Математика и ее приложения : ЖИМО. 2013. Вып. 1 (10). С. 13–18

УДК 512.543

Е. А. Ноговицын[1], А. Л. Колесников[2]

О возможности применения квантового алгоритма Шора к задаче разбиения файла на буферы

Ключевые слова: булево сжатие, квантовый алгоритм Шора, нахождение периода.

В настоящей работе мы рассматриваем квантовый алгоритм решения задачи нахождения порядка (периода случайной функции), которая имеет экспонентоциальную сложность при решении на классических компьютерах. Обсуждается возможность применения квантового алгоритма Шора к решению задачи разбиения файла на буферы.

Keywords: boolean compress, quantum algorithm, order finding.

In this article we show how the quantum algorithm enables us to efficiently solve a number theoretical problem of order finding, which is considered hard on classical computers. A possibility to use the Shor's quantum algorithm to the file decomposition into buffers is discussed.

1. Введение

Квантовые алгоритмы открывают возможности решения задач, которые являются непомерно сложными для классических компьютеров [1]. К таким задачам относится задача разбиения файла на буферы. Если файл разбит на N кортежей длиной n бит каждый, то существует $2^N - 1$ объединений этих кортежей в буферы, которые содержат от 1 до L файлов, где $L = 1, 2..., N$ [2]. О возможности применения применения квантового алгоритма Гровера [3, 4] и соответствии между разбиением файла на буферы и заполнением регистра квантового компьютера указывалось в работе [5]. Но поскольку алгоритм Гровера не изменяет экспонентоциальной сложности задачи, в настоящей работе рассматривается квантовый алгоритм Шора, изначально разработанный для задачи факторизации чисел

[1]Ивановский государственный университет; E-mail: nea282006@yandex.ru

[2]Ивановский государственный университет; E-mail: bancocker@mail.ru. Работа выполнена при финансовой поддержке РФФИ (проект 13-07-00628)

и имеющий полиномиальную сложность[6, 7, 1]. Ключевой процедурой в задаче факторизации является процедура нахождение периода функции на целых числах, значения которой внутри периода случайны. П. Шор разработал алгоритм, позволяющий узнать период (порядок x по модулю N) с вероятность близкой к единице за время, которое растет с ростом n как n^3 для n-значного числа [7].

2. Задача о нахождении порядка

2.1. Арифметические операции по модулю N. Арифметика по модулю основана на единственности представления

$$x = k \cdot N + r,$$

где x и N положительные целые числа, k неотрицательное целое, а $0 \leq r \leq N$. Принята следующая форма записи

$$x = r \;\; mod \; N.$$

Например, $2 = 5 = 8 = 11 \;\; mod \; 3$.

Наибольший общий делитель $gcd(ab)$ двух целых чисел a и b есть наибольшее целое, на которое a и b делятся без остатка. Если $gcd(ab) = 1$, то a и b *взаимно простые* числа. Произведение по модулю N определяется как массив целых чисел

$$m_k = k \cdot a \;\; mod \; N, \quad 0 \leq k \leq N.$$

Например, если $a = 6$ и $N = 15$, то $gcd(aN) = 3$ и

$$m_k = \{6; 12; 3; 9; 0; 6; 12; 3; 9; 0; 6; 12; 3; 9\}.$$

При этом, уравнение $x \cdot 6 = y \;\; mod \; 15$ не имеет решения для $y \subset \{1; 2; 4; 5; 7; 8; 10; 11\}$. Можно определить обратный элемент a^{-1} к a по модулю N:

$$a^{-1} \cdot a = 1 \;\; mod \; N,$$

если a и N - взаимно простые.

Рассмотрим уравнение

$$x^r = 1 \;\; mod \;\; N,$$

которое имеет решение для целых взаимно прстых чисел x и N и $x < N$. Наименьшее целое положительное r, при котором это уравнение выполняется, называется порядком x по модулю N.

Не существует классического алгоритма, который бы решал задачу нахождения порядка за полиномиальное число шагов $O(L)$, где $L = logN$ число бит необходимых для задания N.

2.2. Квантовое преобразование Фуре и оценка фазы. В основе квантового алгоритма Шора для нахождения порядка числа по модулю лежит квантовое преобразование Фурье. Квартовое преобразование Фурье - это аналог дискретного преобразования Фурье, областью значений которого являются равномерно распределенные на интервале $[0, 2\pi)$ точки $2\pi k/N$ для некоторого N. Масштабируя область определения на $\frac{N}{2\pi}$, получаем область значений от нуля до $N-1$. Квантовое преобразование Фурье является унитарным преобразованием:

$$|j\rangle \to \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle, \tag{1}$$

или

$$\sum_{j=0}^{N-1} x_j |j\rangle \to \sum_{k=0}^{N-1} y_k |k\rangle. \tag{2}$$

Преобразование Фурье лежит в основе процедуры, известной как *оценка фазы* [1], которая применяется во многих квантовых алгоритмах. Пусть у унитарного оператора U есть собственный вектор $|u\rangle$ с собственным значением $e^{2\pi i\phi}$, где фаза ϕ неизвестна. Цель алгоритма оценки фазы состоит в том, чтобы оценить ϕ. Чтобы выполнить оценку, предполагается, что имеются доступные черные ящики (оракулы), способные подготовить состояние $|u\rangle$ и совершить U^{2j} операции, для неотрицательных целых чисел j. Использование черных оракулов предполагает, что процедура оценки фазы не является полным квантовым алгоритмом, а, своего рода, подпрограмма или модуль, который объединен с другими подпрограммами и используется для решения вычислительной задачи. Квантовая процедура оценки фазы использует два регистра. Первый регистр содержит t кубит в начальном состоянии $|0\rangle$. Выбор t зависит от точности и вероятности, с которой мы желаем иметь оценку для ϕ. Второй регистр содержит состояние $|u\rangle$, и содержит столько кубит, сколько необходимо для хранения $|u\rangle$. Оценка фазы выполняется в два этапа. Первый регистр преобразуется к конечному состоянию

$$\frac{1}{2^{t/2}}\left(|0\rangle+e^{2\pi i 2^{t-1}\phi}|1\rangle\right)+\left(|0\rangle+e^{2\pi i 2^{t-2}\phi}|1\rangle\right)+... \tag{3}$$

$$+\left(|0\rangle+e^{2\pi i 2^{0}\phi}|1\rangle\right)=\frac{1}{2^{t/2}}\sum_{k=0}^{2^{t-1}}e^{2\pi i\phi k}|k\rangle. \tag{4}$$

Второй этап оценки фазы состоит применении обратного квантового преобразования Фурье. Алгоритм оценки фазы позволяет оценить фазу ϕ собственного значения унитарного оператора U, действующего на соответствующий собственный вектор $|u\rangle$. Существенная особенность процедуры заключается в возможности с помощью обратного преобразования Фурье выполнить преобразование

$$\frac{1}{2^{t/2}}\sum_{j=0}^{2^{t-1}}e^{2\pi i\phi j}|j\rangle|u\rangle\to|\tilde{\phi}\rangle|u\rangle, \tag{5}$$

где $\tilde{\phi}$ - состояние с хорошо определенной фазой.

2.3. Квантовый алгоритм Шора. Определим L-кубитный унитарный оператор [1]

$$U|y\rangle\equiv\begin{cases}|x\cdot y \quad mod\ N\rangle, & 0\le y\le N-1\\ |y\rangle, & N\le y\le 2^L-1\end{cases}. \tag{6}$$

Состояние

$$|u_s\rangle=\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-i2\pi sk}{r}\right]|x^k \quad mod\ N\rangle, \tag{7}$$

определенное для целых $0\le s\le r-1$, является собственным вектором оператора U, так как

$$U|u_s\rangle=\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-i2\pi sk}{r}\right]|x^{k+1} \quad mod\ N\rangle= \tag{8}$$

$$=\frac{1}{\sqrt{r}}\sum_{k=1}^{r}\exp\left[\frac{-i2\pi s(k-1)}{r}\right]|x^k \quad mod\ N\rangle=\exp\left[\frac{i2\pi s}{r}\right]|u_s\rangle, \tag{9}$$

поскольку $x^r=x^0\ mod\ N$ и $\exp\left[\frac{-i2\pi s(r-1)}{r}\right]=\exp\left[\frac{i2\pi s}{r}\right]$. Теперь, применяя алгоритм для оценки фазы [1], можно с достаточной надежностью определить отношение s/r.

Чтобы получить достаточную точность при оценке фазы, необходимо использовать $t = 2L+1+[\log(2+1/2\varepsilon)]$ кубит в первом регистре, и приготовить второй регистр в состоянии $|1\rangle$. Тогда мы будем получать значение фазы $\phi = s/r$ для случайных $0 \le s \le r$ с вероятностью, по крайней мере, $1-\varepsilon$. Зная, что фаза $\phi = s/r$ есть рациональное число, где s и r целые числа не больше L бит, можно классически определить s и r при использовании $O(L^3)$ гейт.

3. Нахождение порядка и сжатие информации

Рассмотрим пример. Пусть $x = 5$ и $N = 21$. Тогда

$$m_k = \{5; 4; 20; 16; 17; 1; 5; 4; 20; 16; 17; 1; 5; 4; 20; 16; 17; 1; 5; 4\}\,.$$

Порядок x по модулю N в этом случае равен $r = 6$. Алгоритм Шора позволяет определить порядок числа по модулю за полиномиальное число шагов. Зная порядок, мы знаем количество повторяющихся чисел, которые могут быть объединены в буферы с соответствующими значениями r. Т. е. в различные буферы можно объединять различные периоды, а в кодирующее уравнение должен входить параметр количества повторений периода. Каждому буферу ставится в соответствие булев полином и кодирующее уравнение [2, 5].

Ясно, что алгоритм Шора не решает задачу разбиения файла на буферы. Необходимо установить соответствие между разбиением файла на буферы и регистрами квантового компьютера. Квантовый регистр – это упорядоченное множество кубитов. Один из способов отображения разбиения файла на квантовый регистр был предложен в работе [5].

Список литературы

1. *Nielsen M.A., Chuang I. L.* Quantum Computation and Quantum Information 10th Anniversary Edition. Cambridge University Press : The Edinburgh Building, Cambridge CB2 8RU, UK. 2010. 670 p.

2. *Толстопятов А. А.* Возможные подходы к разбиению файла на буферы при булевом сжатии // Математика и ее приложения: журн. Иван. мат. о-ва. 2009. Вып. 1(6). С. 129–138.

3. *Grover L.* A fast quantum mechanical algorithm for data base search // STOC'28. 1996. P. 212–219.

4. *Grover L.* Quantum mechanics helps in searching for a needle in a haystack // Phys. Rev. Lett. 1997. Vol. 79 (2). P. 325. (arXive e-print quant-ph/9706033).

5. *Толстопятов А. А.* Квантовыйалгоритм разбиения файла на буферы // Математика и ее приложения: журн. Иван. мат. о-ва. 2011. Вып. 1(8). С. 113–120.

6. *Shor P. W.* Algorithm for Quantum Computation: Discrete log and Factoring // FOCS'35. 1994. P. 124.

7. *Shor P. W.* Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM J. Comp. 1997. Vol. 26 (5). P. 1484–1509.

Поступила в редакцию 26.11.2013.