоритма квантового поиска, сохраняющего двумерное векторное пространство.

Из общего фазового условия вытекают два следствия, доказательства которых приведены в приложении В. Эти следствия удобны для проверки того, удовлетворяет ли алгоритм фазовому условию. Напомним, что $p = |U_{\tau\gamma}|$.

СЛЕДСТВИЕ 1. Пусть $p < 1/2$, а углы θ и ϕ либо лежат в одном и том же квадранте, либо удовлетворяют условиям $|\theta - \phi| < \pi/2$ и $\cos \theta \cos \phi < 0$. Тогда $\sin \Delta \leq |\beta|$, и алгоритм достоверно находит отмеченное состояние тогда и только тогда, когда

$$|\theta - \phi| \leq \arccos(2p^2 \cos \theta \cos \phi + \sqrt{1 - 4p^2 \cos^2 \phi}).$$

СЛЕДСТВИЕ 2. Пусть θ и ϕ или лежат в одном и том же квадранте, или выполнены условия $\cos \theta \cos \phi < 0$ и $\sin \theta \sin \phi < 0$. Тогда $\sin \Delta > |\beta|$, и алгоритм непригоден для достоверного нахождения отмеченного состояния при $|\sin(\theta - \phi)| > |\beta|$.

4.2. Оптимальное число шагов итерационной схемы. При совпадающих углах вращения $\theta = \phi$ можно уменьшить оптимальное число k_o шагов итерационной схемы. В этом случае

$$k_o = \frac{\arcsin \sqrt{1 - p^2 \cos^2 \phi}}{\arcsin(2p |\cos \phi| \sqrt{1 - p^2 \cos^2 \phi})}.$$

Пусть $p \cos \phi = \sin \xi$. Тогда $k_o = (\pi - 2\xi)/4\xi = \pi/4\xi - 1/2$. При $\phi = 0$ имеем $p = \sin \xi$, и k_o есть оптимальное число шагов итераций для алгоритма Гровера, полученное в работе [2]. Более того, пусть $p = \sqrt{1/N}$. Тогда $k_o = (\pi - 2\theta)/4\theta$ задает оптимальное число шагов итераций в исходном алгоритме Гровера при $\sin^2 \theta = 1/N$ [4]. Авторы работы [5] получили формулы для аппроксимаций оптимального числа итераций при совпадающих углах вращений. Они полагали, что $U_{\tau\gamma} = e^{i\xi} \sin \beta$. Тогда $\sin \beta = p$, что также отличается от $\sin \xi = p \cos \phi$.

Пусть $p = 1/\sqrt{N}$, где $N = 2^{10}$. Точные значения для оптимального числа шагов итераций собраны в таблице. Для первоначального алгоритма Гровера оптимальное число шагов итераций равно 24.625.

ϕ	$4\pi/9$	$5\pi/12$	$\pi/3$	$\pi/4$	$\pi/5$	$\pi/6$	$\pi/8$	$\pi/10$	$\pi/15$
k_o	144.21	96.590	49.763	35.037	30.561	28.516	26.699	25.922	25.515

ЗАМЕЧАНИЕ 2. Если выполнено фазовое условие $\sin \Delta \leq |\beta|$, то оптимальное число итераций, необходимое для достоверного нахождения отмеченного состояния, задается формулой (2). С учетом фазового условия получим, что $0 < k_o \Delta = \arcsin(\sin \Delta / |\beta|) \leq \pi/2$. Таким образом, при $0 < k \Delta \leq k_o \Delta \leq \pi/2$ имеем $|\sin(k \Delta)| = \sin(k \Delta)$ и $|b_k| = |\beta| \sin(k \Delta) / \sin \Delta$. Отсюда можно заключить, что величина $|b_k|$, рассматриваемая как функция от k , строго монотонно возрастает с ростом k от 0 до k_o .

5. УСЛОВИЕ СОВПАДЕНИЯ УГЛОВ ВРАЩЕНИЯ НЕ ЯВЛЯЕТСЯ НЕОБХОДИМЫМ

В этом разделе мы покажем, что условие совпадения углов вращения $\theta = \phi$ достаточно, но не необходимо для достоверного нахождения отмеченного состояния.

5.1. Условие совпадения углов вращения достаточно. При условии $\theta = \phi$ имеем $\sin \Delta = 2p |\cos \phi| \sqrt{1 - p^2 \cos^2 \phi}$, следовательно, $\sin \Delta / |\beta| = \sqrt{1 - p^2 \cos^2 \phi} \leq 1$. Таким образом, при $\theta = \phi$ из фазового условия из раздела 4 следует, что квантовый алгоритм Q должен достоверно находить отмеченное состояние во всех случаях, кроме $I_\gamma = I_\tau = I$.

5.2. Условие совпадения углов вращения не необходимо. Предъявим примеры, показывающие, что условие $\theta = \phi$ не необходимо, и можно выбирать несовпадающие углы вращения для достоверного нахождения отмеченного состояния, если только эти углы удовлетворяют фазовому условию из раздела 4.

ПРИМЕР 1. Пусть $\phi = 0$. Тогда $\sin \Delta \leq |\beta|$, и алгоритм достоверно находит отмеченное состояние тогда и только тогда, когда $|\sin \theta| \leq 2p^2 / |1 - 2p^2|$.

В самом деле, фазовое условие при $\phi = 0$ дает

$$\frac{\sin \Delta}{|\beta|} = \frac{\sqrt{1 - (1 - 2p^2)^2 \cos^2 \theta}}{2p} \leq 1,$$

что эквивалентно $|\sin \theta| \leq 2p^2 / |1 - 2p^2|$.

Например, при $p = 0.5$, $\phi = 0$ и $\theta = \pi/3$ имеем $\sin \pi/3 < 2p^2 / |1 - 2p^2| = 1$, и фазовое условие при этом выполнено. В этом случае $k_o = 1$.

ПРИМЕР 2. Предположим, что $\theta = 0$. Тогда легко показать, что $\sin \Delta \leq |\beta|$ тогда и только тогда, когда $\cos^2 \phi \geq 1/(1 + 4p^4)$.

Примеры 1 и 2 показывают, что условие совпадения углов вращения $\theta = \phi$ не является необходимым для достоверного нахождения отмеченного состояния, тем не менее представляет собой важный случай фазового условия.

ПРИЛОЖЕНИЕ А

Отталкиваясь от рекуррентных соотношений $r_{k+1} = (\alpha + \delta)r_k + (\beta\lambda - \alpha\delta)r_{k-1}$, можно вывести точную формулу для b_k в виде функции типа синуса. Пусть

$$r_{k+1} = (z_1 + z_2)r_k - z_1 z_2 r_{k-1}, \quad (3)$$

где $z_1 + z_2 = \alpha + \delta$ и $z_1 z_2 = -(\beta\lambda - \alpha\delta)$. Заметим, что $r_1 = 1$ и $r_2 = \alpha + \delta = z_1 + z_2$. Тогда $r_{k+1} = z_1 r_k + z_2 r_k - z_1 z_2 r_{k-1}$, и имеют место равенства

$$r_{k+1} - z_1 r_k = z_2 r_k - z_1 z_2 r_{k-1} = z_2 (r_k - z_1 r_{k-1}), \quad (4)$$

$$r_{k+1} - z_2 r_k = z_1 r_k - z_1 z_2 r_{k-1} = z_1 (r_k - z_2 r_{k-1}). \quad (5)$$

Учитывая (4), получим

$$r_{k+1} - z_1 r_k = z_2 (r_k - z_1 r_{k-1}) = z_2^2 (r_{k-1} - z_1 r_{k-2}) = \cdots = z_2^{k-1} (r_2 - z_1 r_1),$$

таким образом,

$$r_{k+1} - z_1 r_k = z_2^{k-1} (r_2 - z_1 r_1). \quad (6)$$

Аналогично, учитывая (5), получим

$$r_{k+1} - z_2 r_k = z_1^{k-1} (r_2 - z_2 r_1). \quad (7)$$

Отсюда

$$\begin{aligned} z_1 r_{k+1} - z_2 r_{k+1} &= z_1^k (r_2 - z_2 r_1) - z_2^k (r_2 - z_1 r_1) = \\ &= z_1^k (z_1 + z_2 - z_2) - z_2^k (z_1 + z_2 - z_1) = z_1^{k+1} - z_2^{k+1}. \end{aligned}$$

Заметим, что $r_2 = z_1 + z_2$ и $r_1 = 1$.

Из результата 6 приложения Б получим, что $z_1 \neq z_2$, если только $\cos \phi \neq 0$, и таким образом $r_{k+1} = (z_1^{k+1} - z_2^{k+1}) / (z_1 - z_2)$.

ПРИЛОЖЕНИЕ Б

Здесь собрано несколько результатов. Во-первых, величины α , β , λ и δ в формулах (1) можно представить в виде

$$\begin{aligned}\alpha &= e^{i2\theta} - (e^{i2\theta} + 1)(e^{i2\phi} + 1)|U_{\tau\gamma}|^2, & \beta &= (e^{i2\phi} + 1)U_{\tau\gamma}, \\ \lambda &= -e^{i2\phi}(e^{i2\theta} + 1)U_{\tau\gamma}^*, & \delta &= e^{i2\phi}.\end{aligned}$$

Тогда

$$\begin{aligned}\beta\lambda &= -e^{i2\phi}(e^{i2\phi} + 1)(e^{i2\theta} + 1)|U_{\tau\gamma}|^2, \\ \alpha\delta &= e^{i2\phi}(e^{i2\theta} - (e^{i2\theta} + 1)(e^{i2\phi} + 1)|U_{\tau\gamma}|^2),\end{aligned}$$

откуда следует

РЕЗУЛЬТАТ 1. $\alpha\delta - \beta\lambda = e^{i2(\theta+\phi)}$. (Напомним, что $p = |U_{\tau\gamma}|$.)

РЕЗУЛЬТАТ 2.

$$\begin{aligned}\alpha + \beta &= e^{i2\theta} + e^{i2\phi} - 4\cos\theta\cos\phi e^{i(\theta+\phi)}p^2 = \\ &= 2(\cos(\theta - \phi) - 2p^2\cos\theta\cos\phi)e^{i(\theta+\phi)} = \\ &= 2((1 - 2p^2)\cos\theta\cos\phi + \sin\theta\sin\phi)e^{i(\theta+\phi)}.\end{aligned}$$

РЕЗУЛЬТАТ 3. $|\cos(\theta - \phi) - 2p^2\cos\theta\cos\phi| \leq 1$, и равенство имеет место тогда и только тогда, когда $\cos\theta = \cos\phi = 0$.

ДОКАЗАТЕЛЬСТВО. Заметим, что $\cos(\theta - \phi) - 2p^2\cos\theta\cos\phi = (1 - 2p^2)\cos\theta\cos\phi + \sin\theta\sin\phi$, и $|1 - 2p^2| < 1$, если только $0 < p < 1$. Если $\cos\theta\cos\phi = 0$, то очевидно, что $|(1 - 2p^2)\cos\theta\cos\phi + \sin\theta\sin\phi| \leq 1$. Докажем, что $|(1 - 2p^2)\cos\theta\cos\phi + \sin\theta\sin\phi| < 1$ если только $\cos\theta\cos\phi \neq 0$. Имеются несколько случаев.

СЛУЧАЙ 1.1. Пусть $\cos\theta\cos\phi > 0$, $0 < p < \sqrt{2}/2$. Тогда

$$\begin{aligned}0 &< 1 - 2p^2 < 1, & 0 &< (1 - 2p^2)\cos\theta\cos\phi < \cos\theta\cos\phi, \\ \sin\theta\sin\phi &< (1 - 2p^2)\cos\theta\cos\phi + \sin\theta\sin\phi < \cos(\theta - \phi) \leq 1.\end{aligned}$$

Таким образом, $|(1 - 2p^2)\cos\theta\cos\phi + \sin\theta\sin\phi| < 1$.

СЛУЧАЙ 1.2. Пусть $\cos\theta\cos\phi > 0$, $\sqrt{2}/2 \leq p < 1$. Тогда

$$\begin{aligned}-1 &< 1 - 2p^2 \leq 0, & -\cos\theta\cos\phi &< (1 - 2p^2)\cos\theta\cos\phi \leq 0, \\ -\cos(\theta + \phi) &< (1 - 2p^2)\cos\theta\cos\phi + \sin\theta\sin\phi \leq \sin\theta\sin\phi.\end{aligned}$$

При этом $|(1 - 2p^2)\cos\theta\cos\phi + \sin\theta\sin\phi| < 1$.

СЛУЧАЙ 2.1. Пусть $\cos \theta \cos \phi < 0$, $0 < p < \sqrt{2}/2$. Тогда

$$\begin{aligned} 0 < 1 - 2p^2 < 1, \quad \cos \theta \cos \phi < (1 - 2p^2) \cos \theta \cos \phi < 0, \\ \cos(\theta - \phi) < (1 - 2p^2) \cos \theta \cos \phi + \sin \theta \sin \phi < \sin \theta \sin \phi. \end{aligned}$$

Также получим, что $|(1 - 2p^2) \cos \theta \cos \phi + \sin \theta \sin \phi| < 1$.

СЛУЧАЙ 2.2. Пусть $\sqrt{\cos \theta \cos \phi} < 0$, $\sqrt{2}/2 \leq p < 1$. Тогда

$$\begin{aligned} -1 < 1 - 2p^2 \leq 0, \quad 0 \leq (1 - 2p^2) \cos \theta \cos \phi < -\cos \theta \cos \phi, \\ \sin \theta \sin \phi \leq (1 - 2p^2) \cos \theta \cos \phi + \sin \theta \sin \phi < -\cos(\theta + \phi). \end{aligned}$$

И в этом случае $|(1 - 2p^2) \cos \theta \cos \phi + \sin \theta \sin \phi| < 1$.

Итак, если $\cos \theta \cos \phi \neq 0$, то $|(1 - 2p^2) \cos \theta \cos \phi + \sin \theta \sin \phi| < 1$.

Докажем теперь вторую часть утверждения. Если $|(1 - 2p^2) \cos \theta \cos \phi + \sin \theta \sin \phi| = 1$, то $\cos \theta \cos \phi = 0$ и $|\sin \theta \sin \phi| = 1$. Тогда $|\sin \theta| = |\sin \phi| = 1$, следовательно, $\cos \theta = \cos \phi = 0$.

Обратно, если $\cos \theta = \cos \phi = 0$, то $|\sin \theta| = |\sin \phi| = 1$ и $|(1 - 2p^2) \cos \theta \cos \phi + \sin \theta \sin \phi| = 1$. Доказательство завершено.

РЕЗУЛЬТАТ 4. $|\alpha + \beta| = 2|\cos(\theta - \phi) - 2p^2 \cos \theta \cos \phi| \leq 2$, что тривиально следует из результатов 2 и 3.

РЕЗУЛЬТАТ 5. Предположим, что $\rho > 0$. Тогда $\rho + 1/\rho \geq 2$, и равенство имеет место тогда, и только тогда, когда $\rho = 1$.

РЕЗУЛЬТАТ 6. Пусть $z_1 + z_2 = \alpha + \beta$, $z_1 z_2 = \alpha \delta - \beta \lambda$. Тогда $z_1 \neq z_2$, если $\beta \neq 0$ ($\cos \phi \neq 0$).

ДОКАЗАТЕЛЬСТВО. Предположим, что $z_1 = z_2$ и $z_1 = z_2 = \rho e^{i\psi}$. Поскольку $|z_1 z_2| = 1$, получим, что $\rho = 1$, $|\alpha + \beta| = 2$, т.е. $|\cos(\theta - \phi) - 2p^2 \cos \theta \cos \phi| = 1$. Из результата 3 приложения Б получаем, что $\cos \theta = \cos \phi = 0$. Это противоречит условию $\cos \phi \neq 0$.

ПРИЛОЖЕНИЕ В

ДОКАЗАТЕЛЬСТВО СЛЕДСТВИЯ 1. Если θ и ϕ лежат в одном и том же квадранте, то

$$\cos(\theta - \phi) - 2p^2 \cos \theta \cos \phi = (1 - 2p^2) \cos \theta \cos \phi + \sin \theta \sin \phi > 0.$$

Если $|\theta - \phi| < \pi/2$, $\cos \theta \cos \phi < 0$, то $\cos(\theta - \phi) > 0$ и $\cos(\theta - \phi) - 2p^2 \cos \theta \cos \phi > 0$.

Необходимость. Если $\sin \Delta \leq |\beta|$, то

$$\sqrt{1 - (\cos(\theta - \phi) - 2p^2 \cos \theta \cos \phi)^2} \leq |\beta|, \quad 1 - 4p^2 \cos^2 \phi \leq (\cos(\theta - \phi) - 2p^2 \cos \theta \cos \phi)^2.$$

При наложенных условиях

$$\sqrt{1 - 4p^2 \cos^2 \phi} \leq |\cos(\theta - \phi) - 2p^2 \cos \theta \cos \phi| = \cos(\theta - \phi) - 2p^2 \cos \theta \cos \phi.$$

Таким образом, $|\theta - \phi| \leq \arccos(2p^2 \cos \theta \cos \phi + \sqrt{1 - 4p^2 \cos^2 \phi})$.

Достаточность. Очевидно, что $\cos(\theta - \phi) \geq \sqrt{1 - 4p^2 \cos^2 \phi} + 2p^2 \cos \theta \cos \phi$. Если $\cos(\theta - \phi) - 2p^2 \cos \theta \cos \phi > 0$, то из результата 3 приложения Б следует, что $4p^2 \cos^2 \phi \geq 1 - (\cos(\theta - \phi) - 2p^2 \cos \theta \cos \phi)^2 \geq 0$. Таким образом, $\sin \Delta \leq |\beta|$. Доказательство завершено.

В работе [6] показано, что если $|\theta - \phi| < |\beta|$, то алгоритм Q находит отмеченное состояние с вероятностью единица. Это утверждение есть аппроксимация первого порядка для фазового условия. Ниже мы приведем анализ случая $|\theta - \phi| > |\beta|$.

ДОКАЗАТЕЛЬСТВО СЛЕДСТВИЯ 2. Заметим, что если θ и ϕ лежат в одном и том же квадранте, то имеют место соотношения

$$\begin{aligned} 1 - (\cos(\theta - \phi) - 2p^2 \cos \theta \cos \phi)^2 &= \\ &= \sin^2(\theta - \phi) + 4p^2 \cos \theta \cos \phi ((1 - p^2) \cos \theta \cos \phi + \sin \theta \sin \phi) > \sin^2(\theta - \phi), \end{aligned}$$

выполненные при условиях следствия. Таким образом, если $|\sin(\theta - \phi)| > |\beta|$, то $\sin \Delta > |\beta|$. Доказательство завершено.

Благодарности. Авторы благодарны Ченг Гуо за полезные обсуждения способов построения более простых формул для амплитуд. Работа была частично финансово поддержана NSFC, грант № 60433050, Основным Исследовательским Фондом Университета г. Цингуа (КНР), грант № JC2003043, и Главной Государственной Лабораторией Интеллектуальных Технологий и Систем.

Список литературы

- [1] P. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In: Proc. of the 35th Annual Symposium on Foundation of Computer Science (Santa Fe, New Mexico, 20–22 November, 1994). IEEE Computer Society Press: Los Alamos, CA, 1994. P. 124.
- [2] L. K. Grover. Phys. Rev. Lett. 1998. V. 80. P. 4329.
- [3] L. K. Grover. Phys. Rev. Lett. 1997. V. 79. P. 325.
- [4] M. Boyer, G. Brassard, P. Høyer, A. Tapp. Fortsch. Phys. 1998. V. 46. P. 493.
- [5] G. L. Long, Y. S. Li, W. L. Zhang, Li Niu. Phys. Lett. A. 1999. V. 262. P. 27.
- [6] Dafa Li, Xinxin Li. Phys. Lett. A. 2001. V. 287. P. 304; quant-ph/0105035.
- [7] P. Høyer. Phys. Rev. A. 2000. V. 62. P. 052304.
- [8] G. L. Long Y. S. Li, W. L. Zhang, C. C. Tu. Phys. Rev. A. 2000. V. 61. P. 042305; G. L. Long. Phys. Rev. A. 2001. V. 64. P. 022307.
- [9] E. Biham, O. Biham, D. Biron et al. Phys. Rev. A. 2000. V. 63. P. 012310.
- [10] Dafa Li, Xinxin Li, H. Huang, Xiangrong Li. Phys. Rev. A. 2002. V. 66. P. 044304.

Поступила в редакцию 26.X.2003 г.,
после доработки 4.III.2005 г.