УДК 681.3.06:530.145.001.57

В.Ф. Гузик, С.М. Гушанский, О.К. Евсеев

СПОСОБ ОРГАНИЗАЦИИ ВЕТВЛЕНИЯ В КВАНТОВЫХ ВЫЧИСЛЕНИЯХ

Использование квантовых вычислителей позволяет решать задачи экспоненциального класса сложности такие, как факторизация целых чисел, поиск в неупорядоченных массивах данных и моделирование свойств объектов наномира за полиномиальное (относительно сложности задачи) количество времени. Ни одна из последовательных и даже параллельных или кластерных вычислительных систем по своей природе не может обладать такой эффективностью.

Главным отличием квантового вычислителя является по сути алгоритмическая организация квантовой вычислительной системы на основе бит квантового регистра и культивация её состояний до получения решения задачи. Традиционно же формализуемые задачи решаются путём поэтапных вычислений.

Процесс квантового вычисления, в отличие от классического, обычно описывается линейным алгоритмом, определяющим ход преобразования состояний вычислительной системы.

В отличие от обычного компьютера, оперирующего наборами из конечного числа дискретных состояний битов, квантовый компьютер работает с конечными наборами элементарных непрерывных состояний, называемых квантовыми битами (q-битами).

Каждый q-бит имеет два выделенных состояния (к примеру, для спинов это состояния “спин вверх” и “спин вниз”). Выделенные (базисные) состояния определяют только чистые состояния системы. Кроме того, возможны и любые линейные комбинации базисных состояний с комплексными коэффициентами. Состояние такой системы выражается пси-функцией [1] и описывается выражением

$$\varphi(x) = a\left|0\right\rangle + b\left|1\right\rangle, \quad (1)$$

где a, b – комплексные коэффициенты, называемые амплитудами и характеризующие вероятность нахождения системы в состоянии логического нуля и логической единицы, такие, что

$$\left|a\right|^2 + \left|b\right|^2 = 1. \quad (2)$$

Для реализации вычислительного процесса может использоваться несколько q-битов, образующих ансамбль [2]. Состояние q-бита можно представить вектором в двухмерном комплексном векторном пространстве с выделенным ортонормированным базисом. Возможные состояния систем из n q-битов, в которой состояние каждой частицы описывается вектором в двухмерном пространстве, образует пространство состояний размерностью 2^n.

Пространство состояний системы нескольких спинов описывается через тензорное произведение пространств состояний частиц системы [1], причём размерность полученного пространства состояний будет равна произведению размерностей пространств состояний микрочастиц, образующих систему.

Этот факт приводит к экспоненциальному росту пространства состояний и гипотетическому экспоненциальному увеличению эффективности вычислений для реального квантового вычислителя.

Существуют наборы унитарных [1] операторов, отражающих формализованные управляющие воздействия на q-бит или их систему. Важным следствием того, что квантовые преобразования унитарны (сохраняют скалярное произведе-

ние), является их обратимость. Повторное действие унитарного оператора на произвольную квантовую систему переводит ее в исходное состояние.

Если A − множество унитарных операторов, то схема квантового вычисления – это последовательность операторов

$$U = U_1 \times U_2 \ldots \times U_j \ldots \times U_L, \quad (2)$$

где L – размерность квантовой схемы, а каждый оператор U_j принадлежит множеству A.

Схема U вычисляет функцию $F(x)$, если для любого x выполняется выражение [1]:

$$\sum_z \left| \left\langle F(x), z \middle| x \middle| x, O^{N-n} \right\rangle \right|^2 \geq 1 - \varepsilon, \varepsilon < 1 \text{., x/z/e}, \quad (3)$$

где x – любое число, ε – фиксированное число, меньше $1/2$, z – число, образованное дополнительными битами, которые используются для вычисления и не учитываются в результате, O^{N-n} – набор q-битов в состоянии логического нуля. В общем случае x и $F(x)$ состоят из разного количества битов, хотя длина вектора $\left\langle F(x), z \right|$ равна длине $\left| x, O^{N-n} \right\rangle$.

Квантовые вычисления сами по себе не включают понятий условных переходов и циклического выполнения участков алгоритма. Весь процесс вычисления представляется линейно и выглядит как последовательность операторов, применяемая к различным элементам квантовой вычислительной системы. Хотя условные операторы используются в квантовых вычислениях, они предназначены для модификации состояний подсистемы, на которую воздействуют в случае выполнения условий. Однако это не могут быть операторы присвоения конкретных состояний: доступны только операторы, модифицирующие текущее состояние квантовой вычислительной системы или её части.

Структура квантового вычислителя имеет мало общего с классическими архитектурами ЭВМ (фон-неймановской, гарвардской), поэтому термин “квантовый компьютер” не является вполне корректным. Структурная схема квантового вычислителя может быть представлена в виде, показанном на рис. 1.

Так, кроме набора квантовых бит (квантового регистра) той или иной природы, необходимо наличие системы, задающей управляющие воздействия для произведения вычислений на квантовом регистре, и системы измерения состояний квантового регистра для получения результата производимого вычисления.

Управление деятельностью составляющих частей квантового вычислителя может производиться с помощью классической ЭВМ [3].

Квантовый вычислитель является по форме последовательной вычислительной системой (управляющие воздействия подаются в виде последовательных серий), однако по сути вычисления параллельны. Квантовый параллелизм вычислений достигается за счёт соответствующей алгоритмической реализации и использования эффекта “квантовых связей” (entanglement [1]). Управляющие воздействия реализуют операторы, действуют на биты регистра, которые, в свою очередь, могут быть связаны со многими (или даже со всеми) другими q-битами вычислительной системы. В результате, безотносительно к размерности квантовой вычислительной системы, возможна организация параллельного вычисления с привлечением всех её элементов.

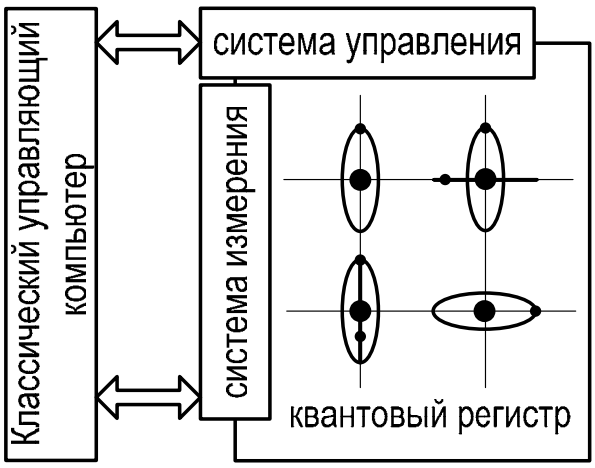

Рис. 1. Структурная схема квантового вычислителя

Квантовая система в значительной степени подвержена внешним случайным воздействиям. И для корректной работы вычислителя необходимо, чтобы весь процесс протекал за интервал времени, гарантирующий вероятность минимального накопления возмущений. В противном случае значение квантового регистра может быть нецеленаправленно изменено, что исказит результат вычисления.

Если максимально допустимое количество операций до того, как вероятность декогерентизации системы станет недопустимо велика, равно N, то максимум через каждые N тактов вычисления необходимо сохранять промежуточный результат и инициализировать квантовый регистр этими значениями прежде, чем можно будет продолжать вычисления. В этом случае появляются моменты, когда состояние системы приходится измерять и сохранять в классическом регистре.

Таким образом, до тех пор, пока не будет разработана технология, дающая возможность проводить квантовые вычисления без технических остановок, может использоваться методика организации классических операций с данными, временно сохраняемыми в регистре классической природы.

Набор доступных операций может включать классические вычислительные операции, такие как присвоение значений (не существует в квантовом виде), арифметические операции и т.п.

Однако самое важное, что возможными становятся операции перехода в рамках программы управляющей ЭВМ по значениям определённых наборов q-бит либо безусловные переходы.

Благодаря этому замечанию, алгоритм квантового вычисления может быть преобразован из линейного в ветвящийся (рис. 2), что в определённых условиях даёт большие преимущества.

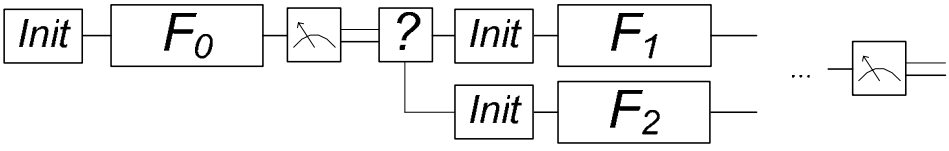

Рис. 2. Схема процесса вычисления:
Init – инициализация квантового регистра; F_i – *i*-ый шаг вычисления;
? – анализ полученных значений

Схема, приведённая на рис. 2, изображает этапы модифицированного квантового вычисления (слева направо):

1) инициализация, вычисление, измерение с сохранением результата – то же, что и в обычном варианте квантовых вычислений;

2) обработка и анализ сохранённого результата, ветвление по некоторым условиям;

3) повторение действий, аналогичных этапу 1;

4) завершение вычисления измерением результирующего состояния системы.

Следует отметить, что методика, приведённая на схеме, не может быть использована в случае организации непрерывного квантового вычисления. Причина именно в том, что измерение состояний квантовых систем приводит к проецированию смешанных состояний на оси сферы Блоха. В результате будут потеряны все преимущества, связанные с запутанностью и квантовым параллелизмом вычислений.

Реализовать предложенную методику модификации квантовых вычислений можно посредством дополнения программы управляющего компьютера возможностями анализа и изменения сохраняемых значений квантового регистра и перехода на заданные участки управляющей программы вычислений в зависимости от анализируемых значений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Китаев А., Шень А., Вялый М.* Классические и квантовые вычисления. – Москва: МЦНМО, ЧеРо 1999. – 192с.
2. *Кокин А. А.* Твердотельные ядерные магнитно-резонансные (ЯМР) ансамблевые квантовые компьютеры (Исследование физических основ и проблем реализации). – Москва: Физико-технологический институт Российской Академии Наук, 2003. – 187с.
3. *Кокин А.А.* Физические реализации квантового компьютера. – Москва: ФТИАН / http://elanina.narod.ru/lanina/index.files/student/tehnology /text/ kvant .htm#J18.

УДК 681.51

А.О. Кожанов

МЕТОД СКРЫТИЯ ПЕРЕДАЧИ ИНФОРМАЦИИ ПРИ ПОМОЩИ СТРАННОГО АТТРАКТОРА АНИЩЕНКО–АСТАХОВА

В последние годы был предложен ряд способов скрытой передачи информации, базировавшихся на применении в качестве несущего сигнала широкополосных колебаний генератора хаоса. Авторы работ по данной тематике с целью выделения информационного сигнала из хаотического обычно использовали явление хаотической синхронизации. Методы, основанные на явлении синхронизации, имеют ряд недостатков, наиболее существенным из которых является требование идентичности генераторов хаотических колебаний в приемнике и передатчике [1].

В статье представлен метод обработки и защиты информации, основанный на теории глобальной реконструкции динамической хаотической системы Анищенко–Астахова с использованием синергетического наблюдателя.

Моделирование системы

Для построения модели использовался подход параметрически модулированных хаотических генераторов. Исходная динамическая система Анищенко–Астахова описывается нелинейными дифференциальными уравнениями: