УДК 539.12

КВАНТОВАЯ ИНФОРМАЦИЯ, КУБИТЫ И КВАНТОВЫЕ АЛГОРИТМЫ

С.А. Дуплий, В.В. Калашников, Е.А. Маслов
Харьковский национальный университет им. В. Н. Каразина
пл. Свободы, 4, г. Харьков, 61077, Украина
E-mail: Steven.A.Duplij@univer.kharkov.ua. Internet: http://www.math.uni-mannheim.de/~duplij
Поступила в редакцию 15 марта 2005 г.

В работе кратко изложены главные идеи и понятия теории квантовой информации и принципы квантовых вычислений, лежащие в основе квантовых компьютеров. Рассматриваются свойства кубитов и их обобщения, преобразования над ними, различные типы квантовых гейтов. Показано, что сцепленные квантовые состояния получаются действием R-матрицы как универсального двукубитного квантового гейта. Излагаются некоторые алгоритмы квантовых вычислений и поясняются их особенности, отличающие от соответствующих классических алгоритмов.
КЛЮЧЕВЫЕ СЛОВА: квантовый компьютер, квантовый гейт, кубит, регистр, кубитная теория поля

Теоретические представления о первичности квантового характера взаимодействий структурных элементов вычислительных систем естественным образом привели к созданию теории квантовой информации [1] как симбиозу классической теории информации, теории вычислений и нерелятивистской квантовой механики [2] и построению модели универсального вычислительного устройства — квантового компьютера [3,4]. Анализ квантово-инфомационных и соответствующих им классических построений показал наличие зависимости от набора базовых (определяющих) математических аксиом свойств вычислительной системы — таких, как вычислительная сложность, классы алгоритмов, размерность представления задачи и, как следствие, наличие в квантовом базисе эффективных процедур решений многих практических задач (см. например, [5,6]). Основное преимущество квантовых каналов связи по сравнению с классическими заключается в их качественно более высоком уровне защиты: совершенный квантовый канал (без шума) имеет, в принципе, абсолютную защиту, поскольку любая попытка вмешательства в систему сразу же обнаруживается — квантовый канал связи можно разрушить, но невозможно вскрыть [3,5].

Идея квантовых вычислений была высказана Ричардом Фейнманом в 1982 [7], который обсуждал два вопроса: 1) существует ли какие-нибудь физические ограничения на функционирование компьютера, накладывающие запреты на реализуемость алгоритмов; 2) если построить квантовое вычислительное устройство, будут ли его возможности превосходить возможности обычных вычислительных устройств? Также, Фейнман предположил, что квантовый компьютер может быть полезен для моделирования самих квантовых систем [7]. В 1980 г. Беннефф [8] показал, что обратимая унитарная эволюция в состоянии реализовать машину Тьюринга [9], так что вычислительная мощность квантового компьютера не меньше, чем у классического. Но он не выяснял, являются ли квантовые устройства более мощными, чем классические, а сам термин "квантовый компьютер"он не употреблял. Затем в 1985 г. Дойч [10] создал формальную теорию квантовых вычислений [11], он определил квантовую машину Тьюринга и квантовую цепь, а также некоторые свойства этих систем (см. также [6,12]).

КУБИТЫ И ИХ ОБОБЩЕНИЯ

В классических вычислительных системах минимальной единицей информации является бит [13], т.е. структура, имеющая 2 состояния (обозначаемые обычно 0 и 1), образущих одномерное дискретное пространство. Такая вычислительная система, состоящая из одного бита, может выполнять всего 4 вида преобразований: тождественное (*id*), отрицание (not), вычисление константы 0 (*set*0) и вычисление константы 1 (*set*1).

Минимальной единицей информации, которой оперирует квантовый компьютер, является так называемый *кубит* [10]— квант, имеющий два детерминированных состояния $|0\rangle$ и $|1\rangle$. Квантовая природа кубита заключается в принципе суперпозиции, согласно которому кубит находится одновременно сразу в обоих своих базовых состояниях.

Например, “частицу со спином $1/2$” можно рассматривать, как кубит, являющийся суперпозицией двух состояний, когда спин частицы направлен вверх и когда он направлен вниз, соответственно. Квантовый компьютер можно трактовать как множество, состоящее из n кубитов, для которого практически определены следующие операции [2,8,11]:

1. Каждый кубит можно приготовить в некотором известном состоянии $|0\rangle$.

2. Каждый кубит может быть измерен в базисе $\{|0\rangle, |1\rangle\}$.

3. Универсальный квантовый гейт (или набор гейтов) можно применить к любому подмножеству, состоящему из фиксированного числа кубитов.

4. Состояние кубитов изменяется только посредством вышеуказанных преобразований [12].

Для минимальной реализации любого квантового алгоритма необходимо иметь всего лишь двукубитный квантовый компьютер, устройство ввода-вывода и хранилище квантовой информации [3]. Тогда можно производить "конструктивные"операции с кубитами только “внутри” него, а также обмениваться информацией с внешней "памятью". Все, что требуется от “памяти” — это “ничего не делать” с кубитами, а хранить именно квантовую информацию в суперпозиционном виде.

Для двух состояний $|0\rangle$ и $|1\rangle$ кубит записывается в виде

$$|\psi\rangle = a|0\rangle + b|1\rangle, \qquad |a|^2 + |b|^2 = 1. \tag{1}$$

В матричных обозначениях Дирака

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \ |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2}$$

кубит (1) имеет вид $|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$.

Таким образом, векторы состояний $|0\rangle$ и $|1\rangle$ образуют (в отличие от классического случая) двумерное пространство, морфизмы которого задают матричное представление квантовых аналогов классических базисных функций [10]. Тождественное преобразование представляется единичной матрицей, представление функции отрицания *not* имеет вид

$$not = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{3}$$

и совпадает с матрицей Паули σ_x , а функции *set*0 и *set*1 равны

$$set0 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, set1 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}. \tag{4}$$

Для квантового случая можно построить неограниченное число преобразований, не имеющих классических аналогов [2, 12].

Конкретную реализацию вычислительного преобразования принято называть вентилем (гейтом) [14]. В классическом случае единственным однобитным гейтом является только базисное преобразование *not*. Среди квантовых однокубитных преобразований, не имеющих классических аналогов, выделяются следующие:

H-гейт Адамара

$$H \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{5}$$

S-фазовый гейт

$$S \equiv \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \tag{6}$$

$\pi/8$-гейт

$$T \equiv \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}, \tag{7}$$

для которых существуют простые физические интерпретации [1].

Отметим, что оператор плотности, отвечающий кубиту (1) имеет вид [15]

$$\hat{\rho} = |\psi\rangle\langle\psi| = |a|^2|0\rangle\langle 0| + ab^*|0\rangle\langle 1| + a^*b|1\rangle\langle 0| + |b|^2|1\rangle\langle 1|, \tag{8}$$

что соответствует матрице плотности

$$\rho = \begin{pmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{pmatrix}. \tag{9}$$

Это позволяет найти квантовый аналог энтропии фон Ноймана для кубита [15]

$$S_Q(\hat{\rho}) = -Tr_\Psi \left[\hat{\rho}\log_2\hat{\rho}\right], \tag{10}$$

(след берется по всем степеням свободы, ассоциированным с квантовым состоянием Ψ) которая сводится к классической формуле Шеннона для энтропии, если $\hat{\rho}$ есть смешанное состояние, составленное из ортогональных квантовых состояний. Для кубита $S_Q(|\psi\rangle) = 1$.

По аналогии с дираковским сопряжением двухкомпонентных спиноров антикубит определяется как

$$\langle\bar{\psi}| = \langle\psi^+|\gamma^0 = \langle\psi^+|(i\sigma_y) = (a^*, b^*)\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = (-b^*, a^*) = a^*\langle 1| - b^*\langle 0|, \tag{11}$$

где σ_y — матрица Паули. Соответствующая матрица плотности для антикубита имеет вид

$$\bar{\rho} = \begin{pmatrix} |a|^2 & -ab^* \\ -a^*b & |b|^2 \end{pmatrix}, \tag{12}$$

и для антикубита $S_Q(\langle\bar{\psi}|) = -1$ [15].

Аналогичным образом можно описать трехуровневые квантовые системы — кутриты [16]. Примером конкретной реализации кутрита является трехуровневая система, основанная на поляризационных состояниях бифотонов (суперпозиция двухфотонного состояния и вакуума), которую можно представить формулой [16]

$$|\psi\rangle = a\,|2,0\rangle + b\,|1,1\rangle + c\,|0,2\rangle\,, \quad |a|^2 + |b|^2 + |c|^2 = 1. \tag{13}$$

В работе [17] кубиты трактовались как "парафермионы" в некотором пространстве Фока, т.е. гибридные фермион-бозонные частицы с "промежуточной" статистикой, которые могут быть только составными [18].

Перспективным также является построение кубитной теории поля [19], в рамках которой наблюдаемые не коммутируют в разделенных пространственно-временных областях, и это не приводит к противоречиям.

В суперсимметричной кубитной теории поля [15] для описания кубитов применяется формализм суперсимметричной квантовой механики [20, 21], причем оператор суперзаряда Q трактуется как "корень квадратный" из *not*. В рамках этой модели вводятся антикоммутирующие кубиты, и кубит-антикубитные пары трактуются как аналог фермионного конденсата, который в свою очередь интерпретируется как информационный вакуум [15].

СЦЕПЛЕННЫЕ СОСТОЯНИЯ И R-МАТРИЦА

Конечный упорядоченный набор n кубитов (изолированных или взаимодействующих) называют n-разрядным квантовым регистром, причем число его базисных состояний (упорядоченных строк из нулей и единиц, например $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$) равно 2^n, что совпадает с общим числом состояний классического регистра [11].

Произвольный вектор состояния n-разрядного квантового регистра в общем случае есть

$$|\psi\rangle = \sum_{i=0}^{2^n-1} a_i\,|i\rangle\,, \tag{14}$$

где $|i\rangle$ — двоичная запись базисного состояния.

Если два кубита находятся в определенных состояниях $|\psi_1\rangle$ и $|\psi_2\rangle$, то состояние 2-разрядного регистра будет определяться их тензорным произведением

$$|\psi_{12}\rangle = |\psi_1\rangle \otimes\ |\psi_2\rangle. \tag{15}$$

Состояния двух кубитов, которые не описываются таким тензорным произведением (15), называются сплетенными (entangled) [22]. Именно такие состояния [23] ответственны за специфичность квантовых вычислительных систем [24].

В общем случае состояние двух кубитов определяется формулой

$$|\psi_{12}\rangle = A|00\rangle + B|01\rangle + C|10\rangle + D|11\rangle. \tag{16}$$

Из определения (1) и отождествления $|ij\rangle \equiv |i\rangle \otimes\ |j\rangle$ следует, что условием невыполнения (15) является неравенство

$$AD - BC \neq 0, \tag{17}$$

которое поэтому и является условием того, что состояние $|\psi_{12}\rangle$ сплетенное [23]. Каждое несплетенное состояние может быть преобразовано в сплетенное с помощью квантового гейта, который является универсальным (теорема Брулинских [25]) так, что сумма вероятностей всех состояний сохраняется.

В общем случае двукубитный квантовый гейт представляет собой унитарную матрицу, которая удовлетворяет квантовому уравнению Янга-Бакстера [26], то есть R-матрицу [27] специального вида. Классификация таких R-матриц была проведена в [28].

В качестве примера приведем 4-вершинную R-матрицу, которая действует на тензорное произведение двух кубитов $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ формулой $R\,(|\psi\rangle \otimes |\psi\rangle)$, сцепливает их при выполнении (17) и имеет вид (16)

$$R = 2\begin{pmatrix} A & 0 & 0 & 0 \\ 0 & 0 & B & 0 \\ 0 & C & 0 & 0 \\ 0 & 0 & 0 & D \end{pmatrix}. \tag{18}$$

КВАНТОВЫЕ АЛГОРИТМЫ

В отличие от случая обычной формальной логики, операции над кубитами носят квантовый, вероятностный характер, что обусловливает некоторые особенности таких операций [8,10]. В общем случае, выделяют три класса квантовых алгоритмов [24]: 1) алгоритмы, основанные на квантовых версиях преобразования Фурье; 2) алгоритмы квантового поиска; 3) алгоритмы моделирования квантовых систем. Во всех случаях квантовый алгоритм решает залачу эффективней классического.

Фундаментальным свойством квантовых вычислений является квантовый параллелизм, позволяющий вычислять функцию $f(x)$ для некоторых значений x одновременно. Рассмотрим вычисление функции от битовой переменной $f(x) : \{0,1\} \to \{0,1\}$. На квантовом компьютере введем двукубитовое состояние $|x,y\rangle$, где x и y можно трактовать как регистры (данных и мишени). Тогда с помощью последовательности гейтов, представляемое унитарным преобразованием U, состояние $|x,y>$ можно преобразовать таким образом $|x,y\rangle \to |x, y \oplus f(x)\rangle$. Если $y = 0$, то состояние второго кубита совпадает со значением вычисляемой функции, и получаем $|x,0\rangle \to |x, f(x)\rangle$. Таким образом, в результате квантового вычисления мы имеем информацию о значении функции в двух точках одновременно, что и называется термином “квантовый параллелизм” [2]. В отличие от параллельных вычислений на классических компьютерах, где технически создается несколько цепей, производящих вычисления, в квантовом компьютере вычисления проводятся в одной цепи, но на суперпозиции состояний [4, 11].

Рассмотрим классическую задачу Дойча [10] и ее решение при помощи модели квантового компьютера [4]. Пусть $f : \{0, 1\} \to \{0, 1\}$ — однозначная функция над битом информации. Очевидно, таких функций можно задать всего четыре — две “константы” $f_{00}(x) = 0$ и $f_{11}(x) = 1$ и две “балансирующие” функции

$$f_{01}(x) = \begin{cases} 0, x = 1 \\ 1, x = 0 \end{cases}, \qquad f_{10}(x) = \begin{cases} 1, x = 1 \\ 0, x = 0 \end{cases}. \tag{19}$$

Задача состоит в том, чтобы определить, является $f(x)$ константой или балансирующей. В случае классического компьютера необходимо вычислить выражение $f(0) \oplus f(1)$, где символом $\oplus$ обозначено сложение по модулю 2), для чего необходимо дважды вычислить функцию $f(x)$, однако квантовый компьютер может дать ответ на этот вопрос и за одно вычисление. Действительно, построим оператор U_f следующим образом

$$|x\rangle|y\rangle \xrightarrow{U_f} |x\rangle|y \oplus f(x)\rangle. \tag{20}$$

Легко видеть, что для получения значения функции $f(x)$ при помощи этого оператора его необходимо применить к комбинации $|x\rangle|0\rangle$, так как $0 \oplus a = a$ для любого значения a . Рассмотрим результат применения U_f к $|x\rangle$ и суперпозиции $\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$ в виде

$$|x\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}} \xrightarrow{U_f} \begin{cases} |x\rangle\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}, x{=}\ 0, \\ |x\rangle\dfrac{|1\rangle - |0\rangle}{\sqrt{2}}, x{=}\ 1. \end{cases} \tag{21}$$

Построим результат применения U_f к комбинации суперпозиции $\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$ и суперпозиции $\dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}}\frac{|0\rangle - |1\rangle}{\sqrt{2}} \xrightarrow{U_f} (-1)^{f(0)}\left(\frac{|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle}{\sqrt{2}}\right)\frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{22}$$

Искомый результат, $f(0) \oplus f(1)$, может быть измерен физическими методами. Так что, при помощи квантового компьютера ответ на заданный вопрос может быть получен *однократным* применением оператора U_f .

Таким образом, квантовые вычисления позволяют получать информацию о значении функции в нескольких точках одновременно — в результате многие классические алгоритмы при применении их на квантовом компьютере могут быть значительно упрощены.

Один из наиболее важных алгоритмов в теории квантовых вычислений — алгоритм нахождения периода функции. Рассмотрим функцию $f(x)$ с периодом $r : f(x + r) = f(x)$. Зададим некое значение x, при котором легко вычислить $f(x)$, и выберем каким-либо образом целое N такое, чтобы $N/2 < r < N$. Организуем систему из $2n$ кубитов, где $n = [\log_2 N]$ и $[x]$ — операция “округления вверх”, собранных в два “регистра” по n кубитов — x и y . Исходное состояние системы есть

$$\frac{1}{\sqrt{\omega}}\sum_{x=0}^{\omega-1}|x\rangle|0\rangle, \tag{23}$$

здесь $\omega = 2^n$. Применим к этой системе оператор U_f и получим

$$\frac{1}{\sqrt{\omega}}\sum_{x=0}^{\omega-1}|x\rangle|f(x)\rangle. \tag{24}$$

Как уже упоминалось, данная операция вычисляет за один шаг значения $f(x)$ в $\omega = 2^n$ точках. Квантовые законы определяют невозможность доступа к каждому из этих значений по отдельности, поэтому просто перебрать полученные значения невозможно — каждое измерение регистра y по вычислительному базису даст некое значение $f(x) = u$. То есть регистр y "переброшен" в состояние $|u\rangle$, и общее состояние системы таково

$$\frac{1}{\sqrt{M}}\sum_{j=0}^{M-1}|d_u + jr\rangle|u\rangle. \tag{25}$$

В этом выражении $d_u + jr$ — это все значения x , для которых $f(x) = u$. Другими словами, периодичность $f(x)$ означает, что регистр x представлен в виде суперпозиции M состояний (где $M \simeq \omega/r$) при значениях x, взятых с периодом r . Для определения периодичности x применим преобразование Фурье

$$U_{\mathbf{FJ}}|x\rangle = \frac{1}{\sqrt{\omega}}\sum_{k=0}^{\omega-1}e^{i2\pi kx/\omega}|k\rangle. \tag{26}$$

Надобность в регистре y отпала, так что в выражении для состояния системы его можно опустить. Итак,

$$U_{\mathbf{FJ}}\frac{1}{\sqrt{\omega/r}}\sum_{j=0}^{\omega/r-1}|d_u + jr\rangle = \frac{1}{\sqrt{r}}\sum_{k}\tilde{f}(k)|k\rangle, \tag{27}$$

где $\left|\tilde{f}(k)\right| = \begin{cases} 1, \text{если } k \text{ кратно } \omega/r, \\ 0, \text{в остальных случаях}. \end{cases}$

Измерение регистра x после проведенных преобразований дает значение, кратное ω/r, а именно $x = \lambda\omega/r$, где λ — неизвестное целое. Если λ и r не имеют общих множителей, то для вычисления r достаточно дробь x/ω привести к несократимой и взять ее знаменатель. В противном случае все шаги алгоритма необходимо повторить. В [29] показано, что вероятность решения поставленной задачи после не более, чем $\log_2 r$ повторений, сколь угодно близка к 1.

Вся важность этого алгоритма для решения практических задач видна на примере построенного на нем метода факторизации целого числа — алгоритма Шора [6]. Задача факторизации считается сложной для классического компьютера, поэтому многие схемы криптографии с открытым ключом построены на практической невозможности решения этой задачи для большого исходного числа. Однако применяя рассмотренный квантовый алгоритм определения периода функции к $f(x) = a^x \bmod N$, где N — число, которое требуется факторизовать, а a — произвольное целое $a < N$, можно получить некий период этой функции r . Из элементарной теории чисел известно, что r — четное число, а величина $a^{r/2} \pm 1$ будет иметь общий множитель с N , который, будучи вычислен, например, классическим алгоритмом Евклида, будет нетривиальным делителем N . Используя какой-нибудь эффективный метод вычисления $f(x)$, например, последовательные возведения в квадрат (по модулю N) и разложение $f(x)$ в сумму полученных значений, можно эффективно решать на квантовом компьютере неразрешимую для классических компьютеров задачу [6].

Среди прочих алгоритмов квантовых вычислений следует отметить квантовый алгоритм Гровера — алгоритм поиска по неотсортированной базе данных [30]. В случае классического компьютера такой поиск занимает в среднем $N/2$ шагов, а алгоритм Гровера, использующий свойство квантового параллелизма, за $\sqrt{N}$ шагов. Отметим, что алгоритм Гровера является оптимальным в том смысле, что ни один квантовый алгоритм не может работать быстрее, чем $O\left(\sqrt{N}\right)$ [8].

ВЫВОДЫ

Таким образом, в работе рассмотрены идеи, лежащие в основе квантовых компьютеров: базовые понятия теории квантовой информации и принципы квантовых вычислений, проанализированы различные свойства кубитов, преобразования над ними, рассмотрены различные типы квантовых гейтов. Показано, что сцепленные квантовые состояния получаются действием R-матрицы как универсального двукубитного квантового гейта. Представлены алгоритмы квантовых вычислений и обсуждаются те их особенности, которые приводят к большей скорости вычислений, чем соответствующие классические алгоритмы.

СПИСОК ЛИТЕРАТУРЫ

1. Galindo A., Martin-Delgado M. A. Information and computation: Classical and quantum aspects // Rev. Mod. Phys. - 2002. - V. 74. - P. 348.
2. Холево А. С. Введение в квантовую теорию информации. - М.: МЦНМО, 2002.
3. Дойч Д. Квантовая теория, принцип Черча-Тьюринга и универсальный квантовый компьютер // Квантовый компьютер и квантовые вычисления. - 1999. - Т. 2. - С. 157.
4. Williams C. P., Clearwater S. H. Explorations in Quantum Computing. - New York-Berlin-Heidelberg: Springer-Verlag, 1998.
5. Шор П. В. Полиномиальные по времени алгоритмы разложения числа на простые множители и нахождения дискретного логарифма для квантового компьютера // Квантовый компьютер и квантовые вычисления. - 1999. - Т. 2. - С. 200.
6. Shor P. W. Algorithms for quantum computation: Discrete logarithms and factoring // Proceeding of the 35th Annual Symposium on Foundations of Computer Science. - Los Alarnitos. IEEE Computer Society Press, 1994. - P. 124–134.
7. Feynman R. Simulating physics with computers // Int. J. Theor. Phys. - 1982. - V. 21. - P. 467–468.
8. Benioff P. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines // J. Stat. Phys. - 1980. - V. 22. - P. 563–591.
9. Turing A. On computable numbers with an application to the Entscheidungsproblem // Proc. London Math. Society. - 1937. - V. 42. - P. 230–265.
10. Deutsch D. Quantum theory, the Church-Turing principle and the universal quantum computer // Proc. Roy. Soc. London. - 1985. - V. A400. - P. 96–117.
11. Китаев А., Шень А., Вялый М. Классические и квантовые вычисления. - М.: МЦНМО, 1999.
12. Стин Э. Квантовые вычисления. - Ижевск: НИЦ Регулярная и хаотическая динамика, 2000.
13. Цымбал В. П. Теория информации и кодирование. - К.: Высшая школа, 1992.
14. Хоровиц П., Хилл У. Искусство схемотехники. Т. 1. - М.: Мир, 1986. - 508 с.
15. Hruby J. Supersymmetry and qubit field theory // Prague, 2004. - 20 p. (Preprint Institute of Physics, quant-ph/0402188).
16. Богданов Ю. И., Кривицкий Л. А., Кулик С. П. Статистическое восстановление квантовых состояний оптических трехуровневых систем // Письма в ЖЭТФ. - 2003. - Т. 78. - № 6. - С. 804–806.
17. Wu L.-A., Lidar D. A. Qubits as parafermions // J. Math. Phys. - 2002. - V. 43. - № 9. - P. 4506–4525.
18. Marcinek W. Categories and quantum statistics // Rep. Math. Phys. - 1996. - V. 38. - № 2. - P. 149–174.
19. Deutsch D. Qubit field theory // Oxford, 2004. - 23 p. (Preprint Clarendon Laboratory, quant-ph/0401024).
20. Witten E. Dynamical breaking of supersymmetry // Nucl. Phys. - 1981. - V. B188. - P. 513–537.
21. Cooper F., Freedman B. Spontaneous supersymmetry breaking in quantum mechanics // Ann. Phys. - 1983. - V. 146. - № 2. - P. 262–288.
22. Kauffman L. H., Lomonaco S. J. Braiding operators are universal quantum gates // New J. Phys. - 2004. - V. 6. - P. 134–139.
23. Werner R. F. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model // Phys. Rev. - 1989. - V. A40. - P. 4277–4286.
24. Cleve R., Ekert A., Macchiavello C., Mosca M. Quantum algorithms revisited // Phil. Trans. Royal Soc. London. - 1998. - V. A454. - P. 339–354.
25. Brylinski J. L., Brylinski R. Universal quantum gates // Mathematics of Quantum Computation. - Boca Raton. Chapman & Hall/CRC Press, 1994. - P. 124–134.
26. Zhang Y., Kauffman L. H., Ge M.-L. Yang-Baxterization, Universal quantum gate, and Hamiltonians // Chicago, 2005. - 36 p. (Preprint Univ. Illinois, quant-ph/0502015).
27. Lambe L. A., Radford D. E. Introduction to the Quantum Yang-Baxter Equation and Quantum Groups: An Algebraic Approach. - Dordrecht: Kluwer, 1997. - 292 p.
28. Dye H. A. Unitary solutions to the Yang-Baxter equation in dimension four // Quantum Information Processing. - 2003. - V. 2. - P. 117–150.
29. Ekert A., Jozsa R. Quantum quantum computation and Shor's factoring algorithm // Rev. Mod. Phys. - 1996. - V. 68. - P. 733–745.
30. Grover L. K. Quantum mechanics helps in searching for a needle in a haystack // Phys. Rev. Lett. - 1997. - V. 79. - P. 325–328.

QUANTUM INFORMATION, QUBITS AND QUANTUM ALGORITHMS

S.A. Duplij, V.V. Kalashnikov, E.A. Maslov

Department of Physics and Technology

V. N. Karazin Kharkov National University, Svoboda Sq. 4, Kharkov 61077, Ukraine

The main ideas and notions of quantum information theory and principles of quantum computing, which are basic in quantum computers, are reviewed. Various proprerties of qubits and their generalizations are considered. Some quantum computing algorithms are explored and their peculiarities which differ them from correspondent classical algorithms are presented.

KEY WORDS: quantum computer, quantum gate, qubit, register, qubit field theory