- унификация операционных систем основных серверов ЛВС на базе Debian Linux (используемой в настоящий момент в ЛВС БрГТУ на серверах, обеспечивающих VPN-доступ, веб-хостинг и HTTP-proxy) с сохранением ОС Windows для аутентификации ключей аппаратной защиты приложений в виде физических или виртуальных серверов (при успешном эксперименте по работе виртуализованных серверов аутентификации прикладных программ — формирование централизованного сервера аутентификации программ с аппаратными ключами);
- установка первичного контроллера сети Microsoft для аутентификации пользователей на рабочих станциях и, возможно, роуминга пользовательских профилей (рабочих столов); установка резервного контроллера на случай отключения первичного контроллера;
- Использование отдельного сервера аутентификации пользователей на базе протокола LDAP для хранения учетных записей; репликация базы на два сервера с автоматическим перенаправлением (балансировкой) трафика для обеспечения высокой надежности (high-availability cluster) и, возможно, использованием протокола Kerberos для безопасной аутентификации;
- Замена почтового сервера MDaemon на решение на базе Debian Linux + Postfix (либо аналогичный почтовый сервер) для использования единого сервера аутентификации и базы пользователей. Перенастройка аутентификации на proxy-сервере для аналогичных целей.
- Установка репозитория обновлений пакетов на одном из серверов сети с установленным ftp-протоколом для оперативного устранения уязвимостей в программном обеспечении.

К преимуществам данного решения относится использование единой программной платформы для обеспечения унифицированного администрирования серверов. Необходимо отметить также преимущество использования открытых стандартов, которые могут быть реализованы на серверных платформах как GNU/Linux, так и Microsoft Windows (протоколы SMB и LDAP), что позволяет при необходимости произвести перевод серверных операционных систем с одной операционной системы на другую без изменения инфраструктуры ЛВС и настроек рабочих станций. Причиной такого перевода может быть изменившийся уровень квалификации обслуживающего персонала, а также вопросы лицензирования программного обеспечения (в отличие от решений на базе Debian Linux, не требующих оплаты, серверные операционные системы Microsoft требуют материальных вложений для покупки лицензий).

Среди недостатков можно упомянуть более сложную процедуру настройки рабочей станции для функционирования в составе домена сети Microsoft (необходимость точного соответствия адреса и имени машины, сохраненных в базе данных сервера, индивидуализированному дисковому образу машины). Проблема хранения множественных образов может решаться применением одной из программных систем инкрементных образов с дедупликацией данных.

Дополнительно в связке с данным решением может использоваться продукт Novell ZENworks (поставляемый отдельно от серверных операционных систем Novell) для сохранения прежней системы сетевой загрузки приложений.

Перечисленные действия по реструктуризации ЛВС подразделяются на незначительные изменения, которые в целом не представляют угрозы для штатного функционирования ЛВС, и на кардинальные перемены, проведение которых требует особого внимания для исключения нарушения работоспособности ЛВС на стадии фактического отключения изношенного оборудования и замены серверных платформ. Подготовка таких этапов реструктуризации может выполняться без нарушения нормальной работы предприятия, однако предпочтительным временем выполнения фактической замены является период, следующий за окончанием производственного процесса (учебного процесса университета).

Авторы выражают благодарность сотрудникам Информационно-технического центра БрГТУ за продуктивное обсуждение решений и технологий в процессе подготовки статьи

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Таненбаум, Э. Компьютерные сети. – СПб.: Питер, 2008. – 992 с.
2. Сиян, К. TCP/IP. Для профессионалов / К. Сиян, Т. Паркер – СПб.: Питер, 2004. – 864 с.
3. Таненбаум, Э. Современные операционные системы. – СПб.: Питер, 2010. – 1120 с.
4. Крэйг, З. Планирование и поддержка сетевой инфраструктуры Microsoft Windows Server 2003. Учебный курс MSCE. – М.: Русская редакция, 2005. – 544 с.
5. Terpstra, J.H. The Official Samba-3 HOWTO and Reference Guide / J.H. Terpstra, J.R. Vernooij – N.J.: Prentice Hall PTR, 2005. – 944 p.

Материал поступил в редакцию 07.12.10

POITA P.S., DRAGAN V.I., DUNETS A.P., KOSTIUK D.A., HVEDCHUK V.I., DERECHENNIK S.S. Modernization approach for heterogeneous network infrastructure by example of the university information computer network

Factors that are accumulating at exploitation of complex local area network (LAN) and causing the restructuring necessity are investigated. Specialties of organization and necessary changes are inspected at levels of users services, backbone network and routing, using the university network as a model of complex heterogeneous LAN. Three strategies are formulated, providing the maximal simplicity of support, the minimal changes, or the minimal limitations of the functionality. A set of actions is proposed for each strategy for the example of the university LAN.

УДК 530.145

Гердт В.П., Прокопеня А.Н.

МОДЕЛИРОВАНИЕ КВАНТОВОГО АЛГОРИТМА НАХОЖДЕНИЯ ПОКАЗАТЕЛЯ ЦЕЛОГО ЧИСЛА НА ОСНОВЕ ПАКЕТА *QUANTUMCIRCUIT*

Введение. Резкое возрастание научно-технического интереса к квантовым вычислениям и квантовой информатике [1, 2], начавшееся в середине 90-х годов прошлого века, продолжается и по настоящее время, о чем свидетельствует неуклонный рост числа публикаций, посвященных различным аспектам данной тематики. Одной из основных причин этого является потенциальная способность квантового компьютера решать некоторые вычислительные задачи значительно эффективнее любого классического компьютера. Наиболее выразительными и интересными, с прикладной точки зрения, примерами таких задач является поиск записи в неупорядоченной базе данных, эффективно решаемый квантовым алгоритмом Гровера [3], и факторизация целого числа, эффективно выполняемая квантовым

Гердт Владимир Петрович, *профессор, д.ф.-м.н., начальник сектора алгебраических и квантовых вычислений Лаборатории информационных технологий Объединенного института ядерных исследований.*
Россия, 141980, Московская обл., г. Дубна, ул. Жолио-Кюри, 6.
Прокопеня Александр Николаевич, *доцент, д.ф.-м.н., проф. кафедры физики Брестского государственного технического университета.*
Беларусь, БрГТУ, 224017, г. Брест, ул. Московская, 267.

алгоритмом Шора [4]. Кроме того, имеются косвенные указания на прогресс в практической реализации квантовых вычислений [5], хотя говорить о создании реалистичного квантового компьютера еще слишком рано. В этой связи возникает особый интерес к созданию симуляторов квантовых вычислений на классических компьютерах, которые позволяли бы, с одной стороны, лучше понять алгоритмические аспекты работы квантового компьютера, а с другой стороны, могли использоваться для разработки и тестирования новых эффективных квантовых алгоритмов.

В работах [6, 7] представлено описание пакета “QuantumCircuit”, написанного на языке системы Mathematica [8], который имеет удобный пользовательский интерфейс и является универсальным в том смысле, что позволяет моделировать произвольный квантовый алгоритм. С его помощью можно легко спроектировать квантовую схему, визуализировать ее, а также вычислить соответствующую ей унитарную матрицу, которая позволяет найти конечное состояние квантового регистра памяти по заданному начальному состоянию и определить вероятность получения требуемого результата. В качестве примера в работе [9] выполнено моделирование квантового алгоритма поиска Гровера [3] и показано, что этот алгоритм дает квадратичное ускорение решения задачи поиска. В данной работе производится подробный анализ квантового алгоритма нахождения показателя (мультипликативного порядка) простого целого числа по модулю другого простого целого числа и проверка его работы на конкретном примере, позволяющем выяснить основные особенности и проблемы квантовых вычислений. В качестве программного средства для моделирования используется пакет “QuantumCircuit” и система Mathematica.

Квантовые вычисления на основе квантовых схем. Среди нескольких моделей квантовых вычислений (см. [1]) наиболее простой в теоретическом плане является модель квантовых схем, в рамках которой квантовые вычисления выполняются подобно вычислениям на классическом компьютере. Имеется квантовый регистр памяти, в котором хранятся входные данные и промежуточные результаты вычислений, реализованный в виде набора квантовых битов или кубитов. Каждый кубит представляет собой квантовую систему, которая имеет два различных состояния, условно обозначаемых $|0\rangle$ и $|1\rangle$, где символ $|a\rangle$ соответствует стандартному обозначению состояний в квантовой механике. В отличие от классического бита, который может находиться только в одном из фиксированных состояний 0 или 1, кубит как квантовая система может находиться в произвольной суперпозиции состояний

$$|a\rangle = \alpha|0\rangle + \beta|1\rangle,$$

где комплексные числа α и β должны удовлетворять условию нормировки $|\alpha|^2 + |\beta|^2 = 1$, а квадраты их модулей $|\alpha|^2$, $|\beta|^2$ определяют вероятности получить значения 0 и 1 соответственно при измерении кубита. Таким образом, в общем случае состояние кубита представляет собой вектор в двумерном комплексном пространстве, в котором состояния $|0\rangle$ и $|1\rangle$ образуют ортонормированный базис и называются состояниями вычислительного базиса. Соответственно, состояние регистра памяти, содержащего n кубитов, определяется вектором в многомерном комплексном пространстве, базисные векторы которого определяются соотношением

$$|a_{n-1}\rangle \otimes |a_{n-2}\rangle \otimes \cdots \otimes |a_0\rangle \equiv \equiv |a_{n-1}\rangle |a_{n-2}\rangle \ldots |a_0\rangle \equiv |a_{n-1}a_{n-2}\ldots a_0\rangle, \quad (1)$$

где $a_j = 0,\ 1\ (j = 0,1,\ldots,n-1)$, а символ $\otimes$ обозначает тензорное произведение векторов $|a_j\rangle$. Так как любая комбинация нулей и единиц вида $(a_{n-1}a_{n-2}\ldots a_0)$ соответствует двоичному представлению некоторого n–битового числа k из диапазона $0 \le k < 2^n$, для базисных векторов (1) обычно используют более короткую форму записи $|k\rangle_n$, где индекс n определяет число кубитов в регистре. Используя для базисных состояний кубита $|0\rangle$ и $|1\rangle$ стандартное векторное представление

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

и определение (1), произвольный базисный вектор $|k\rangle_n$ можно представить в виде столбца, у которого $(k+1)$-ая компонента равна 1, а все остальные компоненты равны нулю:

$$|0\rangle_n = \begin{pmatrix}1\\0\\0\\\vdots\\0\end{pmatrix},\ |1\rangle_n = \begin{pmatrix}0\\1\\0\\\vdots\\0\end{pmatrix},\ \ldots,\ |2^n-1\rangle_n = \begin{pmatrix}0\\0\\\vdots\\0\\1\end{pmatrix}. \quad (3)$$

Таким образом, состояние регистра памяти, содержащего n кубитов, представляет собой вектор в 2^n-мерном комплексном пространстве, который можно представить в виде суперпозиции базисных векторов (1) или (3). В общем случае соответствующее выражение содержит 2^n комплексных чисел, значения которых ограничены только одним условием – условием нормировки. Следовательно, объем памяти, требуемый для записи этих чисел, растет экспоненциально с ростом числа кубитов, что накладывает естественные ограничения на возможность моделирования квантовых вычислений с помощью классического компьютера.

При использовании модели квантовых схем предполагается, что квантовый регистр памяти можно приготовить в требуемом начальном состоянии, а затем преобразовать так, чтобы после измерения конечного состояния кубитов получить желаемый результат с высокой вероятностью. При этом преобразования или вычисления, как и в случае классических вычислений, можно реализовать в виде последовательности квантовых логических элементов - вентилей, действующих на отдельные кубиты или группы кубитов, и изобразить в виде диаграммы, которая и называется квантовой схемой. В качестве примера на рис. 1 показана квантовая схема на трех кубитах. Исходное состояние регистра памяти изображается в виде столбца

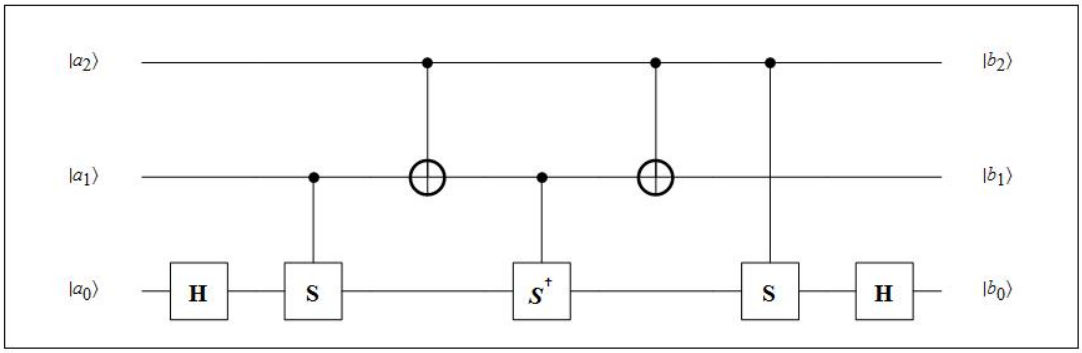

Рис. 1. Пример квантовой схемы на трех кубитах

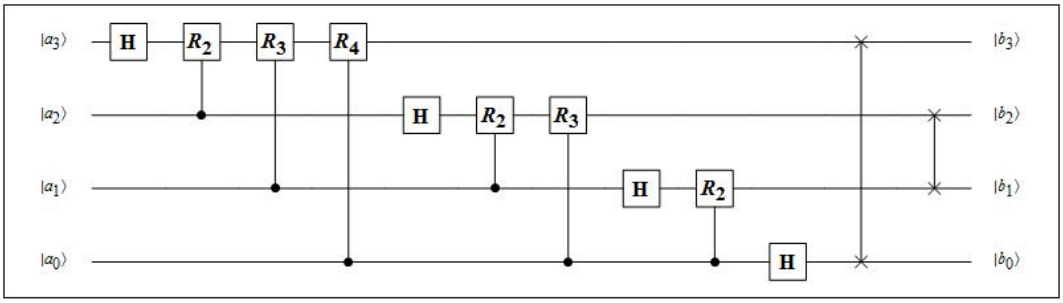

Рис. 2. Четырехкубитное квантовое преобразование Фурье

кубитов $|a_2\rangle$, $|a_1\rangle$, $|a_0\rangle$ в левой части диаграммы. Перемещение слева направо вдоль линий, идущих от кубитов, отображает их эволюцию во времени и взаимодействие друг с другом посредством однокубитных и многокубитных вентилей, для которых используются стандартные обозначения (см., например, [1]). В результате регистр памяти переводится в некоторое конечное состояние, изображаемое столбцом $|b_2\rangle$, $|b_1\rangle$, $|b_0\rangle$ в правой части схемы, которое может быть измерено. Поскольку изменение состояния любой квантовой системы во времени определяется соответствующим унитарным оператором эволюции, а состояние регистра памяти описывается вектором в 2^n-мерном комплексном пространстве, каждой квантовой схеме можно сопоставить унитарную $2^n \times 2^n$ матрицу, которая и выполняет преобразование исходного состояния регистра в конечное. Таким образом, основной задачей классического симулятора квантовых вычислений является определение $2^n \times 2^n$ унитарной матрицы, соответствующей квантовой схеме на n кубитах, и предсказание вероятностей различных конечных состояний регистра памяти по заданному начальному состоянию. Заметим, что пакет "QuantumCircuit" позволяет успешно решать такую задачу для произвольной квантовой схемы, конечно, с учетом ограничений на имеющиеся ресурсы компьютера.

Квантовое преобразование Фурье. Квантовое преобразование Фурье является основой многих интересных и эффективных квантовых алгоритмов [1, 2]. В ортонормированном базисе (3) это преобразование определяется как линейный оператор U_{FT}, действующий на базисные состояния по формуле:

$$U_{FT}\,|\,x\rangle_n = \frac{1}{2^n}\sum_{y=0}^{2^n-1}\exp\left(2\pi i\frac{xy}{2^n}\right)|\,y\rangle_n . \qquad (4)$$

Для преобразования (4) существует квантовая схема, которая эффективно его вычисляет. В состав такой схемы входят квантовые вентили только трех типов, а именно, вентиль Адамара (H), управляемый вентиль фазового сдвига (R_k) и вентиль SWAP, осуществляющий обмен состояний двух кубитов. В качестве примера на рис. 2 показана квантовая схема для вычисления преобразования Фурье на четырех кубитах. При увеличении числа кубитов n общая структура схемы сохраняется, а число логических элементов, необходимых для реализации алгоритма, возрастает как $O(n^2)$. Заметим, однако, что лучшие известные классические алгоритмы для вычисления дискретного преобразования Фурье 2^n-компонентного вектора, такие как быстрое преобразование Фурье (FFT), используют $O(n\cdot 2^n)$ элементов (см. [1]). Таким образом, для выполнения преобразования Фурье на классическом компьютере требуется экспоненциально больше операций, чем для решения той же задачи на квантовом компьютере. Естественно, при моделировании квантового преобразования Фурье на классическом компьютере время вычислений также растет экспоненциально с ростом числа кубитов независимо от вида симулятора. Например, для вычисления унитарной матрицы размерности 1024×1024, соответствующей квантовому преобразованию Фурье на десяти кубитах, с помощью пакета "QuantumCircuit", установленному на персональном компьютере с оперативной памятью 4 GB и двухядерным процессором с тактовой частотой 2 GHz, требуется около 70 секунд. При этом добавление одного кубита приводит к возрастанию времени вычислений примерно в 4 раза.

Квантовый алгоритм нахождения показателя. Рассмотрим два взаимно простых целых числа b и N_0, причем $b < N_0$. Напомним, что показателем числа b по модулю N_0 называется наименьшее положительное целое число r, удовлетворяющее равенству

$$b^r \pmod{N_0} = 1. \qquad (5)$$

Задача нахождения показателя состоит в отыскании числа r для заданных чисел b и N_0. Считается, что это очень трудная задача для классического компьютера в том смысле, что неизвестен решающий ее алгоритм, количество операций которого растет полиномиально с ростом n_0, где n_0 – число битов, необходимое для записи числа N_0.

Заметим, что функция $f(x) = b^x \pmod{N_0}$ является периодической, причем ее период равен показателю r. В этой связи может показаться, что задача отыскания периода функции не является трудной. Однако функция $f(x)$ определена только для целых чисел, причем ее значения на отрезке $x \in [0,\ r]$ изменяются довольно хаотично. Поэтому из значения функции в произвольной точке x нельзя извлечь никакой информации об ее возможном значении в точке $(x+1)$. На рис. 3 приведен пример такой функции, который показывает, что даже оценить значение периода по графику крайне трудно, хотя он равен 993. Если же речь идет о числах b и N_0, содержащих сто или двести цифр, то задача отыскания периода становится не решаемой на любом классическом компьютере, так как время расчетов превышает всякие разумные пределы.

В 1994 г. П. Шор предложил эффективный квантовый алгоритм (см. [4]) нахождения показателя, число операций которого растет как $O(n^2 \log n \log\log n)$, где n – число кубитов. Поскольку многие практически важные алгоритмы базируются на алгоритме Шора, рассмотрим его подробнее, используя в качестве средства для моделирования пакет "QuantumCircuit". Пусть имеется два регистра памяти, первый из которых содержит n кубитов и называется входным регистром, а второй содержит n_0 кубитов и называется выходным регистром. Входной регистр используется для записи аргумента x функции $f(x) = b^x \pmod{N_0}$, а выходной – для записи значений этой функции. Размер n_0 выходного регистра равняется числу бит, которое требуется для задания числа N_0, поскольку значения функции $f(x)$ не превышают $(N_0 - 1)$. Число кубитов n входного регистра должно быть по крайней мере в два раза больше n_0, чтобы точность вычисления периода r была достаточно высокой (см. [2]). В исходном состоянии кубиты входного регистра установлены в состояние $|\,0\rangle$, а кубиты выходного регистра – в состояние $|\,1\rangle$. Следует отметить, что для вычисления значений функции

$f(x) = b^x \pmod{N_0}$ имеется эффективный квантовый алгоритм (см. [1]), который мы здесь обсуждать не будем, а соответствующий модуль на квантовой схеме обозначим через управляемый элемент U_f (рис. 4).

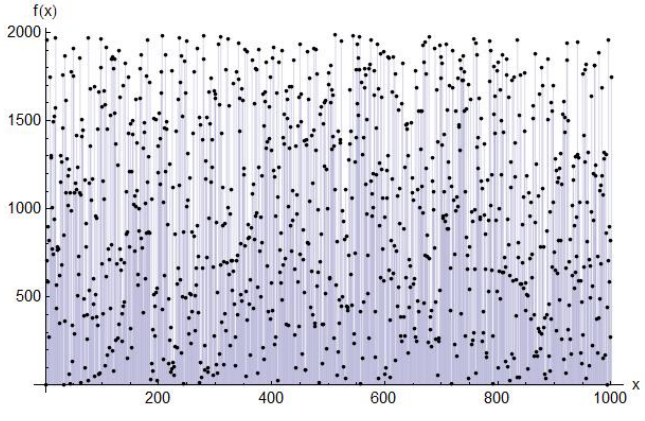

Рис. 3. Значения функции $f(x) = 709^x \pmod{1987}$

Одной из важных особенностей квантового компьютера является возможность приведения его регистра памяти в состояние, которое представляет собой суперпозицию всех состояний вычислительного базиса (3) с одинаковыми коэффициентами. Для этого достаточно к каждому кубиту регистра, находящегося в состоянии $|0\rangle$, применить вентиль Адамара. На схеме, изображенной на рис. 4, соответствующая операция, обозначенная символом $H^{\otimes n}$, применяется к входному регистру и переводит его в состояние

$$|0\rangle_n \to \frac{1}{2^{n/2}} \sum_{j=0}^{2^{n/2}-1} |j\rangle_n . \qquad (6)$$

Таким образом, на вход модуля управляемый-U_f, который производит вычисление функции $f(x) = b^x \pmod{N_0}$, поступают все возможные значения аргумента *x* одновременно. Получаемое в результате квантовое состояние регистров содержит информацию обо всех возможных значениях функции $f(x)$ и определяется формулой

$$|0\rangle_n |1\rangle_{n_0} \to \frac{1}{2^{n/2}} \sum_{j=0}^{2^{n/2}-1} |j\rangle_n |1\rangle_{n_0} \to \frac{1}{2^{n/2}} \sum_{j=0}^{2^{n/2}-1} |j\rangle_n |f(j)\rangle_{n_0} =$$

$$= \frac{1}{2^{n/2}} \sum_{j=0}^{2^{n/2}-1} |j\rangle_n |b^j \mod N_0\rangle_{n_0} \qquad (7)$$

Такая возможность вычисления всех значений функции за одно обращение к соответствующей процедуре U_f носит название квантового параллелизма и является одним из источников вычислительной мощи квантового компьютера.

Заметим, что коэффициенты при всех состояниях в правой части суммы (7) одинаковы. Следовательно, при измерении состояния $|y\rangle_n$ входного регистра с равными вероятностями мы получим одно из целых чисел *j* из интервала $[0,\ 2^n - 1]$. Однако состояния входного и выходного регистров после обращения к процедуре U_f оказываются связанными. В соответствии с правилом Борна в процессе измерений входного регистра выходной регистр перейдет в соответствующее состояние $|b^j \mod N_0\rangle_{n_0}$, и последующее его измерение даст число $(b^j \mod N_0)$ с вероятностью 1. При этом информация о значениях функции $f(x)$ при других значениях аргумента будет утеряна, и определить период функции не удастся.

Если начать измерения с выходного регистра, то получается одно из возможных значений функции $f(x) = b^x \pmod{N_0}$, например, f_0. Так как эта функция является периодической с периодом *r*, то на интервале $[0,\ 2^n - 1]$ имеется несколько целых чисел *x*, при которых функция принимает то же самое значение f_0. Обозначая через x_0 наименьшее из этих чисел $(0 \le x_0 < r)$, а через m – наименьшее целое число, удовлетворяющее неравенству $x_0 + mr \ge 2^n$, легко видеть, что $m = \left[\frac{2^n}{r}\right]$ или $m = \left[\frac{2^n}{r}\right] + 1$ в зависимости от значения x_0, где $[a]$ обозначает целую часть числа a. В результате регистры перейдут в квантовое состояние

$$\frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + kr\rangle_n |f(x_0)\rangle_{n_0} . \qquad (8)$$

Это состояние содержит информацию о периоде *r* функции $f(x)$, но измерение входного регистра даст с равными вероятностями только одно их чисел вида $x_0 + kr$, что также недостаточно для определения периода, так как все три параметра x_0, k и r являются неизвестными. При повторении вычислений мы опять получим состояние вида (8), но с другим значением x_0, так как вероятность получения того же самого f_0 при измерении выходного регистра очень мала.

Чтобы избежать зависимости результата измерений от значения x_0, применим к входному регистру, находящемуся в состоянии (8), квантовое преобразование Фурье (4), а затем произведем измерение. Таким образом, полная квантовая схема, реализующая квантовый алгоритм нахождения порядка, примет вид, изображенный на рис. 5. Заметим, что после измерения выходного регистра его состояние $|f_0\rangle$ остается неизменным, поэтому далее рассмотрим только состояние входного регистра.

В результате применения квантового преобразования Фурье состояние входного регистра принимает вид:

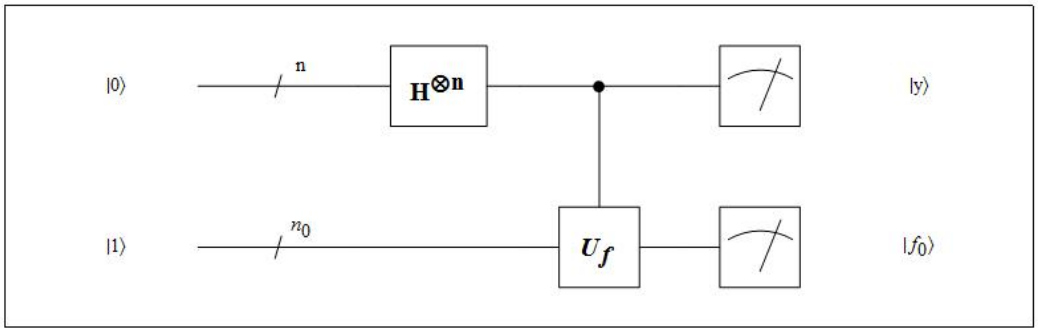

Рис. 4. Квантовая схема вычисления функции $f(x) = b^x \pmod{N_0}$

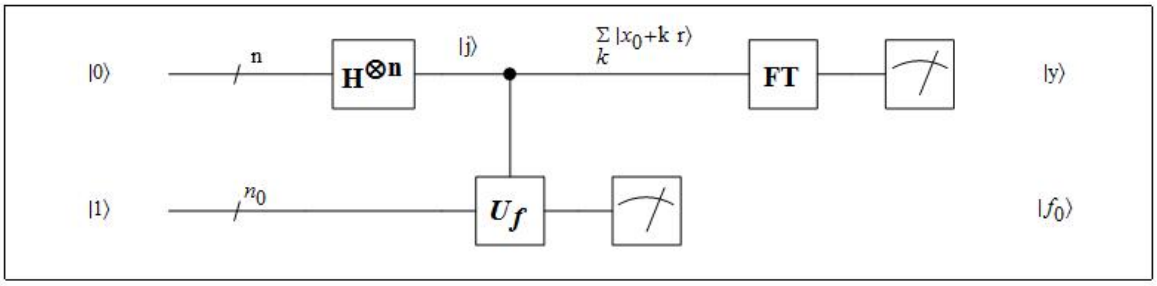

Рис. 5. Квантовая схема для алгоритма нахождения порядка

$$\frac{1}{\sqrt{m}}\sum_{k=0}^{m-1}|\,x_0+kr\rangle_n \to \frac{1}{\sqrt{m}}\sum_{k=0}^{m-1}\frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}\exp\left(2\pi i\frac{(x_0+kr)y}{2^n}\right)|\,y\rangle_n =$$

$$=\sum_{y=0}^{2^n-1}\exp\left(2\pi i\frac{x_0 y}{2^n}\right)\left[\frac{1}{2^{n/2}\sqrt{m}}\sum_{k=0}^{m-1}\exp\left(2\pi i\frac{kry}{2^n}\right)\right]|\,y\rangle_n . \quad (9)$$

Как видим, число x_0 содержится только в фазовом множителе в правой части (9) и не влияет на результат измерений, поскольку модуль экспоненты от чисто мнимого аргумента равен 1. Вероятность же получить произвольное значение y из интервала $[0,\ 2^n-1]$ в результате измерения входного регистра равняется квадрату модуля соответствующего множителя при $|\,y\rangle_n$, заключенного в квадратные скобки в правой части (9), и может быть представлена в виде

$$p(y)=\frac{1}{2^n m}\left|\sum_{k=0}^{m-1}\exp\left(2\pi i\frac{kry}{2^n}\right)\right|^2=\frac{1}{2^n m}\frac{\sin^2\left(\frac{\pi ym}{2^n/r}\right)}{\sin^2\left(\frac{\pi y}{2^n/r}\right)}. \quad (10)$$

Если искомый период можно представить в виде $r=2^l$, где l – целое число, то $m=[2^n/r]=2^{n-l}$ и формула (10) принимает вид

$$p(y)=\frac{1}{2^n m}\left|\sum_{k=0}^{m-1}\exp\left(2\pi i\frac{kry}{2^n}\right)\right|^2=\frac{1}{r}\delta_{y,2^{n-l}j},$$

$$(j=0,1,\ldots,r-1)$$

Следовательно, в результате измерений входного регистра с равной вероятностью будет получено одно их чисел $y=2^{n-l}j=\frac{2^n}{r}j$.

Тогда $r=\frac{2^n}{y}j$ и, проверяя выполнение условия $b^r\ (\mathrm{mod}N_0)=1$ при различных значениях j с помощью обычного компьютера можно легко найти период r. Однако вероятность того, что период имеет вид $r=2^l$, крайне мала и обычно отношение $2^n/r$ оказывается рациональным числом.

Анализ функции, стоящей в правой части выражения для вероятности (10), показывает, что при выполнении условия $r<<2^n$, которое достигается путем увеличения числа кубитов во входном регистре по сравнению с заданным числом кубитов n_0 в выходном регистре, эта функция будет принимать максимальные значения при

$$y=y_j=\left[\frac{2^n}{r}\right]j,\ (j=0,1,\ldots,r-1). \quad (11)$$

Поэтому измерение входного регистра приведет к одному из значений (11) с высокой вероятностью. Тогда, вычисляя отношение $y_j/2^n$, получим аппроксимацию рационального числа j/r с точностью, определяемой неравенством

$$\left|\frac{y_j}{2^n}-\frac{j}{r}\right|=\frac{j}{r}\left|\frac{[2^n/r]}{2^n/r}-1\right|\le\frac{j}{r}\frac{1/2}{2^n/r}=\frac{j}{2^{n+1}}<\frac{r}{2^{n+1}}. \quad (12)$$

Поскольку период функции $f(x)=b^x\ (\mathrm{mod}\ N_0)$ при заданных числах b и N_0 фиксирован, то увеличение числа кубитов n во входном регистре позволяет найти рациональной число j/r с высокой точностью, а его знаменатель и равняется искомому периоду.

В качестве примера рассмотрим случай $N_0=13$, $b=7$. Для записи числа N_0 достаточно 4 бита, т.е. $n_0=4$. Пусть входной регистр содержит $n=10$ кубитов. Так как период r не может превышать N_0, то согласно (12) отношение $y_j/2^n$ аппроксимирует рациональное число j/r с точностью $\frac{r}{2^{n+1}}\sim\frac{2^{n_0}}{2^{n+1}}=\frac{1}{2^7}\approx 0{,}01$. Для моделирования квантового алгоритма нахождения порядка вычисляем значения функции $f(x)=b^x\ (\mathrm{mod}\ N_0)$ для всех целых $x\in[0,\ 2^n-1]$, а затем выбираем случайным образом одно из значений, моделируя процесс измерения выходного регистра. Получаем, например, $f_0=9$, причем на интервале $[0,\ 2^n-1]$ имеется $m=85$ значений числа x, для которых функция $f(x)$ принимает одно и то же значение f_0. Следовательно, состояние регистров (8) содержит суперпозицию из 85 базисных состояний (3), которая легко находится. Далее, используя пакет “QuantumCircuit”, вычисляем унитарную матрицу, выполняющую квантовое преобразование Фурье на 10 кубитах и с ее помощью переводим найденное состояние (8) в конечное состояние (9). Вычисляя квадраты модулей коэффициентов при $|\,y\rangle_n$ в (9), находим вероятности получения различных значений y при измерении входного регистра (рис. 6).

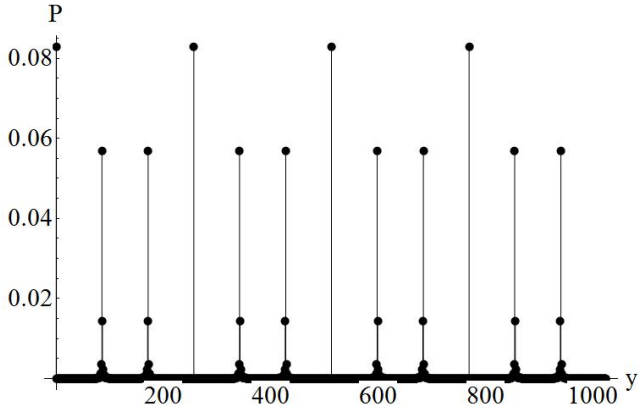

Рис. 6. Распределение вероятностей, определяемых функцией (10)

Как видим, максимальной вероятности $p=0{,}083$ соответствуют четыре числа: 0, 256, 512 и 768. Предположим, что в результа-

те измерения входного регистра мы получили одно из них, например, $y = 256$. Тогда $j/r = [y/2^n] = 256/1024 = 1/4$, что означает, что искомый период является целым кратным 4. Простая проверка показывает, что искомый период равняется 12, т.е. $7^{12} (\mathrm{mod} 13) = 1$.

Заметим, что имеется еще ряд значений *y*, например, 85, 171, 341, 427, 597, 683, 853, 939, вероятность получения которых в результате измерений входного регистра $p = 0{,}057$, т.е. достаточно высока. Пусть, например, мы получили число $y = 597$. Тогда с точностью до 0,01 (см. (12)) находим рациональное число $j/r = [y/2^n] = 7/12$, знаменатель которого сразу дает искомый период. Оставшиеся семь значений *y*, приведенных выше, дают то же значение периода *r*.

Аналогичным образом убеждаемся в том, что еще 8 значений *y*, а именно: 86, 170, 342, 426, 598, 682, 854, 938, каждое из которых может быть получено с вероятностью $p = 0{,}014$, также приводят к периоду $r = 12$. Таким образом, суммарная вероятность получить одно из приведенных выше 20 чисел и найти правильное значение периода *r* превышает 0,9, т.е. очень высока, даже если исключить число $y = 0$, получение которого в результате измерений не приводит к нахождению периода. В случае $y = 0$, а также при получении в результате измерений других значений *y*, вероятность чего мала, вычисления следует повторить.

Заключение. В данной работе подробно проанализирован квантовый алгоритм нахождения показателя простого целого числа по модулю другого простого числа и продемонстрирована его работа на конкретном примере. Показано, что однократная реализация этого алгоритма позволяет найти показатель с достаточно большой вероятностью, хотя и не равной 1. В этом существенное отличие квантового компьютера от классического, который всегда получает однозначный результат, причем его правильность определяется только корректностью алгоритма. В случае квантового компьютера возможны разные результаты вычислений, и алгоритм считается хорошим, если искомый результат находится, возможно, путем многократной работы алгоритма, с любой достаточно высокой вероятностью. Очевидно, возможность получения решения задачи, которая не может быть решена с помощью классического компьютера, но может быть решена, с высокой вероятностью правильного результата, на квантовом компьютере является хорошим стимулом к дальнейшему исследованию квантовых вычислений и практическим попыткам создания такого компьютера.

Исследования, представленные в этой работе, выполнены при поддержке гранта РФФИ № 10-01-00200.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Нильсен, М. Квантовые вычисления и квантовая информация: Пер. с англ. / М. Нильсен, И. Чанг. – М.: Мир, 2006. – 824 с.
2. Mermin, N.D. Quantum computer science. An introduction / N.D. Mermin. – Cambridge University Press, 2007. – 220 p.
3. Grover, L.K. Quantum mechanics helps in searching for a needle in a haystack / L.K. Grover // Physical Review Letters. – 1997. – Vol. 79. – P. 325–328.
4. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer / P.W. Shor // SIAM J. of Computations – 1997. – Vol. 26, No. 5. – P. 1484–1509.
5. World's first 28-qubit quantum computer demonstrated online at Supercomputing 2007 conference [Electronic resource]. – D-Wave Systems, Inc., 2007. – Mode of access: http://www.nanotechwire.com/news.asp?nid=5254. – Date of access: 13.11.2007.
6. Gerdt, V.P. A Mathematica package for construction of circuit matrices in quantum computation / V.P. Gerdt, R. Kragler, A.N. Prokopenya // Acta Academiae Aboensis. Seb. B. – 2007. – Vol. 67, No. 2. – P. 28–38.
7. Gerdt, V.P. Some algorithms for calculating unitary matrices for quantum circuits / V.P. Gerdt, A.N. Prokopenya // Programming and computer software. – 2010. – Vol. 36, No. 2. – P. 111–116.
8. Wolfram, S. The Mathematica book / S. Wolfram. – 4th ed. – Wolfram Media/Cambridge University Press, 1999. – 1470 p.
9. Gerdt, V.P. A Mathematica package for simulation of quantum computation / V.P. Gerdt, R. Kragler, A.N. Prokopenya // Lecture notes in computer science. – 2009. – Vol. 5743. – P. 106–117.

Материал поступил в редакцию 25.11.10

GERDT V.P., PROKOPENYA A.N. Simulation of the quantum algorithm for order finding with the *QuantumCircuit* package

Quantum algorithm for order finding is discussed in detail and its application to a concrete example is demonstrated. It has been shown that one can find a period with high enough probability after only one run of the algorithm. All calculations are done with the system Mathematica and the package QuantumCircuit designed on its basis.

УДК 621.315.592

Кушнер Т.Л., Янусик И.С.

ФОТОЭЛЕКТРИЧЕСКИЕ СВОЙСТВА ПОВЕРХНОСТНО-БАРЬЕРНЫХ СТРУКТУР $In/CuIn_3Se_5$, $In/CuGa_3Se_5$, $In/CuGa_5Se_8$

Введение. Фоторезистивные эффект – свойство полупроводника измененять электрическое сопротивление, обусловленное исключительно действием оптического излучения и не связанное с его нагреванием, является на сегодняшний момент хорошо изученным физическим явлением. Зависимость фотопроводимости ряда полупроводников от освещенности используется в фоторезисторах, получивших широкое практическое применение. Для возникновения фоторезистивного эффекта необходимо, чтобы в полупроводнике происходило либо собственное поглощение оптического излучения или фотонов с образованием новых пар носителей заряда, либо примесное поглощение с образованием носителей одного знака при возбуждении однотипных дефектов. В результате увеличения концентрации носителей заряда уменьшается сопротивление полупроводника. Таким образом, установились два самостоятельных понятия: собственная и примесная фотопроводимость.

Наиболее чувствительные фоторезисторы изготавливают из сернистого кадмия (CdS), у которого фотопроводимость в 10^5–10^6 раз превышает темновую проводимость. Широкое распространение получили фоторезисторы из сернистого свинца (PbS), чувствительного к далекой инфракрасной области спектра. Используются и другие полу-

***Кушнер Татьяна Леонидовна**, к.ф.-м.н., доцент, декан факультета довузовской подготовки Брестского государственного технического университета.*

***Янусик Ирина Семёновна,** старший преподаватель кафедры физики Брестского государственного технического университета.*
Беларусь, БрГТУ, 224017, г. Брест, ул. Московская, 267.