УДК 004.31, 538.945, 530145

А.К. БЕЛЯЕВ, В.П. КЛИМЕНКО

АНАЛИЗ МОДЕЛИ КВАНТОВЫХ ВЫЧИСЛЕНИЙ

Abstract: *In a brief abstract review an analysis over of quantum model of calculations is brought in classic presentation and in geometrical algebra. As a result of analysis the possibility of presentation of quantum model of calculations is shown in the symmetric group of transformations, particularly in the system of transformations defined on an abstract p-positional register.*

Key words: *quantum computations, quantum geometric algebra, quantum algorithms, quantum computing models, quantum register, abstract* p *-positional register.*

Анотація: *У стислому реферативному огляді наведено аналіз квантової моделі обчислень у класичному уявленні та в геометричній алгебрі. В результаті аналізу показано можливість представлення квантової моделі обчислень у симетричній групі перетворень, зокрема, в системі перетворень, визначеній на абстрактному p-позиційному регістрі. Приводиться оцінка порядку повної групи двокубітових квантових перетворень.*

Ключові слова: *квантові обчислення, квантова геометрична алгебра, квантові алгоритми, квантові моделі обчислень, квантовий регістр, абстрактний* p *-позиційний регістр.*

Аннотация: *В кратком реферативном обзоре приводится анализ квантовой модели вычислений в классическом представлении и геометрической алгебре. В результате анализа показана возможность представления квантовой модели вычислений в симметрической группе преобразований, в частности, в системе преобразований, определенной на абстрактном p-позиционном регистре. Приводится оценка порядка полной группы двухкубитовых квантовых преобразований.*

Ключевые слова: *квантовые вычисления, квантовая геометрическая алгебра, квантовые алгоритмы, квантовые модели вычислений, квантовый регистр, абстрактный* p *-позиционный регистр.*

1. Введение

С развитием новых информационных технологий возрастающие объемы и сложность решения задач требуют наличия адекватных вычислительных средств: сверхвысокой производительности, надежности, малых габаритов и потребляемой энергии.

Традиционные методы вычислений, основанные на классических моделях и существующей элементной базе, уже не могут удовлетворить возрастающие потребности вычислений. Это приводит к поиску и разработке новых логических и физических принципов, основанных на фундаментальных законах физики взаимодействия элементов на атомном уровне. Квантовая механика и квантовые вычисления являются одними из таких направлений вычислений.

В настоящее время работы по квантовым вычислениям ведутся практически во всех промышленно развитых странах [1]. Так, в Европейском Союзе и США [2, 3] разработаны и выполняются подробные дорожные карты в области квантовых вычислений. Ускорение этих исследований произошло в результате открытия квантовых алгоритмов решения задач [4], практически не решаемых с применением традиционных вычислительных средств. Кроме того, появление нового алгебраического аппарата – геометрической алгебры [5] существенно сблизило квантовую механику и вычисления, расширило представления об их взаимодействии.

В качестве физической основы для квантовых вычислений предложены различные физические явления и эффекты [6]. Однако наиболее перспективным считается направление, представляющее сверхпроводящие цепи с Джозефсоновскими контактами. Так, Джозефсоновские кубиты (квантовые биты) представляют собой макроскопическую квантовую двухуровневую систему, и их экспериментальная реализация доступна современному уровню развития микротехнологии [7, 8].

2. Анализ классической квантовой модели вычислений

Квантовые вычисления определяются постулатами квантовой механики. Рассмотрим некоторые из них.

1. Состояния изолированной квантовой системы описываются единичным вектором в конечномерном гильбертовом пространстве H_n состояний. Это комплексное пространство со скалярным произведением, элементы ортонормированного базиса которого образуют вычислительный базис [6]. Так, для описания состояний простейшей двухуровневой системы – кубита в пространстве H_2 выбирается ортонормированный вычислительный базис $|0>$ и $|1>$ – кэт векторов (в обозначениях Дирака). В матричной записи базисные векторы соответствуют матричным столбцам $|0>=\begin{pmatrix}1\\0\end{pmatrix}$, а $|1>=\begin{pmatrix}0\\1\end{pmatrix}$. Тогда скалярные произведения базисных векторов равны соответственно $<0|0>=<1|1>=1$ и $<0|1>=<1|0>=0$. Произвольное векторное состояние записывается в виде суперпозиции базисных состояний $|\varphi>=a|0>+b|1>$ и $|a|^2+|b|^2=1$, где $a,b\in \mathrm{H}_2$ – комплексные числа; $|a|^2$ и $|b|^2$ представляют собой вероятности измерения состояний $|0>$ и $|1>$ соответственно.

Для двухкубитовой системы в пространстве H_4 произвольный вектор также представляется в виде суперпозиции состояний ортонормированного вычислительного базиса и имеет вид

$$|\varphi>=a|00>+b|01>+c|10>+d|11> \text{ и } |a|^2+|b|^2+|c|^2+|d|^2=1,$$

где $a,b,c,d\in \mathrm{H}_4$ – комплексные числа, $|a|^2$, $|b|^2$, $|c|^2$ и $|d|^2$ – представляют собой вероятности измерения состояний $|00>,|01>$, $|10>$ и $|11>$ соответственно. Элементы вычислительного базиса в матричной записи имеют вид

$$|00>=\begin{pmatrix}1\\0\\0\\0\end{pmatrix}, |01>=\begin{pmatrix}0\\1\\0\\0\end{pmatrix}, |10>=\begin{pmatrix}0\\0\\1\\0\end{pmatrix}, |11>=\begin{pmatrix}0\\0\\0\\1\end{pmatrix}.$$

Таким образом, суперпозиция состояний представляется основным свойством квантовой системы и охватывает как всю систему, так и отдельные ее элементы. Поэтому суперпозиция состояний – источник параллелизма квантовых вычислений.

2. Эволюция замкнутой системы на временном интервале описывается унитарным преобразованием $|\psi>=U|\varphi>$, здесь $|\psi>$ и $|\varphi>$ – векторы состояния системы, а U – унитарное преобразование. В матричном представлении, если U – унитарно, то $U^{-1}=(\overline{U})^{I}$, где U^{-1} – обратная матрица, а $(\overline{U})^{I}$ – трансформированная комплексно сопряженная матрица. Определитель унитарной матрицы – единица.

Отсюда следует, что эволюция квантовой системы описывается обратимыми преобразованиями.

Множество унитарных преобразований бесконечно. Однако, с некоторым приближением, квантовые преобразования над конечным множеством кубитов можно представлять элементами некоторого универсального конечного набора преобразований (вентилей) [9]. В [6] описываются возможные наборы квантовых вентилей для различных применений. Таким образом, модель квантовых вычислений представляется в виде набора квантовых схем. Рассмотрим состав некоторого стандартного универсального набора вентилей [6], предназначенного для аппроксимации произвольных унитарных операторов.

Это однокубитовые элементы Адамара – H, сдвига фазы – S, $\pi/8$ – T и двухкубитовый оператор $CNOT$. В матричном представлении эти элементы имеют вид

$$H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix};\; S=\begin{bmatrix}1 & 1\\ 0 & i\end{bmatrix};\; T=\begin{bmatrix}1 & 1\\ 0 & \exp(i\pi/4)\end{bmatrix}.$$

Элемент $CNOT$ используется как в классических, так и в квантовых вычислениях. Функционально элемент представляет управляемое NOT, т.е. условную инверсию. В матричном представлении элемент $CNOT$ имеет вид

$$CNOT=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}.$$

Эта подстановочная матрица элементов соответствующей группы подстановочных преобразований [11], которая изоморфна симметрической группе перестановок. Таким образом, элементу $CNOT$ соответствует некоторая транспозиция симметрической группы перестановок.

В настоящее время показано [10], что минимальный набор квантовых элементов образуется элементами двух типов: однокубитового преобразования Адамара (H) и элемента Тоффоли (CCN) – трехкубитового оператора. Это универсальный вычислительный набор преобразований квантовой системы.

Матричное представление элемента Тоффоли имеет вид

$$CCN=\left[\begin{array}{c|c}\begin{matrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{matrix} & 0\\ \hline 0 & \begin{array}{c|c}\begin{matrix}1 & 0\\ 0 & 1\end{matrix} & 0\\ \hline 0 & \begin{matrix}0 & 1\\ 1 & 0\end{matrix}\end{array}\end{array}\right].$$

Квантовые элементы Тоффоли также представляются подстановочными матрицами [11] и соответствуют некоторым транспозициям симметрической группы. Элемент Тоффоли – условный оператор инверсии состояния кубита при выполнении условия совпадения состояний ($|11>$) двух других кубитов. С другой стороны, элементы Тоффоли в виде транспозиций состояний могут независимо образовывать функционально полный набор обратимых базовых преобразований (микроопераций) абстрактного n-разрядного двоичного регистра [12].

Таким образом, наличие преобразования Адамара в системе образующих определяет квантовую природу преобразований и их представление в общей системе квантовых преобразований.

3. Анализ модели квантовых вычислений в геометрической алгебре

Геометрическая алгебра $\mathbf{G_n}$ [5,13] – это некоторое ассоциативное исчисление, построенное на основе эвклидовых пространств. Элементы алгебры – это скаляры, векторы, бивекторы, n-векторы (элементы ранга 0, 1, 2,.. n соответственно). С каждым элементом отождествляется некоторый геометрический объект.

Элементы алгебры обладают свойством сложения, образуя подклассы, замкнутые по определенному рангу элементов. Операция умножения (геометрическое произведение) ассоциативна, дистрибутивна, антикоммутативна. Квадрат любого вектора – скалярная величина.

Операция сложения выражает одновременное возникновение событий, а произведение – механизм изменения операторов.

В качестве дополнительного постулата модели принято условие совместного возникновения и исключения. Это означает, что простое состояние и его инверсия не могут логически произойти в один и тот же момент времени. Постулат описывается выражением

$$\mathbf{a}+\overline{\mathbf{a}}=\mathbf{a}+(\mathbf{-a})=0 \quad \text{или} \quad (\mathbf{b}+\overline{\mathbf{c}})+(\overline{\mathbf{b}}+\mathbf{c})=0\,. \qquad (1)$$

Это основное соотношение обоснования вычислений квантовой модели в геометрической алгебре.

Как рассматривалось в предыдущем разделе, кубитовые состояния определяются в Гильбертовом пространстве в виде суммы двух комплексных чисел. Топологически такое представление эквивалентно четырехмерному действительному пространству. В качестве физического примера кубита может быть рассмотрена спин-частица ($\frac{1}{2}$), которая принимает два базисных состояния: спин-вверх (используется обозначение $|\uparrow>$ или $|0>$) и спин-вниз (обозначается $|\downarrow>$ или $|1>$). Эти базисы могут наблюдаться и представлять классическое (не суперпозиционное) битовое состояние.

Основываясь на таком представлении кубита, его можно описать в геометрической алгебре. Состояние кубита кодируется двумя битовыми векторными состояниями, которые могут произойти одновременно. Они представляются в виде двух базисных ортонормированных векторов $\{\mathbf{a0}, \mathbf{a1}\}$, порождающих геометрическую алгебру $\mathbf{G_2}$. Принцип совместного возникновения и исключения (1) и алгебра $\mathbf{G}_2$ дают возможность определить состояния кубита в виде суммы независимых векторов в $\mathbf{G}_2^-$ ($\mathbf{G}_2^-$ – подкласс одноранговых векторов).

$$\text{Кубит } A = (\pm\mathbf{a0} \pm \mathbf{a1}).$$

Векторное множество в $\mathbf{G}_2$ порождает линейное пространство размерностью $N = 2^2 = 4$ и содержит элементы $\{\pm1, \mathbf{a0}, \mathbf{a1}, \mathbf{a0a1}\}$, где $\mathbf{a0a1}$ – геометрическое произведение векторов, бивектор или псевдоскаляр. Размерность этого пространства точно соответствует H_2.

Как показано в [14], четыре возможных варианта знаков в сумме, представляющей кубит, обозначают состояния: $A_0 = +\mathbf{a0} - \mathbf{a1}$, $A_1 = -\mathbf{a0} + \mathbf{a1}$, $A_- = -\mathbf{a0} - \mathbf{a1}$, $A_+ = +\mathbf{a0} + \mathbf{a1}$. Размещение векторов на плоскости представлено на рис. 1.

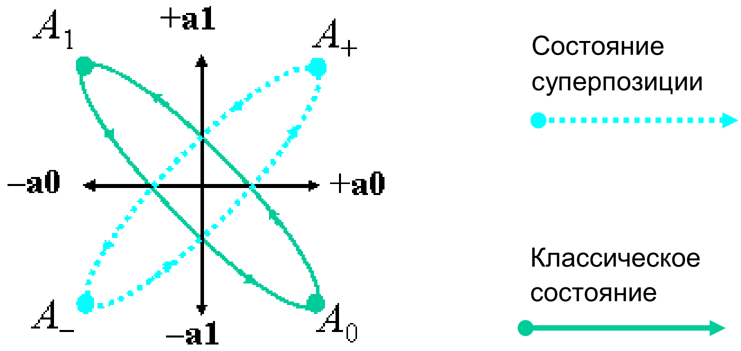


Рис. 1. Векторы и состояния для кубита $A = (\pm\mathbf{a0} \pm \mathbf{a1})$

Значения сумм векторов вычисляются по правилам арифметики по $\mathrm{mod}\,3$ и анализа условия (1). Это линейная операция. Очевидно, что $A_0 + A_1 = 0$ и $A_0 = -A_1$, а также $A_- + A_+ = 0$ и $A_- = -A_+$. Состояния A_0, A_1 и состояния A_-, A_+ – попарно коллинеарные векторы, сами же пары взаимно ортогональны. Состояния A_0, A_1 реализуются антисимметричными суммами и представляют классические состояния. Состояния A_-, A_+ реализуются симметричными суммами и представляют суперпозиционные состояния. Эти бимодулярные результаты представлены в табл. 1. Это модель двухфазового кубита в геометрической алгебре.

Таблица 1. Таблица бимодулярных результатов сложения базовых векторов

Способ фазирования	Состояние кубита	Значения состояния		Гильбертово состояние
Антисимметричные состояния – **классические**	$A_0 = +\mathbf{a0} - \mathbf{a1}$	**a0** *ON*	**a1** *OFF*	$1\,\vert 0> +0\,\vert 1>=\vert 0>$
	$A_1 = -\mathbf{a0} + \mathbf{a1}$	**a0** *OFF*	**a1** *ON*	$0\,\vert 0> +1\,\vert 1>=\vert 1>$
Симметричные состояния – *суперпозиционные*	$A_+ = +\mathbf{a0} + \mathbf{a1}$	**a0** *ON*	**a1** *ON*	$\frac{1}{\sqrt{2}}(\vert 1> + \vert 0>)$
	$A_- = -\mathbf{a0} - \mathbf{a1}$	**a0** *OFF*	**a1** *OFF*	$\frac{1}{\sqrt{2}}(\vert 1> - \vert 0>)$

На плоскости, заданной состояниями $\bar{\mathbf{G}}_2 = \{\mathbf{a0}, \mathbf{a1}\}$, определяется псевдоскаляр $\mathbf{S_A} = (\mathbf{a0}, \mathbf{a1})$, действующий подобно спинору (т.е. преобразованию Адамара) на этой плоскости [14]. Спинор работает независимо на каждом векторе суммы. Нужно отметить, что геометрическая алгебра не содержит комплексных чисел и аппарата алгебры матриц; однако, они могут быть интерпретированы в геометрической алгебре.

В табл. 2 представлено спинорное действие по переключению классических и суперпозиционных состояний. Для вычисления состояний используется антикоммутативное свойство геометрического произведения.

Таблица 2. Спинорное переключение классических и суперпозиционных состояний

Исходная фаза	Исходное состояние кубита	Вариант спинора	Конечное состояние кубита	Конечная фаза
Классичес-кое	$+\mathbf{a0} - \mathbf{a1}$	$+\mathbf{a0}(\mathbf{a0a1}) = +\mathbf{a1}$	$+\mathbf{a0} + \mathbf{a1}$	*Супер-позиционное*
	$-\mathbf{a0} + \mathbf{a1}$	$-\mathbf{a0}(\mathbf{a0a1}) = -\mathbf{a1}$	$-\mathbf{a0} - \mathbf{a1}$	
Супер-позиционное	$+\mathbf{a0} + \mathbf{a1}$	$+\mathbf{a1}(\mathbf{a0a1}) = -\mathbf{a0}$	$-\mathbf{a0} + \mathbf{a1}$	**Классичес-кое**
	$-\mathbf{a0} - \mathbf{a1}$	$-\mathbf{a1}(\mathbf{a0a1}) = +\mathbf{a0}$	$+\mathbf{a0} - \mathbf{a1}$	

Таким образом, приведенные построения показывают, что представление кубита в геометрической алгебре позволяет кодировать состояние двухфазового кубита битовыми состояниями. Дальнейшая отработка модели вычислений в геометрической алгебре связана с представлением квантового регистра в виде геометрического произведения кубитов [14].

4. Представление преобразований двухфазового кубита в симметрической группе преобразований

Анализ квантовых вычислений, представленных векторными состояниями в классической квантовой модели и геометрической алгебре, показывает, что преобразования кубита могут быть сведены к преобразованиям на конечных множествах состояний.

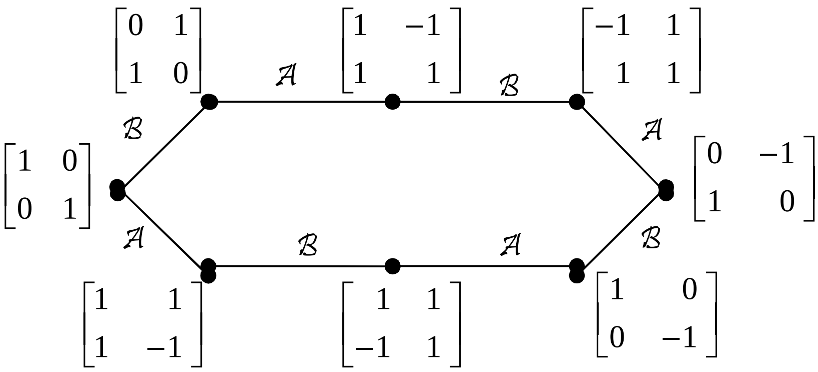
Известные наборы операторов кубита включают оператор Адамара $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ и оператор инверсии классического состояния или состояния разряда классического регистра: $NOT = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Операторы Адамара и NOT образуют группу унитарных преобразований в пространстве H_2.

С точностью до числового множителя эта унитарная группа матриц может быть представлена некоторой конечной группой матричных преобразований $\mathcal{G}$. Элементы такой группы

ISSN 1028-9763. Математичні машини і системи, 2009, № 2

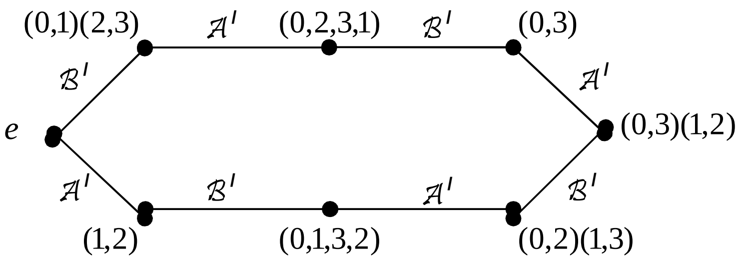
изображены на диагр. 1. Группа порождается образующими $\{\mathcal{A},\mathcal{B}\}$, где $\mathcal{A} = |H| = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, а $\mathcal{B} = |NOT| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Вершины на диаграмме отмечены матричными элементами группы, а ребра отмечены образующими группы. Порядок группы $p = 8$.

Процесс порождения в системе образующих $\{\mathcal{A},\mathcal{B}\}$ проводится в соответствии с методикой [12]. На каждом шаге учитываются только новые элементы. Исходный элемент в системе порождения – тождественное преобразование $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.



Диагр. 1. Элементы группы $\mathcal{G}$

Группе $\mathcal{G}$ может быть поставлена в соответствие некоторая изоморфная ей подгруппа $\mathcal{G}'$ симметрической группы перестановок степени 4 (перестановок четырех состояний: 0, 1, 2, 3). Пример такой подгруппы $\mathcal{G}'$ приведен на диагр. 2. $\{\mathcal{A}',\mathcal{B}'\}$ – система образующих группы $\mathcal{G}'$; здесь $\mathcal{A}' = (1,2)$ и $\mathcal{B}' = (0,1)(2,3)$ (образующие представлены транспозициями). Это инволютивные преобразования, т.е. $(\mathcal{A}')^2 = e$ и $(\mathcal{B}')^2 = e$, где e – единица симметрической группы.



Диагр. 2. Элементы группы $\mathcal{G}'$

С другой стороны, перестановки симметрической группы преобразований описывают преобразования информационных множеств состояний абстрактных операционных устройств [15].

Перестановки, соответствующие преобразованиям двухфазового кубита, преобразуют двоичные переменные двухразрядного операционного устройства. Тогда, в соответствии с [12], перестановки $(0,1)(2,3)$ и $(0,2)(1,3)$ соответствуют инверсиям двоичных переменных, а перестановка $(1,2)$ – обмену этих двоичных переменных, выполняя функции преобразования Адамара. Так, например, для инверсий двоичных переменных выполняется соотношение $(1,2)(0,1)(2,3)(1,2) = (0,2)(1,3)$.

Таким образом, устанавливается взаимно однозначное соответствие преобразований двухфазового кубита и преобразований абстрактного p-позиционного операционного устройства, состояния которого преобразуются в соответствии с логикой преобразования кубита. Поэтому квантовая система на основе кубитов может описываться абстрактным p-позиционным регистром.

Построение преобразований на кубитах сводится к построению конечных симметрических групп преобразований. Так, для двухкубитовой системы порядок соответствующей полной группы преобразований оценивается количеством 322560 элементов.

5. Выводы

В кратком реферативном обзоре приведен анализ квантовой модели вычислений в классическом представлении и на основе геометрической алгебры. В геометрической алгебре также описывается модель двухфазового кубита. На основе проведенного анализа квантовой модели вычислений предложено представление двухфазового кубита в симметрической группе преобразований. В этом случае кубит представляется абстрактным p-позиционным операционным устройством и соответствующей группой преобразований. Таким образом, полученные представления позволяют снизить сложность построения квантовой модели вычислений и упростить ее анализ.

СПИСОК ЛИТЕРАТУРЫ

1. Research in Quantum Computing and Information // http://www.vcpc.univie.ac.at/~ian/hotlist/qc/research.shtml.
2. ERA Pilot Roadmap – Quantum Information Sciences and Technologies. – 2006 // http://qist.ect.it/reports/reports.htm .
3. Quantum Computation Roadmap. – 2004 // http://qist.lanl.gov/qcomp_map.shtml .
4. Rieffel E., Polak W. An Introduction to Quantum Computing for Non-Physicists // arXiv:quant-ph/9809016v2 19 Jan 2000. – 2000 // http://xxx.lanl.gov/pdf/quant-ph/9809016v2 .
5. Macdonald A. A Survey of Geometric Algebra and Geometric Calculus // http://faculty.luther.edu/~macdonal/GA&GC.pdf .
6. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. – М.: Мир, 2006. – 823 с.
7. Омельянчук А.Н., Оболенский М.А. Квантовые компьютеры и джозефсоновские кубиты // Университеты: наука и просвещение / Харьковский национальный университет. – Харьков: Империал, 2005. – № 2(22) – С.10 – 17; № 3 (23). – С. 12 – 19.
8. Войтович І.Д., Корсунський В.М. Перспективи квантових обчислень з використанням надпровідності // Математичні машини і системи. – 2008. – № 4. – С. 23 – 56.
9. Китаев А. и др. Классические и квантовые вычисления / А. Китаев, А. Шень, М. Вялый. – М.: МЦНМО, 1999. – 192 с.
10. Aharonov D. A Simple Proof that Toffoli and Hadamard are Quantum Universal // arXiv:quant-ph/0301040 9 Jan 2003. – 2003 // http://arxiv.org/pdf/quant-ph/0301040v1.
11. Калужнин А.А. Введение в общую алгебру. – М.: Наука, 1973. – 447 с.
12. Беляев А.К. Базовая система микроопераций и ее применение // Кибернетика. – 1972. – № 2. – С. 71 – 76.
13. Matzke D. Quantum computation using geometric algebra // http://www.utdallas.edu/~cantrell/matzke.pdf .
14. Matzke D. Quantum Geometric Algebra // http://www.matzkefamily.net/doug/papers/ANPA24/QuantumGeometricAlgebra.pdf .
15. Глушков В.М. Кибернетика, вычислительная техника, информатика: Избр. тр. в 3 т. – Киев: Наукова думка, 1990. – Т. 1. – С. 179 – 191.

Стаття надійшла до редакції 22.01.2009