УДК 681.3

МОДУЛЯРНЫЕ ОПЕРАЦИИ В КВАНТОВЫХ ВЫЧИСЛЕНИЯХ

С. Л. Ремизов, А. Б. Шелудяков

В статье рассматриваются способы согласования правил модулярной арифметики и квантовых вычислений, а так же реализация суммирования по модулю с помощью квантовых вентилей.

1. Введение

Основным требованием к устройствам цифровой обработки информации, решающим задачи обработки сигналов, изображений, распознавания образов, криптографии, обработки данных большой размерности является высокое быстродействие.

Наиболее перспективный путь повышения быстродействия – это распараллеливание обработки информации. Распараллеливание может осуществляться по следующим направлениям:

- распараллеливание архитектуры вычислительных средств;
- распараллеливание алгоритмов вычисления решаемых задач;
- распараллеливание машинной арифметики, в которой реализуются алгоритмы.

Распараллеливание архитектуры вычислительных средств в основном осуществляется путём повышение степени интеграции сверхбольших интегральных схем (СБИС). Примером такой интеграции является наличие в одном микропроцессоре нескольких ядер, организация внутренних вычислительных конвейеров и многоуровневой кэш-памяти [10]. Однако здесь традиционная микроэлектроника подходит к пределу своих технологических возможностей. Толщина слоёв таких СБИС измеряется нанометрами, что приводит к высокому риску электрических пробоев и проблемам с отводом тепла. Кроме того, при толщине слоёв, сравнимых с размерами атомов, начинают сказываться квантомеханические эффекты [4].

Распараллеливание алгоритмов вычисления решаемых задач наиболее эффективно реализуется при организации квантовых вычислений, использующих линейные преобразования, применяемые одновременно к суперпозиции базисных векторов и создающее таким образом суперпозицию результатов [2, 12].

Распараллеливание машинной арифметики осуществляется путём использования непозиционных (модулярных) систем счисления, в частности, системы остаточных классов (СОК). Об эффективности применения этой системы счисления в вычислительной технике свидетельствует тот факт, что ещё в 60-х годах прошлого века в СССР была создана ЭВМ К-340А для радиолокационных станций системы ПРО. Это была первая в мире ЭВМ с производительностью свыше 1 млн. операций в секунду (1,2 млн. двойных, или 2,4 млн. обычных операций в секунду) при самой низкой в стране стоимости операции (25 коп.). Благодаря высокой надёжности ЭВМ К-340А до сих пор находятся в эксплуатации [7,8].

Существует ряд задач, которые возникают при аппаратной (физической) реализации квантового компьютера. От того, каким образом будут решены эти задачи, зависит и структура вычислительных алгоритмов, использующих квантовый параллелизм [8].

Одной из таких задач является увеличение разрядности квантового компьютера. На сегодняшний день создан 5-ти разрядный квантовый компьютер, реализующий алгоритм Шора по разложению числа на множители [11]. Но для организации качественно нового уровня вычислений необходимо обрабатывать данные длинной несколько десятков разрядов [9].

Применение СОК в вычислительных устройствах даёт следующие ее преимущества:

- повышенную производительность и простоту аппаратной реализации арифметического устройства за счёт малоразрядности оснований;
- повышенную надёжность системы благодаря свойствам СОК, обеспечивающим обнаружение и исправление ошибок, возникающих при выполнении операций в арифметическом устройстве [1, 13].

Использование свойства малоразрядности СОК в квантовых вычислениях позволит увеличить общий диапазон квантового компьютера, но в настоящее время нет модулярных алгоритмов, которые бы удовлетворяли основному требованию, предъявляемому к квантовым вычислениям – свойству обратимости.

Цель данной работы – построение обратимого алгоритма нахождения остатка от числа по заданному модулю и его реализация с использованием квантовых логических схем.

2. Согласование квантовых алгоритмов с правилами модулярной арифметики

Состояния квантовой системы и их преобразования можно описать посредством векторов и матриц. Орто-

Статья поступила в редакцию 10.10.2006;исправленный вариант представлен 13.11.2007.

нормированный базис $\{|0\rangle,|1\rangle\}$ можно записать следующим образом

$$\{|0\rangle,|1\rangle\} \Rightarrow \left\{\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix}\right\} \quad (1)$$

В соответствии с принципом суперпозиции наиболее общее нормированное состояние с базисом вида (1), может быть представлено в виде

$$|\psi\rangle = a|0\rangle + b|1\rangle,\ |a|^2 + |b|^2 = 1, \quad (2)$$

где a и b – комплексные числа.

Состояние вида (2) в теории квантовых вычислений называется кубитом. Проектируя состояние кубита на ортонормированный базис (1) получим

$$\langle 0|\psi\rangle = a\ ;\ \langle 1|\psi\rangle = b \quad (3)$$

где $|a|^2$ – вероятность обнаружить $|\psi\rangle$ в состоянии $|0\rangle$;

$|b|^2$ – вероятность обнаружить $|\psi\rangle$ в состоянии $|1\rangle$.

Кубит может находиться в бесчисленном множестве суперпозиций, но путём измерения из него можно извлечь только один бит классической информации. Так как измерение меняет состояние кубита, то оно не может быть измерено по двум различным базисам.

Эволюцию квантовой системы можно описать с помощью унитарного преобразования [3, 5]. Следствием унитарности квантовых преобразований является их обратимость. Таким образом, и квантовые вентили, реализующие эти преобразования, должны быть обратимыми.

В системе остаточных классов число А представляет собой набор остатков α_i, вычисленных по каждому из оснований p_i

$$A = (\alpha_1, \alpha_2, ..., \alpha_n),$$
$$\alpha_i = |A|_{p_i} = A - \left[\frac{A}{p_i}\right]\cdot p_i, \forall i \in [1, n]. \quad (4)$$

Если основания системы p_i взаимно попарно простые числа, то такое представление, согласно китайской теореме об остатках, единственное. Модель арифметики (алгебра) в СОК формально определяется как совокупность множества-носителя и сигнатуры (<R>,{+,–,x}), где

$$R = \prod_{i=1}^{n} p_i, \quad (5)$$

R – диапазон представления чисел в СОК;

{+,-,x} – множество модульных операций, распараллеливаемых в модулярной арифметике [1].

Таким образом, из выражения (5) видно, что используя представление числа А по основаниям, длина которых не превышает 5 разрядов, можно получить следующую верхнюю границу диапазона представления чисел в СОК.

$$L_{верх} = \prod_{i=1}^{n} p_i \ ,\ \forall p_i \le 2^5 - 1 \ . \quad (6)$$

Простые числа, не превышающие $2^5 - 1$: 2, 3, 5, 7, 11, 13, 17, 19, 23, 31.

Тогда $L_{верх} = 6915878970 \approx 6{,}91 \times 10^9$.

Для исключения переполнения при умножении значения операндов не должны превышать $\sqrt{L_{верх}}$. Тогда максимальная разрядность операндов составит $\log_2\left\lceil \sqrt{L_{верх}} \right\rceil \approx 16$.

Основной операцией модулярной арифметики является операция нахождения остатка числа по модулю.

Анализ преобразователей «позиционная система счисления» – «система остаточных классов», проведённый в [13], показывает, что оптимальным с точки зрения быстродействия и аппаратурных затрат является преобразователь из двоичной системы счисления в систему остаточных классов, реализующий следующее соотношение

$$\alpha_i = \sum_{i=1}^{n} 2^i \pmod{p_i}\ ,\ \forall i\ ,\ \text{для которых}\ \ a_i = 1\ ,$$

$$(a_n a_{n-1} ... a_i ... a_0)_2 = A\ . \quad (7)$$

В [5, 9] показано, что для обеспечения обратимости вычисления классической функции, преобразующей множество битов B^n во множество B^m, на квантовом компьютере вычисляется функция $F_\oplus$: $B^{n+m} \rightarrow B^{m+n}$, заданная соотношением

$$F_\oplus(x, y) = (x, y \oplus F(x)). \quad (8)$$

Тогда значение $F(x)$ можно получить следующим образом

$$F_\oplus(x, 0) = (x, F(x)). \quad (9)$$

В [14] описан алгоритм нахождения $(a \times b) \bmod p$. Условие обратимости этого алгоритма: НОД(b, p) = 1. Модификация алгоритма Шора для выражения (7) и b = 1 выглядит следующим образом.

$\gamma := 0$ ‘начальное значение γ ’

for i = 0 **to** n-1 ‘n – длина двоичного числа’

if $a_i = 1$ **then** ‘ a_i – значение i-того двоичного разряда’

$\gamma := \gamma + 2^i \pmod{p}$

end for

$\gamma := (\text{p-}\gamma) \bmod p$ ‘вычисление, обеспечивающее обратимость’

end.

Данный алгоритм преобразует (A, 0) в (A, γ), где $\gamma = -\alpha \bmod p = (p - \alpha) \bmod p$, a_i – коэффициенты двоичного представления числа А.

Рассмотрим пример. Пусть $A = 13_{10} = 1101_2$, p = 3. Тогда

$$\gamma = 3 - (8 \bmod 3 + 4 \bmod 3 + 1 \bmod 3) =$$
$$= -1 \bmod 3 = (3-1) \bmod 3 = 2.$$

Таким образом, предлагаемый алгоритм преобразует пару (13,0) в (13,2). Рассмотрим теперь преобразование (13,2) в (13,0) с использованием предлагаемого алгоритма.

Теперь начальное значение $\gamma = 2$

$$\gamma = 3 - (2 + 8 \bmod 3 + 4 \bmod 3 + 1 \bmod 3) = -3 \bmod 3 = 0 .$$

Чтобы вычислить остаток α на квантовом компьютере, сделаем следующие уточнения по вычислениям обратимых функций. Пусть на квантовом компьютере вычисляется функция $F_{\otimes}: B^{m+n} \to B^{m+n}$, заданная соотношением

$$F_{\otimes}(x, y) = (x, y \otimes F(x)) , \qquad (10)$$

где символ $\otimes$ означает тензорное произведение.

Тогда значение $F(x)$ можно получить следующим образом

$$F_{\otimes}(x,1) = (x, F(x)) . \qquad (11)$$

Используя выражения (10), (11) пару входных значений $(\gamma,1)$ можно преобразовать в пару (γ,α), где $\alpha = -\gamma \bmod p$, используя следующее выражение.

$$\alpha = \alpha \times \gamma \times (p-1) \bmod p . \qquad (12)$$

Пример для входной пары (2,1): $\alpha = 1 \times 2 \times (3-1) = 4 \bmod 3 = 1$, (2,1) → (2,1).

Пример для входной пары (1,1): $\alpha = 1 \times 1 \times (3-1) = 2 \bmod 3 = 2$, (1,1) → (1,2).

Проведем обратное преобразование для пары (1,2) $\alpha = 2 \times 1 \times (3-1) = 4 \bmod 3 = 1$.

Таким образом (1,2) → (1,1).

3. Реализация логических операций с помощью квантовых вентилей

Рассмотрим теперь, как реализовать операции в алгоритмах нахождения остатка с помощью квантовых вентилей: контролируемого отрицания (CNOT, C_{not}), и вентиля Тоффоли (CCNOT, $\Lambda_{\oplus}$) [5, 9].

Вентиль C_{not} задается следующей функцией

$$C_{not}(x, y) = \begin{cases} y, если\ x = 0 \\ \bar{y}, если\ x = 1 \end{cases} \qquad (13)$$

и имеет следующее графическое обозначение

Вентиль Тоффоли задаётся следующей функцией

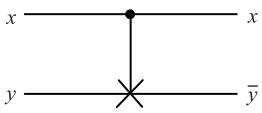

Рис. 1. Контролируемое НЕ

$$\Lambda_{\oplus}(x, y, z) = z \oplus x \wedge y = \begin{cases} x \wedge y, если\ z = 0 \\ x \oplus z, если\ y = 1 \\ x, если\ y = 1, z = 0 \\ \bar{z}, если\ x = y = 1, \end{cases} \qquad (14)$$

где символом $\oplus$ обозначается побитовое сложение по модулю 2, и имеет следующую схему

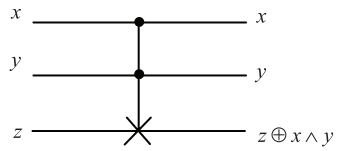

Рис. 2. Вентиль Тоффоли

Основная операция в первом вентиле – это сумма по модулю 2. Покажем, как её можно вычислить с помощью функций булевой алгебры.

Пусть значение суммы по модулю представлено k-разрядным однопозиционным двоичным числом, $S_{k-1}S_{k-2}...S_i...S_0$, где $k = p$. Каждый разряд суммы S_i принимает значение «1» в случае, если слагаемые образуют значение, такое, что

$$\langle a \rangle * \langle b \rangle \equiv i \bmod p , \qquad (15)$$

где операция * обозначает конкатенацию $\langle a \rangle$ и $\langle b \rangle$.

Иначе говоря, $S_i = 1$, когда $\langle a \rangle * \langle b \rangle$ принадлежит классу с номером i по модулю p.

Для модуля 5 и двухразрядных слагаемых значение разрядов S_i можно записать следующим образом.

$S_0 = 1$ для наборов $\langle a \rangle * \langle b \rangle \equiv 0 \bmod 5$: 0, 5, 10;

$S_1 = 1$ для наборов $\langle a \rangle * \langle b \rangle \equiv 1 \bmod 5$: 1, 6, 11;

$S_2 = 1$ для наборов $\langle a \rangle * \langle b \rangle \equiv 2 \bmod 5$: 2, 7, 12;

$S_3 = 1$ для наборов $\langle a \rangle * \langle b \rangle \equiv 3 \bmod 5$: 3, 8, 13;

$S_4 = 1$ для наборов $\langle a \rangle * \langle b \rangle \equiv 4 \bmod 5$: 4, 8, 14.

Тогда совершенная дизъюнктивная нормальная форма (СДНФ) для некоторых S_i и модуля p = 5 будет иметь вид

$$S_0 = \bar{a}_1\bar{a}_0\bar{b}_1\bar{b}_o + \bar{a}_1 a_0 \bar{b}_1 b_0 + a_1\bar{a}_0 b_1 \bar{b}_0$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \qquad (16)$$
$$S_4 = \bar{a}_1 a_0 \bar{b}_1\bar{b}_0 + a_1\bar{a}_0\bar{b}_1\bar{b}_0 + a_1 a_0 b_1 \bar{b}_0$$

Чтобы избежать неэкономичного однопозиционного представления результата суммирования по модулю, рассмотрим n-разрядное двоичное число, $S_{n-1}S_{n-2}...S_i...S_0$, где $n = \lceil \log_2 p \rceil$. Разряды S_i будут равны «1» при выполнении следующего условия

$$\langle a \rangle * \langle b \rangle \equiv 2^i \bmod p . \qquad (17)$$

Но теперь однопозиционным n-разрядным кодом мы можем представить только $p - n + 1$ классов. Так, для модуля 5: $n = 3$ и возможно представить только 3 класса.

$S_0 = 1$ для наборов $2^0 = 1$ $\langle a \rangle * \langle b \rangle \equiv 1 \bmod 5$: 1, 6, 11;

$S_1 = 1$ для наборов $2^1 = 2$ $\langle a \rangle * \langle b \rangle \equiv 2 \bmod 5$: 2, 7, 12;

$S_2 = 1$ для наборов $2^2 = 4$ $\langle a \rangle * \langle b \rangle \equiv 4 \bmod 5$: 4, 9, 14.

Класс «3» можно представить как дизъюнкцию S_0 и S_1. Тогда значения S_0 и S_1 можно переписать следующим образом.

$$\begin{aligned} S_o^{'} &= S_0 \vee S_1 \\ S_1^{'} &= S_1 \vee S_0 \end{aligned} \qquad (18)$$

Представление разрядов S_i с помощью дизъюнктивных нормальных форм для модуля 5 будет иметь вид

$$\begin{aligned} S_0 &= \overline{a}_1\overline{a}_0\overline{b}_1b_0 + \overline{a}_1a_0b_1\overline{b}_0 + a_1a_0\overline{b}_1b_0 \\ S_1 &= \overline{a}_1\overline{a}_0b_1\overline{b}_0 + \overline{a}_1a_0b_1b_0 + a_1a_0b_1\overline{b}_0 \\ S_0^{'} &= S_0 + S_1 \\ S_1^{'} &= S_1 + S_0 \\ S_2 &= \overline{a}_1a_0\overline{b}_1\overline{b}_0 + a_1\overline{a}_0\overline{b}_1b_0 + a_1a_0b_1\overline{b}_0 \end{aligned} \qquad (19)$$

Так выходы представлены с помощью СДНФ, в которых ни одна из элементарных конъюнкций не принадлежит классу «0», то отдельная логическая функция для этого класса не нужна.

Реализация операции умножения по модулю, которая является основной во втором вентиле, осуществляется аналогично операции суммирования.

Реализуем теперь S_2 из выражения (19) с помощью вентилей Тоффоли.

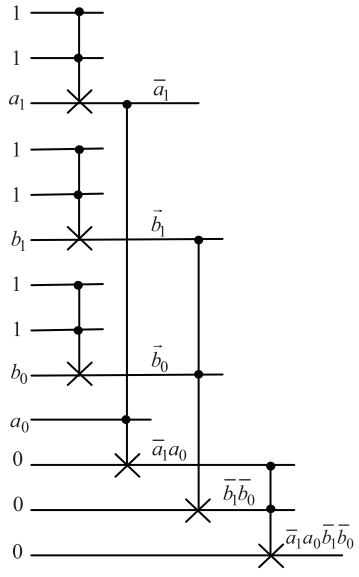

Рис. 3. Реализация элементарной конъюнкции с помощью вентиля Тоффоли

Дизъюнкцию с помощью вентиля Тоффоли можно реализовать следующим образом.

$$\overline{x_1x_2} = \overline{x}_1 \vee \overline{x}_2 \Rightarrow \overline{\overline{x}_1\overline{x}_2} = x_1 \vee x_2 \,. \qquad (20)$$

Отсюда

$$\Lambda_{\oplus}(1,1,\Lambda_{\oplus}(\Lambda_{\oplus}(1,1,x_1),\Lambda_{\oplus}(1,1,x_2),0)) \equiv x_1 \vee x_2. \qquad (21)$$

Схематически реализация дизъюнкции двух конъюнкций из выражения (19) для S_2 с помощью выражения (21) приведена на рис. 4.

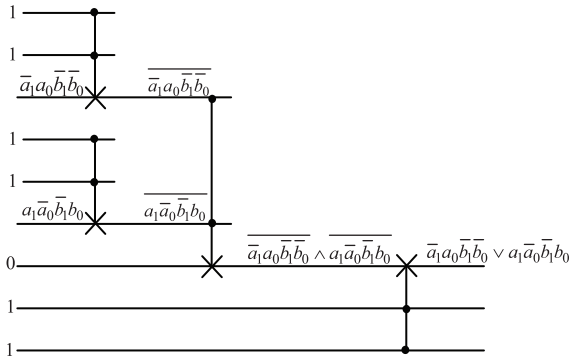

Рис. 4. Реализация элементарной дизъюнкции с помощью вентиля Тоффоли

Рассмотрим теперь реализацию дизъюнкции с помощью унитарных операторов, описывающих вентиль Тоффоли. Матрица унитарного преобразования, описывающая оператор Тоффоли в пространстве базисных состояний 3-х кубитов, определяется на основании следующего равенства [9]

$$\Lambda_{\oplus} = |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes C_{not}\,, \qquad (22)$$

где I – оператор тождественного преобразования,

$$I = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{matrix} |0\rangle & \rightarrow & |0\rangle \\ |1\rangle & \rightarrow & |1\rangle \end{matrix}, \qquad (23)$$

$$C_{not} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X\ , \qquad (24)$$

X – оператор отрицания

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{matrix} |0\rangle & \rightarrow & |1\rangle \\ |1\rangle & \rightarrow & |0\rangle \end{matrix}, \qquad (25)$$

и выглядит следующим образом

$$\Lambda_{\oplus} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Пусть $x_1 = |0\rangle$, $x_2 = |1\rangle$. Найдём с помощью $\Lambda_{\oplus}$ значение $x_1 \vee x_2$. Для этого определим инверсии элементов $\overline{x}_i = \Lambda_{\oplus}(1,1,x_i)$. В трехкубитном базисе аргументы $\Lambda_{\oplus}$ будут выглядеть следующим образом $|110\rangle$, $|111\rangle$; а векторы, соответствующие этим куби-

там, выглядят так $(0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0)^T$, $(0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1)^T$.

Тогда

$\Lambda_\oplus \times x_1 = (0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1)^T \Rightarrow \overline{x}_1 = |1\rangle$;

$\Lambda_\oplus \times x_2 = (0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0)^T \Rightarrow \overline{x}_2 = |0\rangle$.

Следующий этап – вычисление конъюнкции инверсий x_1 и x_2

$$\overline{x}_1 \wedge \overline{x}_2 = \Lambda_\oplus(\overline{x}_1, \overline{x}_2, 0)$$

Аргумент для $\Lambda_\oplus$ при $\overline{x}_1 \wedge \overline{x}_2$ вычислении имеет вид $|100\rangle$ и в векторном виде $(0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0)^T$. С учётом выражения (14) $\overline{x}_1 \wedge \overline{x}_2 = |0\rangle$. Проинвертируем полученную конъюнкцию, и получим искомый результат.

$x_1 \vee x_2 = \Lambda_\oplus(1,1,\overline{x}_1 \wedge \overline{x}_2)$. Аргумент вентиля Тоффоли для данного конкретного случая будет иметь вид $|110\rangle$, или в векторном виде $(0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0)^T$. Окончательный результат: $x_1 \vee x_2 = |1\rangle$.

4. Заключение

В данной работе рассмотрены вопросы расширения диапазона обрабатываемых данных в квантовых компьютерах путём применения системы остаточных классов, построен обратимый алгоритм нахождения остатка по модулю и рассмотрены структуры квантовых вентилей, реализующих вычисления $\sum \bmod p$. Показаны варианты реализаций этих вентилей в базисе $(-, \Lambda_\oplus)$.

ЛИТЕРАТУРА

1. Акушский И.Я., Юдицкий Д.М., Машинная арифметика в остаточных классах. – М.: Советское радио, 1968. – 440 с.
2. Валиев К.А., Кокин А.А. Квантовые компьютеры: надежды и реальность. Ижевск: R&C Dynamics, 2001. – 351 с.
3. Дирак П. Принципы квантовой механики. http://lib.edu.kzn.ru/library/book/15482.html?print#
4. Жувикин Г. Нанокомпьютеры // Компьютерра. – 2005. – №2
5. Китаев А., Шень А., Вялый М. Классические и квантовые вычисления. М.: МЦМНО ЧеРо, 1990. – 192 с.
6. Малашевич Б. К 75-летию Давлета Исламовича Юдицкого. http://kis.pcweek.ru/Year2004/N33/CP1251/Opinions/chapt3.htm
7. Малашевич Б. Неизвестные модулярные суперЭВМ. http://www.computer-museum.ru/histussr/sok_evm.htm
8. Перискил Дж. Квантовые вычисления: за и против// В кн. Квантовые вычисления: за и против. Под ред. В. А. Садовничего. – Ижевск: Издательский дом «Удмуртский университет», 1999. – 212 с.
9. Рифель Е., Полак В. Основы квантовых вычислений // Квантовый компьютер и квантовые вычисления. – 2000. – т. 1, №1 с. 4-57
10. Скробов А. Закон Мура http://cs.usu.edu.ru/study/moore/
11. Федичкин Л.Квантовые компьютеры //Наука и жизнь. – 2001 – №1
12. Холево А. С. Введение в квантовую теорию информации. М.: МЦНМО, 2002. – 228 с.
13. Червяков Н.И., Ряднов С.А., Сахнюк П.А., Шапошников А.В., Модулярные параллельные вычислительные структуры нейропроцессорных систем. – М.: ФИЗМАТЛИТ, 2003. – 288 с.
14. Шор П.В. Полиномиальные по времени алгоритмы разложения числа на простые множители и нахождения дискретного логарифма для квантового компьютера // Квантовые компьютеры и квантовые вычисления. – 1999. – №2

Ремизов Сергей Леонидович

кандидат технических наук, старший преподаватель военной кафедры СибГУТИ тел. (383) 269-82-97, e-mail: micnatserg@rambler.ru

Шелудяков Алексей Борисович

студент гр. П-42 СибГУТИ тел. 89139352006, e-mail: aleksey04@mail.ru