Научная статья
УДК 004.27:004.056.55

Комбинированный подход к моделированию квантового алгоритма Дойча

Александр Сергеевич Горский

Аннотация. Статья посвящена исследованию существующих и разработке нового комбинированного подходов к моделированию квантового алгоритма Дойча на классическом компьютере. Актуальность рассматриваемой тематики связана с разработкой комбинированного подхода, который в отличие от известных позволяет повысить вероятность получения правильного результата при различных сочетаниях входного двухкубитного регистра.

Ключевые слова: квантовый алгоритм Дойча; кубит; матричный оператор; квантовая схема; тензорное произведение; имитационная модель; пользовательская функция

Для цитирования: Горский А.С. Комбинированный подход к моделированию квантового алгоритма Дойча // Вооружение и экономика. 2024. №1(67). С. 40-48.

Original article

A Combined Approach to the Deutsch Quantum Algorithm Modeling

Aleksandr S. Gorskij

Abstract. The article is devoted to the study of existing and development of a new combined approach to the Deutsch quantum algorithm modeling on a classical computer. The relevance of the research under consideration is associated with a combined approach development that unlike the known ones makes it possible to increase the probability of the correct answer obtainment for various combinations of the input two-qubit register.

Keywords: quantum Deutsch algorithm; qubit; matrix operator; quantum circuit; tensor product; simulation model; custom function

For citation: Gorsky A.S. A Combined Approach to the Deutsch Quantum Algorithm Modeling // Armament and Economics. 2024. No.1(67). P. 40-48.

Введение

Бурное развитие технологии квантовых вычислений по всему миру в последнее время связано, прежде всего, с технологически непреодолимым барьером по миниатюризации электронной компонентной базы (ЭКБ), используемой в существующих электронно-вычислительных машинах (ЭВМ). Вычислительная мощность современных компьютеров растет в соответствии с законом Мура, согласно которому каждые два года количество транзисторов на интегральной схеме увеличивается вдвое. Ввиду этого обстоятельства размеры транзисторов приблизились к размеру атома, из-за чего на их работе сказываются квантовые эффекты. Другой причиной, стимулирующей исследования в данной области, является вычислительный барьер по производительности классических компьютеров при решении полиноминально сложных задач. Неизбежно возникает противоречие между ростом объема вычислений и уменьшением размеров ЭКБ, которое заключается в том, что невозможно бесконечно повышать плотность элементов на кристалле процессора без увеличения массогабаритных размеров ЭВМ. Одним из возможных способов его разрешения является создание квантового компьютера.

Квантовые компьютеры – это устройства, которые используют для вычислений принципы квантовой механики. Для некоторых задач квантовые алгоритмы обеспечивают существенное ускорение по сравнению с их лучшим классическим аналогом. Проблемами создания квантового компьютера в настоящее время занимается большое количество ученых во всем мире, в том числе и в нашей стране. В июле 2019 года госкорпорацией «Росатом» совместно с другими заинтересованными организациями была разработана «Дорожная карта развития высокотехнологичной области «Квантовые вычисления», в рамках которой

к 2024 году запланировано создание отечественного квантового компьютера с объемом входного регистра до 100 кубитов[1].

Применение технологии квантовых вычислений предусмотрено соответствующими документами по развитию квантовых технологий в интересах силовых министерств и ведомств, в том числе и Минобороны России.

Несмотря на уже существующие коммерческие модели квантового компьютера, он по-прежнему остаётся труднодоступным для проведения исследований в силу высокой цены и требовательных эксплуатационных характеристик. Этим объясняется востребованность имитационных моделей, с помощью которых стало возможным на классических компьютерах разрабатывать, изучать и симулировать работу квантовых алгоритмов.

1. Теоретические аспекты технологии квантовых вычислений

Фундаментальным понятием в области квантовых вычислений и квантовой информации является квантовый бит или кубит. Классический бит может в любой момент находиться только в одном из булевых состояний – 0 или 1 с вероятностями либо $P(0) = 1$, либо $P(1) = 1$. Кубит в отличие от него находится в квантовой суперпозиции этих двух базисных состояний, которая описывается вектором в двумерном комплексном векторном (гильбертовом) пространстве. Вектор состояния кубита имеет две компоненты, которые являются его проекциями на базисы гильбертова пространства и представляют собой комплексные числа, и в обозначениях Дирака записывается в виде:

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

где α и β – комплексные числа (амплитуды вероятности), удовлетворяющие условию нормировки $|\alpha|^2 + |\beta|^2 = 1$, $|\alpha|^2$ и $|\beta|^2$ являются вероятностями нахождения кубита в состояниях, описываемых вектор-столбцами $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ и $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$ соответственно.

Квантовый компьютер является многокубитовым вычислительным устройством, в котором система из нескольких кубитов образует квантовый регистр. В классическом компьютере в каждый момент регистр имеет четкую последовательность логических нулей и единиц. В квантовом компьютере регистр до измерения его состояния не является явно определенным и описывается линейной композицией с комплексными числами (суперпозицией) n-битовых состояний вида:

$$|\psi\rangle = y_1|0..0\rangle + y_2|0..1\rangle + \cdots + y_n|1..1\rangle.$$

Вероятность нахождения квантового компьютера в состоянии $|0..0\rangle$ равна $|y_1|^2$, в состоянии $|0..1\rangle$ равна $|y_2|^2$ и т. д. За счет такого необычного для булевой логики свойства квантовых вычислений, а именно состояния суперпозиции входного регистра кубитов, появляется возможность параллельных массивных вычислений. Поскольку один кубит представляется двумя состояниями, то два кубита – четырьмя состояниями одновременно. Например, если входной регистр состоит из двух кубитов $|0\rangle$ и $|1\rangle$, то в результате обрабатываются четыре состояния (операции) $|00\rangle$, $|01\rangle$, $|10\rangle$ и $|11\rangle$ за один шаг. Для n кубитов квантовый компьютер вычисляет 2^n операций за один шаг, в то время как на классическом компьютере требуется 2^n шагов.

Регистр из кубитов $|0\rangle$ и $|1\rangle$ вычисляется с помощью произведения Кронекера (тензорного произведения) двух вектор-столбцов:

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}1 \cdot \begin{bmatrix}0\\1\end{bmatrix}\\ 0 \cdot \begin{bmatrix}0\\1\end{bmatrix}\end{bmatrix} = \begin{bmatrix}0\\1\\0\\0\end{bmatrix},$$

где $\otimes$ – тензорное произведение.

[1] Паспорт «Дорожной карты развития высокотехнологичной области «Квантовые вычисления» на период до 2024 года» (утв. Минцифры России 31 июля 2020 г. №14).

Любая логическая операция с кубитами называется квантовым вентилем или гейтом. По числу кубитов преобразователи делятся на однокубитные и многокубитные. Преобразователь переводит одно состояние кубита (а в многокубитном случае – квантового регистра) в другое. Квантовым преобразованием называют унитарное преобразование вектора состояния квантовой системы, которое всегда обратимо. Для демонстрации действия квантового преобразователя на кубиты используют матричную запись соответствующих операторов. Матричная форма операторов, которые чаще всего используются в квантовых алгоритмах, подробно рассмотрена в работах [1-4].

Основой для моделирования квантовых вычислений являются три оператора, действующих на входной квантовый регистр: суперпозиции, квантовой корреляции (запутанного состояния) и интерференции. Преобразование Адамара может обеспечивать как суперпозицию классических состояний, так и интерференцию выходного вектора кубитов. К инициирующим запутанные состояния кубитов относятся оператор контролируемого отрицания (CNOT), а также сочетания унитарных операторов идентичности, отрицания и CNOT. В совокупности операторы суперпозиции, корреляции и интерференции формируют математическую модель квантового алгоритма в виде обобщенного матричного оператора, которая впоследствии может быть преобразована в программный код на классическом компьютере.

В отличие от унитарных преобразований операция измерения квантового регистра приводит к необратимому изменению его состояния – он коллапсирует из суперпозиции в одно из базисных состояний. Одно измерение кубита дает один бит информации о его состоянии. За счет суперпозиции базисных состояний до измерения в нем хранится масса скрытой информации. Объем этой скрытой информации экспоненциально растет с увеличением числа кубитов.

Главная проблема квантовых вычислений состоит в том, что после проведения вычислений получить всю скрытую информацию невозможно, так как в результате измерения получается одно значение из всего множества. Тем не менее при анализе полученного квантового регистра до его измерения можно получить информацию о некоторых его общих свойствах.

Одним из подходов для получения такой информации, демонстрирующим превосходство квантовых вычислений над классическими, является квантовый алгоритм Дойча. Существующие методы его моделирования на классическом компьютере были изучены в ходе анализа ряда научных трудов [3; 4].

На основе результатов проведенного анализа был разработан комбинированный подход к моделированию алгоритма Дойча, позволяющий использовать преимущества, нивелировать недостатки известных подходов и за счет этого повысить точность получаемого результата, применяя только одну итерацию модели. Рассмотрим основные положения этого подхода.

2. Постановка и решение задачи Дойча

Задача Дойча формулируется следующим образом. Пусть на входе квантового алгоритма имеется бинарная функция $f_i(x)$ от переменной $x \in \{0, 1\}$, $i \in \{1, 2, 3, 4\}$. При этом функция $f_i(x)$ является постоянной, когда принимает значения $f_i(x) = 0$ или $f_i(x) = 1$. В случае, когда $f_i(x) = x$ или $f_i(x) = \neg x$, она – сбалансированная. Требуется определить, к какому типу относится функция $f_i(x)$, используя различные сочетания двухкубитного входного регистра.

Исходя из постановки задачи, возможны четыре варианта исследуемой функции (таблица 1).

При использовании классических вычислений необходимо провести как минимум две операции – определить значения $f_i(0)$ и $f_i(1)$. Квантовый алгоритм Дойча позволяет вычислить значение функции за одну операцию.

Существуют два типовых подхода к формированию квантовой схемы данного алгоритма, которые показаны на рисунке 1. Каждый из этих подходов имеет свои преимущества и недостатки, влияющие на точность получаемого результата. Внешне они отличаются только последовательностью применения соответствующих операторов Адамара H и идентичности I ко второму кубиту, который будем называть управляющим.

Таблица 1 – Варианты значений исследуемой функции $f_i(x)$

i	x	f_i	Тип функции
1	0	0	постоянная
	1	0	
2	0	1	
	1	1	
3	0	0	сбалансированная
	1	1	
4	0	1	
	1	0	

При исследовании первого подхода (рисунок 1а) было установлено, что если первый кубит входного регистра в результате всех преобразований изменяет свое значение ($|0_1\rangle$ на $|1_1\rangle$ или $|1_1\rangle$ на $|0_1\rangle$), то искомая функция является сбалансированной с вероятностью 1, в противном случае – либо постоянной с вероятностью $0{,}5$, либо о ее типе однозначно сказать нельзя.

Результат изучения второго подхода (рисунок 1б) [3] заключается в том, что если первый кубит входного регистра на выходе алгоритма изменяет свое значение, то искомая функция является сбалансированной, в противном случае при входном регистре $|01\rangle$ или $|11\rangle$ – постоянной с одинаковой вероятностью 1, при $|10\rangle$ или $|00\rangle$ – о ее типе однозначно сказать нельзя.

Сравнительный анализ подходов позволил определить закономерность: если первый кубит входного регистра изменяет свое значение на выходе алгоритма, то в обоих случаях с вероятностью 1 функция сбалансированная; если нет, то в первом случае с вероятностью $0{,}5$ она постоянная или дать однозначный ответ не представляется возможным. Во втором случае вероятность получения правильного результата зависит от входного значения управляющего кубита: если он равен $|1_2\rangle$, то с вероятностью 1 функция постоянная; если – $|0_2\rangle$, то однозначный ответ не возможен.

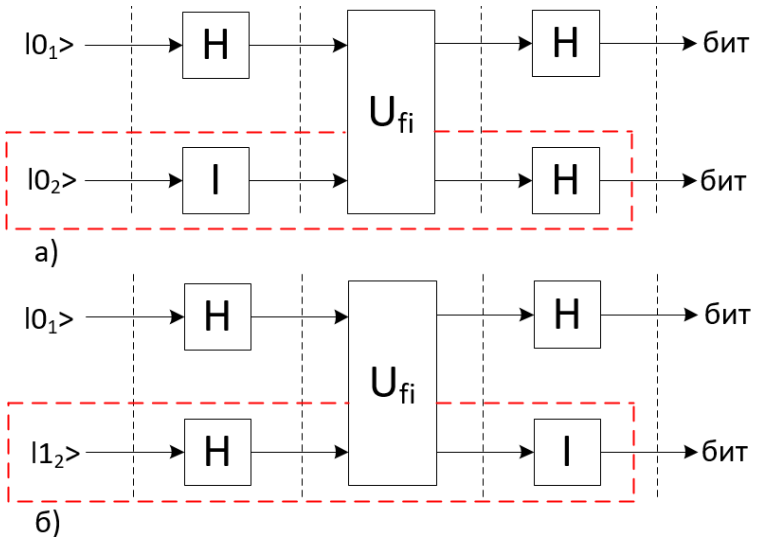

Рисунок 1 – Типовые подходы к моделированию алгоритма Дойча (а, б) и их комбинация по управляющему кубиту (показана красным цветом)[2]

[2] Иванцова О.В., Кореньков В.В., Ульянов С.В. Технологии интеллектуальных вычислений. Ч.2: Квантовые вычисления и алгоритмы. Квантовый алгоритм самоорганизации. Квантовый нечеткий вывод: учеб.-мет. пособие. М.: Курс, 2020. 296 с.; *см. также* [3].

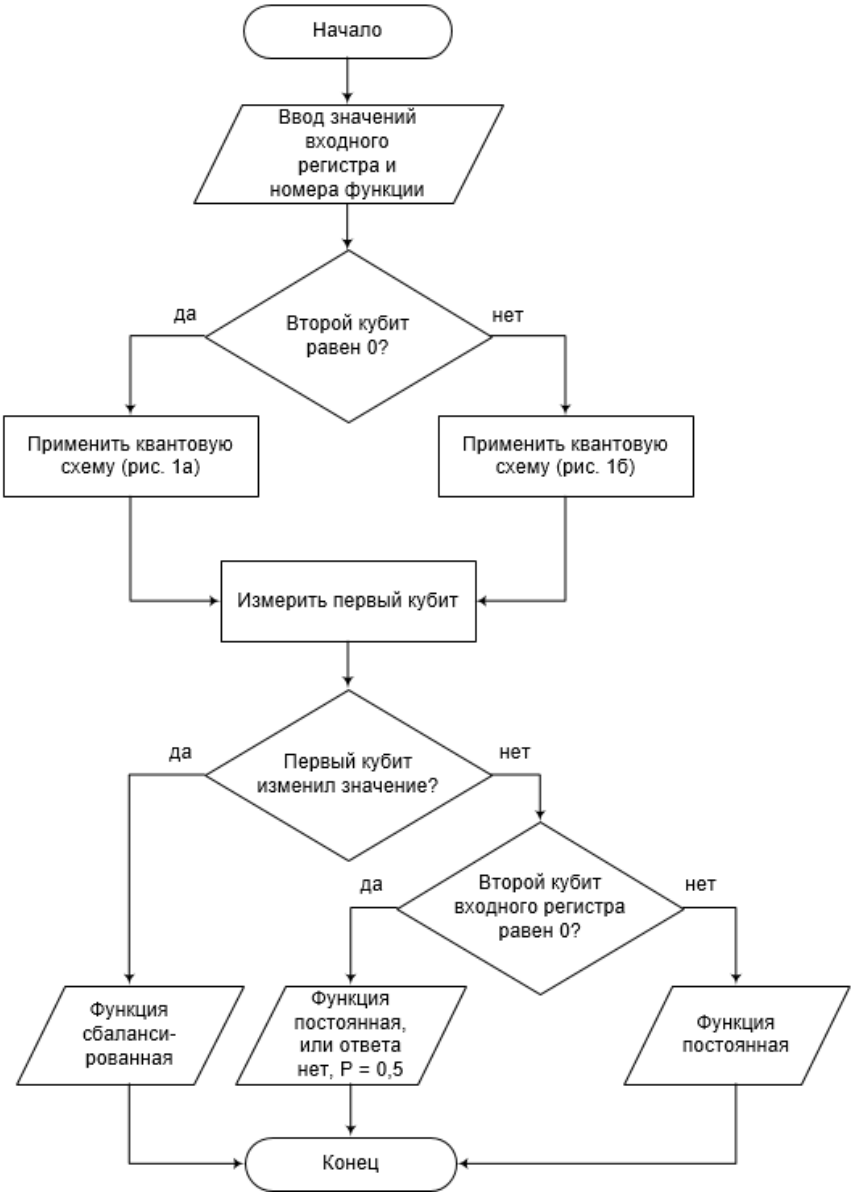

Рисунок 2 – Алгоритм, реализующий комбинированный подход к решению задачи Дойча

С учетом выявленной закономерности был разработан комбинированный подход, представляющий собой адаптивную квантовую схему, динамически изменяющуюся в зависимости от входного значения управляющего кубита (изменяющаяся часть схемы показана на рисунке 1 красным цветом). Если он равен $|0_2\rangle$, то применяем схему на рисунке 1а, в противном случае – схему на рисунке 1б. Алгоритм, реализующий комбинированный подход, представлен на рисунке 2.

Результаты проведенных теоретических расчетов показали, что приведенный алгоритм по сравнению с первым подходом позволяет повысить вероятность того, что функция является постоянной, на $0{,}5$ при условии, что управляющий кубит равен $|1_2\rangle$; по сравнению со вторым подходом – снизить вероятность неоднозначного ответа на $0{,}5$ в случае, когда управляющий кубит равен $|0_2\rangle$.

Теперь можно построить обобщенный матричный оператор G_i в виде композиции операторов, задействованных в схемах на рисунке 1, путем их произведения, выполняемого в обратной последовательности:

$$G_i = \begin{cases} (H \otimes H) \cdot \left(U_{f_i} \cdot (H \otimes I)\right) \text{ при } |\psi\rangle = |0_2\rangle \\ (H \otimes I) \cdot \left(U_{f_i} \cdot (H \otimes H)\right) \text{ при } |\psi\rangle = |1_2\rangle \end{cases}, \quad (1)$$

где H – матрица оператора Адамара, $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$;

I – матрица оператора идентичности, $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$;

U_{f_i} – оператор, который в зависимости от введенного индекса искомой функции f_i принимает вид одной из четырех матриц размерности $4\text{x}4$,

$$U_{f_1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, U_{f_2} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, U_{f_3} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, U_{f_4} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Когда оператор G_i сгенерировал выходной вектор, выполняется операция измерения. Квантовое измерение является недетерминированной операцией, на вход которой подается суперпозиция базисных векторов. Выходом является один из базисных векторов. При этом вероятность каждого из векторов быть измеренным определяется квадратом модуля его комплексной амплитуды в исходной суперпозиции. Например, при вводе в алгоритм, изображенный на рисунке 2, двухкубитного регистра $|11\rangle$ и второго индекса искомой функции, используя нижнюю последовательность операторов в формуле (1), получаем следующую суперпозицию базисных векторов:

$$G_2|11\rangle = \frac{1}{\sqrt{2}}\ |10\rangle + \frac{1}{\sqrt{2}}\ |11\rangle,$$

где $\frac{1}{\sqrt{2}}$ – комплексные амплитуды векторов $|10\rangle$ и $|11\rangle$ перед измерением, амплитуды векторов $|00\rangle$ и $|01\rangle$ равны нулю.

Далее находим вероятности измерения базисных векторов $|10\rangle$ и $|11\rangle$:

$$\left|\frac{1}{\sqrt{2}}\right|^2 = 0{,}5.$$

После измерения получаем один из векторов $|10\rangle$ или $|11\rangle$ и делаем вывод о типе бинарной функции. В нашем случае вне зависимости от результата измерения можно сказать, что функция постоянная с вероятностью 1, так как первый кубит входного регистра $|1_1\rangle$ на выходе алгоритма свое значение не изменит, а управляющий кубит не равен $|0_2\rangle$.

3. Реализация комбинированного подхода к решению задачи Дойча в среде MATLAB/SIMULINK

Модель, реализующая комбинированную квантовую схему (см. рисунок 1), была построена в пакете визуального блочного имитационного моделирования SIMULINK матричной системы MATLAB (рисунок 3) [5].

На вход схемы подаются векторы состояний двух кубитов $Q1$, $Q2$ и номер функции от 1 до 4, для чего используются блоки $Constant$. На первый кубит действуем оператором Адамара H, на второй – либо оператором Адамара, либо оператором идентичности I в соответствии с условием (1). Далее к преобразованным кубитам применяем оператор $U(f_i)$. Затем к первому из результирующих кубитов применяем оператор Адамара, ко второму – оператор Адамара или оператор идентичности в зависимости от значения управляющего кубита. Все преобразования реализованы с помощью соответствующих MATLAB функций. На выходе получаем вероятности измерения базисных векторов $Q1$ и $Q2$, отображающиеся в блоке $Display$. Блок $out.simout$ обеспечивает вывод объединенного вектора вероятностей в рабочее пространство MATLAB для построения графиков и интерпретации полученных результатов.

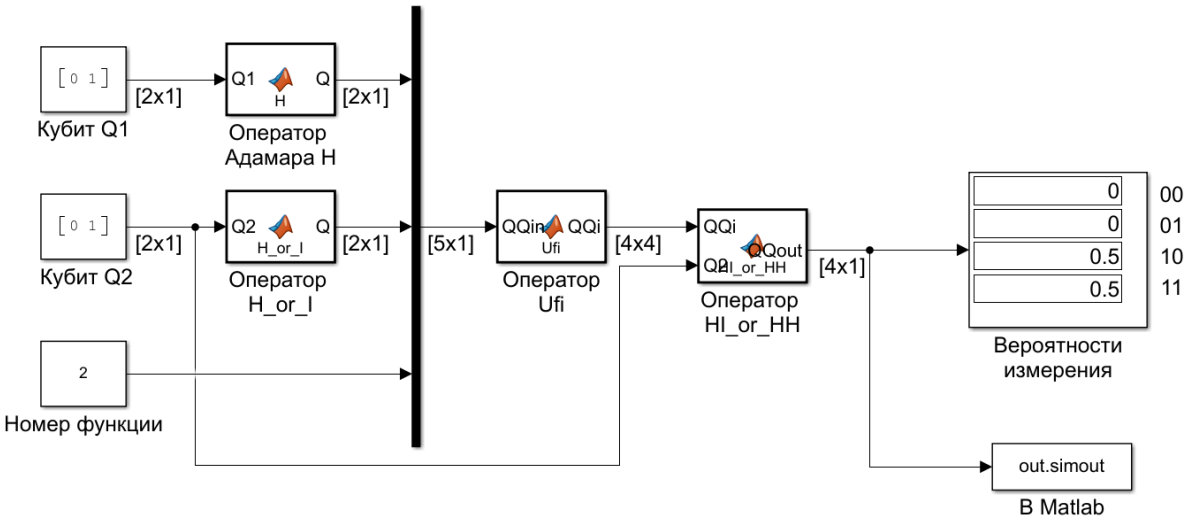

Рисунок 3 – Вид окна в пакете SIMULINK при тестировании комбинированной квантовой схемы решения задачи Дойча

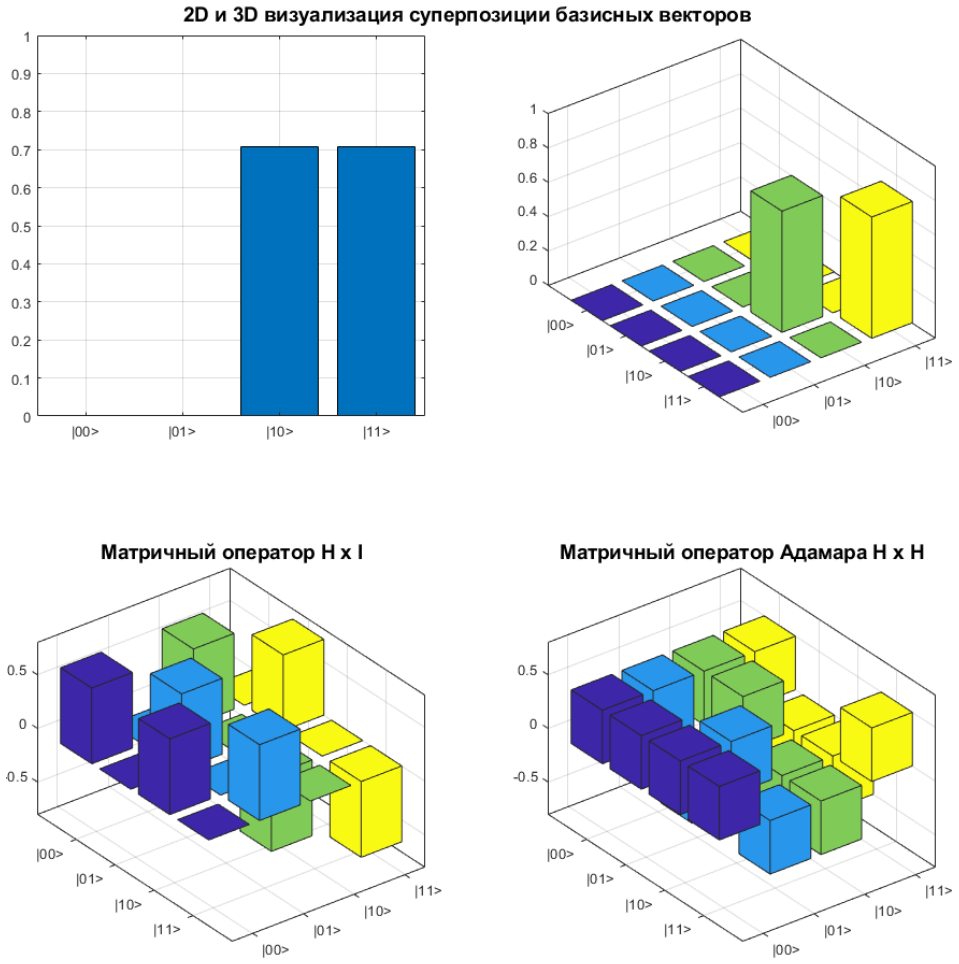

Рисунок 4 – Вид графического окна MATLAB с визуализацией матричных операторов и суперпозиции базисных векторов

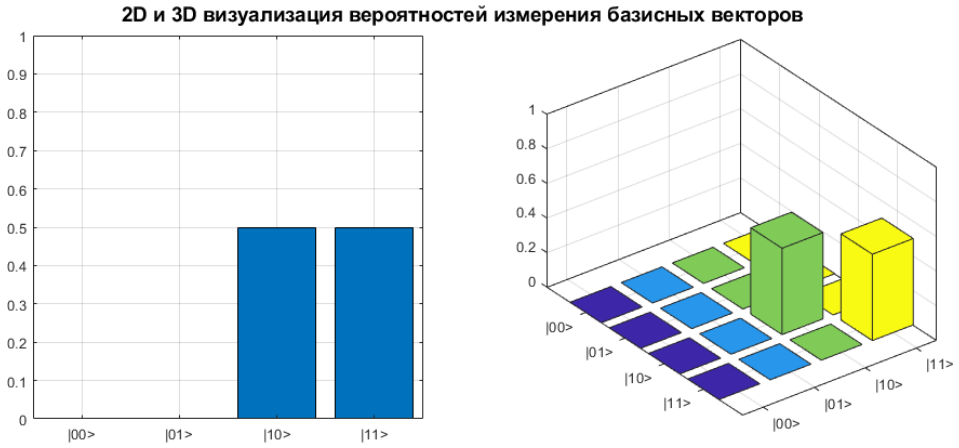

Рисунок 5 – Вид графического окна MATLAB с визуализацией
и интерпретацией полученных результатов до операции измерения

Графическое изображение и интерпретация результатов применения модели и функции $CombDeutsch$ показаны на рисунке 5.

На рисунках 3-5 приведены результаты, полученные после ввода исходных данных в виде вектора $|11\rangle$ и второго индекса искомой функции.

Для автоматического построения графиков и вывода промежуточных и конечного результатов применения модели в среде MATLAB была создана пользовательская функция $CombDeutsch$ в виде M-файла. На рисунке 4 представлена визуализация матричных операторов $H \otimes H$ и $H \otimes I$, используемых в комбинированной квантовой схеме (1), и выходной суперпозиции базисных векторов.

Сравнительный анализ результатов моделирования и теоретических расчетов показал их полное совпадение, что позволяет сделать вывод об отсутствии ошибок в программном коде и адекватности разработанных алгоритма, модели SIMULINK и пользовательской функции $CombDeutsch$, реализующих комбинированный подход к решению задачи Дойча.

Заключение

В статье рассмотрен комбинированный подход к решению задачи Дойча, объединяющий в себе преимущества известных подходов и позволяющий повысить вероятность получения правильного результата при различных сочетаниях входного двухкубитного регистра. Предложенный подход и его программная реализация могут быть использованы при разработке более сложных квантовых алгоритмов с небольшими изменениями в исходном коде.

Главное преимущество квантовых вычислителей перед традиционными заключается в повышенном быстродействии и производительности за счет состояний квантовой суперпозиции и запутанности, что позволяет наиболее эффективно решать задачи полиноминальной сложности, когда объем вычислений и время на его обработку находятся в экспоненциальной зависимости от длины входного регистра. Это обстоятельство является основным ограничением при моделировании квантовых алгоритмов на классическом компьютере.

С учетом этого появление квантовых компьютеров окажет существенное влияние на характеристики систем (комплексов, образцов) вооружения, военной и специальной техники, в частности, на средства защиты информации, использующие современные криптографические алгоритмы и протоколы. Например, квантовый алгоритм факторизации числа (алгоритм Шора) [6] делает криптографическую систему RSA небезопасной, квантовый алгоритм Саймона осуществляет поиск блочных шифров в режимах CBC-MAC, PMAC, GMAC, GCM и

ОСВ [7], квантовый алгоритм Гровера [1] производит полный перебор ключей блочного шифра SDES за миллисекунды. Для классического компьютера решить такие задачи за приемлемое время не представляется возможным. С другой стороны, квантовые алгоритмы могут генерировать шифры, которые невозможно будет взломать классическими алгоритмами, что позволит создавать средства защиты информации с повышенной стойкостью.

Несмотря на то, что в настоящее время прикладная значимость решаемых с помощью квантовых алгоритмов задач пока невысока, представляется целесообразным все разработанные модели объединять в некую базу квантовых алгоритмов, которая будет программной основой для выполнения квантовых вычислений на отечественном квантовом компьютере.

Вполне возможно, что аппаратной основой будет гибридный вариант квантового и классического компьютеров. При этом вычисления будут производиться квантовым процессором, а их результат сообщаться обычному процессору, который будет управлять его работой: настраивать гейты, связывать их друг с другом, запускать квантовые вычисления, инициализировать и измерять кубиты [8; 9].

Список источников

1. Смирнов Ю.А., Актимиров А.В. Моделирование квантового алгоритма Гровера для поиска схемотехнического решения в прикладной программе MATLAB // Молодой ученый. 2019. №13(251). С. 49-62.

2. Смирнов Ю.А., Актимиров А.В. Имитационное моделирование квантового алгоритма решения систем линейных уравнений в прикладной программе MATLAB // Молодой ученый. 2019. №51(289). С. 31-39.

3. Перченок О.В. Квантовое моделирование алгоритма Дойча в среде MATLAB/SIMULINK // Компьютерные инструменты в образовании. 2010. №1. С. 22-29.

4. Шемякина М.А., Бабаев А.М. Моделирование квантового алгоритма Дойча на классическом компьютере // Аллея Науки. 2018. Т.4. №11(27). С. 910-915.

5. Горский А.С., Полушкин В.М., Князев Р.И., Ермоленко А.В., Миргородская К.М. Имитационная модель комбинированного квантового алгоритма Дойча // Свидетельство о гос. рег. программы для ЭВМ RU 2024612944. Дата регистрации 23.01.2024. Дата публикации 07.02.2024.

6. Шемякина М.А. Моделирование квантового алгоритма Шора на классическом компьютере // Международный журнал гуманитарных и естественных наук. 2019. №4-2. С. 55-59.

7. Глушанский С.М., Потапов В.С. Моделирование работы квантового алгоритма Саймона для нахождения периода функции // Информационные технологии, системный анализ и управление, (ИТСАУ-2019): сб. трудов XVII Всеросс. науч. конф. (Таганрог, 4-7 декабря 2019 г.). В 2 т. Т.1. Ростов-н/Д.: Южн. фед. ун-т, 2019. С. 88-91.

8. Валиев К.А., Кокин А.А. Квантовые компьютеры: надежды и реальность: монография. Ижевск: Регулярная и хаотическая динамика, 2001. 352 с.

9. Зрелов П.В., Иванцова О.В., Кореньков В.В., Рябов Н.В., Ульянов С.В. Эффективное моделирование квантовых алгоритмов на симуляторах классической архитектуры // Системный анализ в науке и образовании. 2022. №1. С. 42-54.

Информация об авторе

А.С. Горский – кандидат технических наук.