

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
«БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
КАФЕДРА «ИНТЕЛЛЕКТУАЛЬНЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

Методические указания к лабораторным
и практическим занятиям по дисциплине

«Современные методы защиты компьютерных систем»

*для специальности
6-05-0611-03 Искусственный интеллект*

Брест 2024

УДК 347 77/681.3
ББК 67.403.3 73/32.97

Методические указания содержат теоретический материал по основам квантовых вычислений. Приводится описание квантовых вентилей, рассматриваются простейшие квантовые алгоритмы и описываются механизмы работы алгоритмов Дойча, Гровера, Шора.

Методические указания предназначены для использования студентами специальности 6-05-0611-03 Искусственный интеллект в ходе выполнения лабораторных, практических и контрольных работ по дисциплине «Современные методы защиты компьютерных систем».

Составители: Хацкевич М. В. старший преподаватель кафедры ИИТ
Хацкевич А. С. ассистент кафедры ИИТ

Рецензент: Грицук Д. В. заведующий кафедрой прикладной математики
и информатики БрГУ им. А. С. Пушкина, к. ф.-м. н.

Содержание

Лабораторная работа № 1. «Изучение простейших квантовых систем»	3
Лабораторная работа № 2. «Алгоритм Дойча».....	12
Лабораторная работа № 3. «Алгоритм Гровера, подготовка оракула»	16
Лабораторная работа № 4. «Алгоритм Гровера, оператор диффузии Гровера»	18
Лабораторная работа № 5. «Алгоритм Шора».....	22
Список литературы.....	23

Лабораторная работа № 1 Тема «Изучение простейших квантовых систем»

Цель работы: научиться подготавливать специальные кубитные состояния.

Основы: квантовые состояния

Начнем с обозначений некоторых распространенных квантовых состояний, которыми будем впоследствии манипулировать:

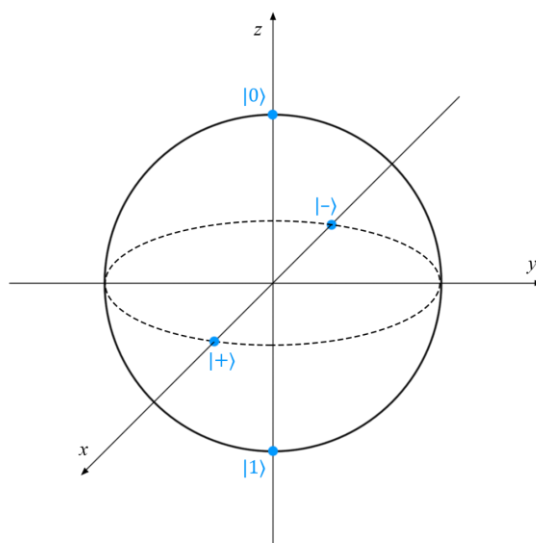
$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} .$$

Все они являются чистыми однокубитными состояниями, поэтому их можно представить в виде точек на сфере Блоха:



Теперь четыре состояния Белла (их еще называют парами ЭПР, в честь Эйнштейна, Подольского и Розена – именно они являются авторами идей, которые впоследствии развил Белл). Это простейшие примеры квантовой запутанности двух кубитов:

$$|\psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

$$|\phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$|\phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

И наконец, будем использовать так называемые состояния ГХЦ (Гринберга – Хорна – Цайлингера). Вот их общая форма (для n кубитов) и простейшая форма (для трех кубитов):

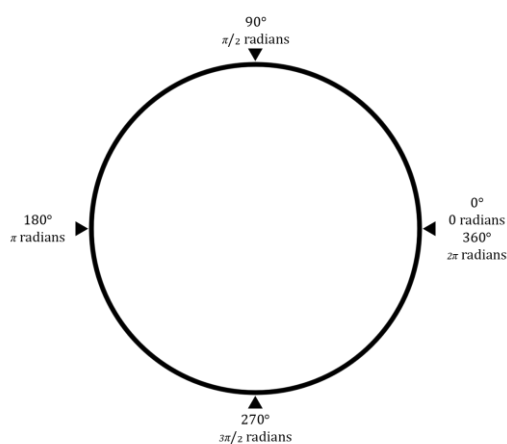
$$|GHZ\rangle_{general} = \frac{|0\rangle^{\otimes n} + |1\rangle^{\otimes n}}{\sqrt{2}}$$

$$|GHZ\rangle_{simplest} = \frac{|000\rangle + |111\rangle}{\sqrt{2}}.$$

Состояния Белла и состояния ГХЦ очень важны, потому что их поведение кардинально отличается от предсказаний классической теории из-за уровня запутанности в таких системах (этот принцип «максимальной запутанности» будет рассмотрен в одной из последующих публикаций).

Основы: радианы

Углы поворота в теории квантовых вычислений измеряются в радианах. Полная окружность (360°) соответствует 2π радиан. Углы измеряются против часовой стрелки. Ниже показаны величины важнейших углов в градусах и в радианах.



Основы: диаграммы квантовых цепей

Перед тем как углубляться в изучение квантовых вентилей, следует изучить основы построения диаграмм квантовых цепей:

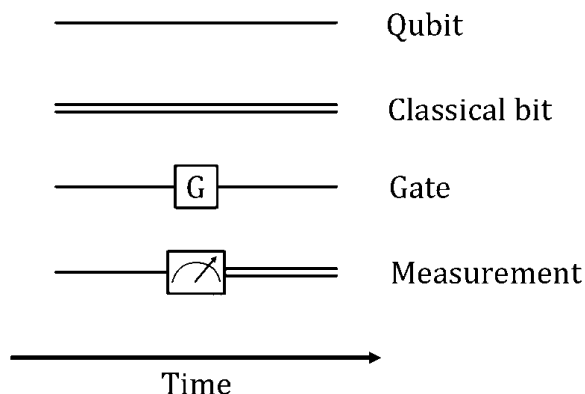
- Время на квантовой диаграмме движется слева направо.
- Каждому кубиту соответствует одиночная горизонтальная линия.

– Вентили обычно обозначаются квадратами. Тип вентилей обозначается буквами или другими символами в этом квадрате (бывают и исключения из этого правила. Обычно это кубитные вентили, у которых есть классические аналоги (пример: вентиль NOT)).

– Некоторым вентилям может соответствовать несколько элементов диаграммы (пример: вентиль NOT).

– В результате измерения кубита все суперпозиции коллапсируют, квантовые свойства кубита исчезают, и он превращается в обычный бит. Поэтому можно считать, что измерительный элемент (показанный ниже) принимает на вход кубит и выдает классический бит.

Обозначения важнейших элементов:



Теоретический материал

1 Квантовый вентиль X

Вентиль X имеет матрицу:

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

и это матрица X Паули, названная в честь Вольфганга Паули. Обозначение часто используется как для вентилей, так и для его унитарной матрицы в стандартных базисных кетах.

Вентиль X обладает свойством:

$$X|0\rangle = |1\rangle;$$

$$X|1\rangle = |0\rangle.$$

Он меняет значение с $|0\rangle$ и $|1\rangle$ и наоборот. Классический вентиль not показан на рисунке 1:



Рисунок 1 – Классический вентиль not

Вентиль not представляется собой «битовую инверсию», и по аналогии говорят, что X является битовой инверсией.

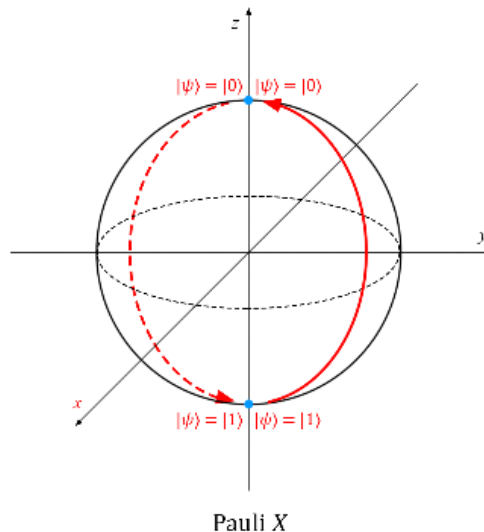
$$\text{Для } |\psi\rangle = a|0\rangle + b|1\rangle:$$

$$X|\psi\rangle = b|0\rangle + a|1\rangle.$$

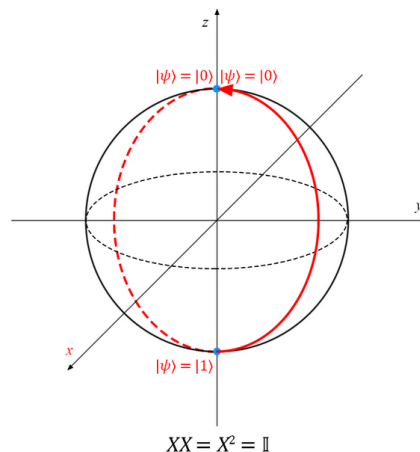
Это меняет вероятности измерения $|0\rangle$ и $|1\rangle$ на противоположные.

σ_x имеет собственные значения $+1$ и -1 для собственных векторов $|+\rangle$ и $|-\rangle$ соответственно.

С точки зрения сферы Блоха вентиль X поворачивается на величину π вокруг оси x . Таким образом инвертируются не только полюса, но и точки в нижней полусфере перемещаются в верхнюю и наоборот, что отображено ниже:



Поскольку $XX = I_2$, вентиль X является своей собственной инверсией. Это разумно, потому что в классическом случае также верно, что $\text{not} \circ \text{not}$ является операцией тождества. Такое преобразование проиллюстрировано ниже:



Вентиль X , показан на рисунке 2.

Горизонтальная линия, называемая проводом, представляет кубит и его состояние.

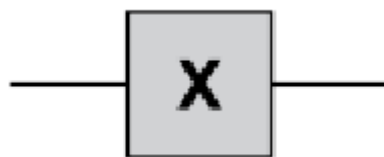
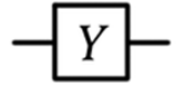


Рисунок 2 – Вентиль X

Входное состояние поступает слева, применяется унитарное преобразование X , и результат в виде нового квантового состояния выводится с правой стороны.

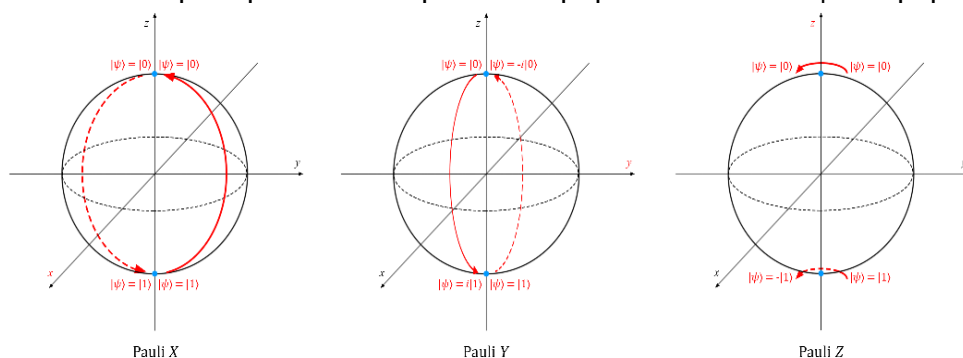
Названия	Матричное представление	Обозначения
Вентиль Паули X	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	 
Вентиль Паули Y	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$	
Вентиль Паули Z	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	

Вентиль X очень похож на классический вентиль NOT: он преобразует $|0\rangle$ в $|1\rangle$, а $|1\rangle$ в $|0\rangle$. Эта операция эквивалентна повороту вектора на сфере Блоха вокруг оси x на π радиан (или 180°).

Вентиль Y ожидаемо соответствует повороту вектора вокруг оси y на π радиан. В результате такой операции вектор $|0\rangle$ превращается в $i|1\rangle$, а $|1\rangle$ — в $-i|0\rangle$.

Вентиль Z представляет собой особый случай вентиля фазового сдвига R_ϕ (см. ниже) при $\phi = \pi = 180^\circ$. Он соответствует повороту вектора вокруг оси z на π радиан. Вектор $|0\rangle$ он оставляет без изменений, а $|1\rangle$ преобразует в $-|1\rangle$.

Ниже работа этих преобразований проиллюстрирована с помощью сферы Блоха:



2 Квантовый вентиль H

Вентиль H или $H \otimes^2$, или вентиль Адамара, описывается матрицей

$$H = \begin{bmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{bmatrix} = \frac{\sqrt{2}}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Согласно матричному умножению

$$H|0\rangle = \frac{\sqrt{2}}{2}(|0\rangle + |1\rangle) = |+\rangle;$$

$$H|1\rangle = \frac{\sqrt{2}}{2}(|0\rangle - |1\rangle) = |-\rangle.$$

В силу линейности:

$$\begin{aligned} H|+\rangle &= H\left(\frac{\sqrt{2}}{2}(|0\rangle + |1\rangle)\right) = \frac{\sqrt{2}}{2}(H|0\rangle + H|1\rangle) = \\ &= \frac{\sqrt{2}}{2}\left(\frac{\sqrt{2}}{2}(|0\rangle + |1\rangle) + \frac{\sqrt{2}}{2}(|0\rangle - |1\rangle)\right) = \frac{1}{2}(|0\rangle + |1\rangle + |0\rangle - |1\rangle) = |0\rangle \end{aligned}$$

Аналогично:

$$H|-\rangle = |1\rangle.$$

Вентиль Адамара – один из наиболее используемых вентилей в квантовых вычислениях. Нередко H является первым вентилем, который применяется в схеме. Если существует необходимость поместить кубит в суперпозицию, то нужно взять кубит, инициализированный в состоянии $|0\rangle$, и применить к нему H.

Матрица Адамара – это изменение базисной матрицы с $\{|0\rangle, |1\rangle\}$ на $\{|+\rangle, |-\rangle\}$. Поскольку $HH = I_2$, вентиль H является обратным себе.

Вентиль H, включенный в схему, показан на рисунке 3.

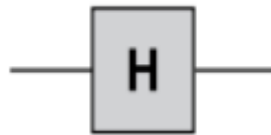


Рисунок 3 – Вентиль H

Для нашего вентиль H:

$$H|0\rangle = \frac{\sqrt{2}}{2}(|0\rangle + |1\rangle);$$

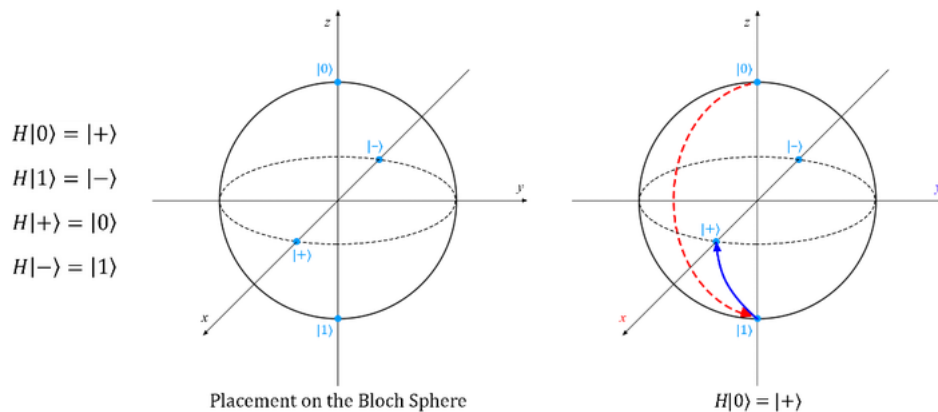
$$H|1\rangle = \frac{\sqrt{2}}{2}(|0\rangle - |1\rangle).$$

Заметим, что:

$$H|u\rangle = \frac{\sqrt{2}}{2}(|0\rangle + |1\rangle^u |1\rangle).$$

когда u является одним из $\{0, 1\}$.

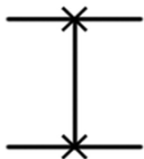
Эти преобразования проиллюстрированы ниже:



Смена базиса с вычислительного базиса $\{|0\rangle, |1\rangle\}$ на базис Адамара $\{|+\rangle, |-\rangle\}$ меняет инверсию бита X на инверсию фазы Z.

3 Многокубитный вентиль SWAP

Многокубитные вентили выполняют операции над двумя или более кубитами. Один из простейших примеров — вентиль SWAP.

Название	Матричное представление	Обозначение
SWAP	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$	

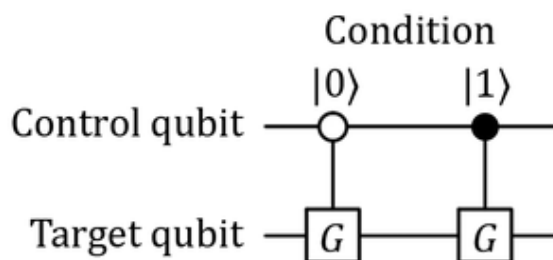
Вентиль SWAP меняет местами два входных кубита.

Например, $\text{SWAP}|0\rangle|1\rangle = |1\rangle|0\rangle$, а $\text{SWAP}|0\rangle|0\rangle = |0\rangle|0\rangle$.

4 Квантовый вентиль CNOT

Еще один класс многокубитных вентилей — так называемые управляемые вентили. На вход любого управляемого вентиля подается по меньшей мере один управляющий и один управляемый кубит, причем вентиль выполнит операцию над управляемым кубитом только в том случае, если управляющий кубит находится в определенном состоянии.

Вентили, которые выполняют операцию при управляющем кубите $|1\rangle$, обозначаются заполненным кругом на проводе управляющего кубита. Вентили, которые выполняют операцию при управляющем кубите, равном $|0\rangle$, обозначаются пустой окружностью, как показано ниже:



Для того чтобы составить матрицу любого управляющего вентиля, нужно дописать единичную матрицу в левом верхнем углу матрицы нужного вентиля, а все остальные ячейки заполнить нулями. Вот пример:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \text{NOT} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

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

Вентиль CNOT является одним из самых важных вентилей в квантовых вычислениях. Он используется для создания запутанных кубитов. Данный вид вентилей не единственный, который может это сделать, но он прост и очень часто используется.

Буква «С» в CNOT означает «контролируемый». В отличие от 1 однокубитного вентиля X, который в безусловном порядке инвертирует $|0\rangle$ на $|1\rangle$ и наоборот, CNOT имеет два кубитных входа и два выхода. Вентили должны быть обратимыми. По этой причине

мы должны иметь одинаковое количество входов и выходов. Мы называем кубиты q_1 и q_2 , а их состояния, соответственно, $|\psi\rangle_1$ и $|\psi\rangle_2$.

CNOT берет два входа: $|\psi\rangle_1$ и $|\psi\rangle_2$. Если $|\psi\rangle_1$ равно $|1\rangle$, то состояние q_1 остается $|\psi\rangle_1$, но $|\psi\rangle_2$ становится $X|\psi\rangle_2$. В противном случае состояния q_1 и q_2 не изменяются. Другими словами, CNOT всегда работает как $ID|\psi\rangle_1$ для q_1 . Когда $|\psi\rangle_1 = |1\rangle$, CNOT действует как $X|\psi\rangle_2$ для q_2 . В противном случае он действует как $ID|\psi\rangle_2$. CNOT является условной битовой инверсией.

В классическом случае мы создаем контролируемый not из xor с помощью схемы (рисунок 4):

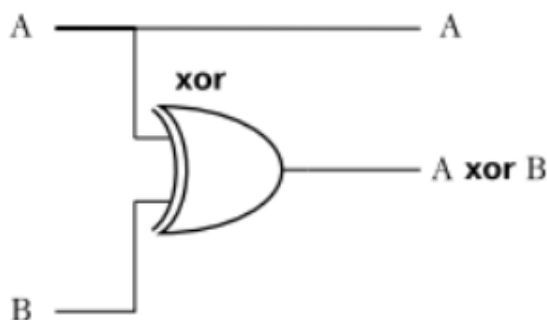


Рисунок 4 – Классический CNOT

Матрица для CNOT такова:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Это матрица перестановок, которая меняет местами третий и четвертый коэффициенты $|\psi\rangle_1 \otimes |\psi\rangle_2$. Левая верхняя подматрица 2×2 равна I_2 , а правая нижняя подматрица 2×2 равна матрице X .

Вентиль CNOT в схеме охватывает два провода. Верхняя линия – это управляющий кубит.

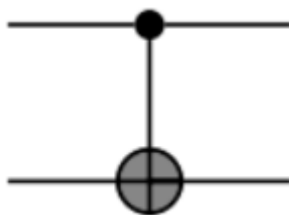


Рисунок 5 – Классический CNOT

$$CNOT|00\rangle = |0\rangle; CNOT|01\rangle = |01\rangle; CNOT|10\rangle = |11\rangle; CNOT|11\rangle = |10\rangle;$$

В силу линейности

$$\begin{aligned} CNOT(a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle) &= \\ = a_{00}CNOT|00\rangle + a_{01}CNOT|01\rangle + a_{10}CNOT|10\rangle + a_{11}CNOT|11\rangle &= \\ = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|11\rangle + a_{11}|10\rangle &= \\ = a_{00}|00\rangle + a_{01}|01\rangle + a_{11}|10\rangle + a_{10}|11\rangle. \end{aligned}$$

Применение вентилей Н Адамара со сменой базиса перед и после вентиля CNOT иллюстрирует интересное свойство CNOT. Матричная форма $H \otimes^2 \circ CNOT \circ H \otimes^2$ такова:

$$M = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{bmatrix}.$$

Сводится к более простой форме:

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

Влияние M на стандартные базисные кеты:

$$M|00\rangle = |00\rangle; M|01\rangle = |11\rangle; M|10\rangle = |10\rangle; M|11\rangle = |01\rangle.$$

Если второй кубит равен $|1\rangle$, то первый кубит инвертируется. Если он равен $|0\rangle$, то первый кубит остается таким же. Это противоположное поведение вентиля CNOT, но оно строится из него с помощью операций Адамара перед и после. В случае с CNOT состояние второго кубита контролируется первым. В этой конструкции наоборот. Если бы хотели, чтобы управляющий кубит был вторым именно таким образом, мы бы нарисовали его с использованием $\bullet$ внизу. Иногда его называют обратным вентилям CNOT (рисунок 6).

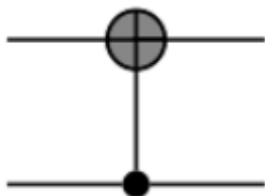
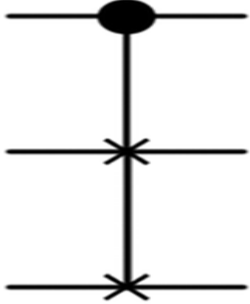


Рисунок 6 – Обратный вентиль CNOT

Ниже описаны другие распространенные управляемые вентили (мы выделили единичную матрицу серым, а матрицу исходного вентиля — черным):

Названия	Матричное представление	Обозначения
CNOT	$\begin{bmatrix} \text{red } 1 & \text{red } 0 & 0 & 0 \\ \text{red } 0 & \text{red } 1 & 0 & 0 \\ 0 & 0 & \text{blue } 0 & \text{blue } 1 \\ 0 & 0 & \text{blue } 1 & \text{blue } 0 \end{bmatrix}$	
CCNOT, вентиль Тoffoli	$\begin{bmatrix} \text{red } 1 & \text{red } 0 & \text{red } 0 & \text{red } 0 & \text{red } 0 & \text{red } 0 & 0 & 0 \\ \text{red } 0 & \text{red } 1 & \text{red } 0 & \text{red } 0 & \text{red } 0 & \text{red } 0 & 0 & 0 \\ \text{red } 0 & \text{red } 0 & \text{red } 1 & \text{red } 0 & \text{red } 0 & \text{red } 0 & 0 & 0 \\ \text{red } 0 & \text{red } 0 & \text{red } 0 & \text{red } 1 & \text{red } 0 & \text{red } 0 & 0 & 0 \\ \text{red } 0 & \text{red } 0 & \text{red } 0 & \text{red } 0 & \text{red } 1 & \text{red } 0 & 0 & 0 \\ \text{red } 0 & \text{red } 0 & \text{red } 0 & \text{red } 0 & \text{red } 0 & \text{red } 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \text{blue } 0 & \text{blue } 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & \text{blue } 1 & \text{blue } 0 \end{bmatrix}$	

CSWAP, вентиль Фредкина	$ \begin{bmatrix} 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 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} $	
-------------------------	---	---

Индивидуальные задания

Исходя из варианта, подготовьте специальные кубитные состояния, используя вентили H, X, CNOT. Проведите анализ специального кубитного состояния. Постройте схему. Проверьте работоспособность схемы на квантовом компьютере.

Вариант	
1	$ 000\rangle + 111\rangle$
2	$ 101\rangle + 010\rangle$
3	$ 000\rangle + 001\rangle + 010\rangle + 011\rangle + 100\rangle + 101\rangle + 110\rangle + 111\rangle$

Необходимо собирать квантовую схему, используя квантовые логические элементы CNOT, X, H и Z. Подаем на вход цепочки элементов двухкубитовое состояние кубит, получаем выходное двухкубитовое состояние, и, используя матричное представление схемы, сравниваем результаты теоретических расчетов с полученными экспериментальными данными.

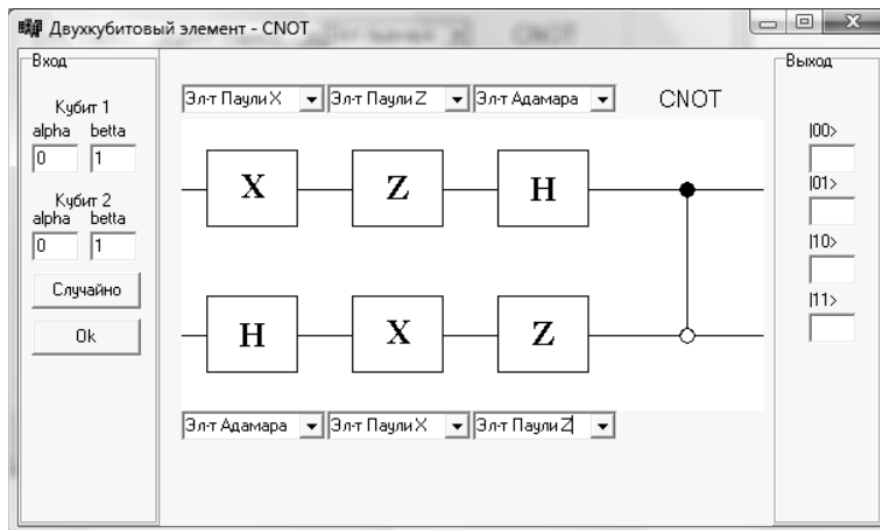


Рисунок 7 – Эксперимент

Лабораторная работа № 2 Тема «Алгоритм Дойча»

Цель работы: изучить работу алгоритма Дойча.

Теоретический материал

Используя вентили X, H и CNOT, можно проводить эксперименты с первым в мире алгоритмом квантовых вычислений: алгоритм Дойча является одним из наиболее распространенных квантовых алгоритмов, который определяет тип функции.

В отличие от классических алгоритмов, алгоритм Дойча демонстрирует ускорение алгоритмов квантовых вычислений.

Задача: у производителя есть два ящика с красками, чтобы покрасить два шарика разного веса в черный и белый цвета. В одном из них краска одного цвета, которая окрашивает оба вида мячей либо в черный, либо в белый цвет (рисунок 8). В другом ящике краска двух цветов, которая окрашивает шары одного веса в черный цвет, а шары другого веса – в белый (рисунок 9). Необходимо определить, в каком ящике находится двухцветная краска.



Рисунок 8 – Ящик с одноцветной краской

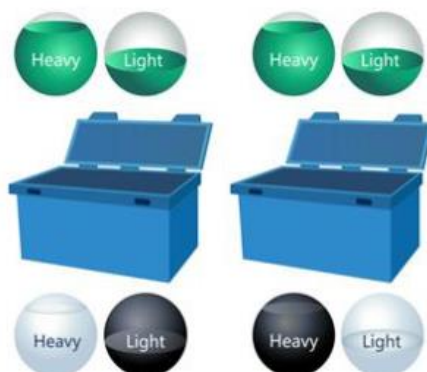


Рисунок 9 – Ящик с двухцветной краской

Представим шарик в виде переменной x , когда $x = 0$ – легкий шарик, а $x = 1$ – тяжелый шарик. Функция $F(x)$ представляет ящик с краской, где окрашиваются шарик. $F(x) = 0$ указывает, что x – шар белого цвета после окрашивания, а $F(x) = 1$ означает, что x – шар черного цвета после окрашивания.

Рассмотрим вычисление на классическом компьютере:

1. Поместим легкие шарик "0" в ящик с краской, чтобы получить результаты окрашивания $F(0) = 0$ или 1.



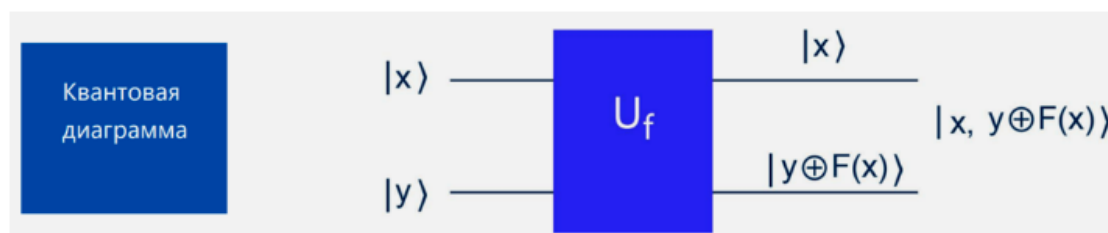
2. Поместим легкие шарик "1" в ящик с краской, чтобы получить результат окрашивания $F(1) = 0$ или 1.



3. Сравним $F(0)$ и $F(1)$: если $F(0) = F(1)$ – ящик с одноцветной краской, а $F(0) \neq F(1)$ – ящик с двухцветной краской.

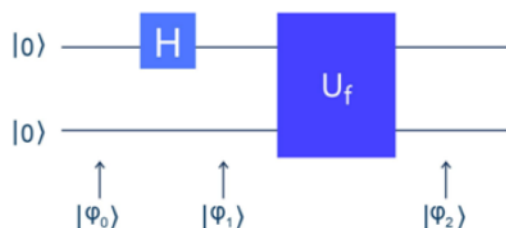


В квантовом мире, чтобы определить, является ли краска в ящике двухцветной, нам достаточно использовать ящик один раз.



Когда $y = 0$, состояние выхода второго кубита $|F(x)\rangle$.

Алгоритм Дойча:

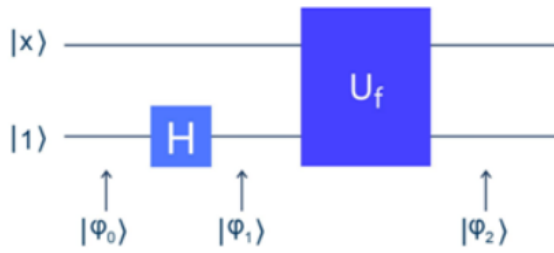


Когда $y = 0$, состояние выхода второго кубита $|F(x)\rangle$

$$|\varphi_0\rangle = |0, 0\rangle$$

$$|\varphi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle$$

$$|\varphi_2\rangle = \frac{1}{2}(|0, F(0)\rangle + |0, F(1)\rangle + |1, F(0)\rangle + |1, F(1)\rangle)$$



$$|\varphi_0\rangle = |x, 1\rangle$$

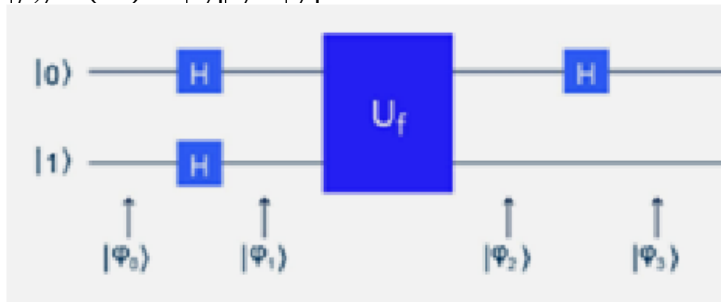
$$|\varphi_1\rangle = |x\rangle[|0\rangle - |1\rangle] = |x, 0\rangle - |x, 1\rangle$$

$$|\varphi_2\rangle = |x, 0 \oplus F(x)\rangle - |x, 1 \oplus F(x)\rangle = |x, F(x)\rangle - |x, \overline{F(x)}\rangle =$$

$$= |x\rangle[F(x)\rangle - |\overline{F(x)}\rangle]$$

$$|\varphi_2\rangle = \begin{cases} |x\rangle[|0\rangle - |1\rangle] & \text{если } F(x) = 0 \\ |x\rangle[|1\rangle - |0\rangle] & \text{если } F(x) = 1 \end{cases}^x$$

$$|\varphi_2\rangle = (-1)^{F(x)} |x\rangle[|0\rangle - |1\rangle]$$



$$|\varphi_2\rangle = |0, 0 \oplus F(0)\rangle - |0, 1 \oplus F(0)\rangle + |1, 0 \oplus F(1)\rangle - |1, 1 \oplus F(1)\rangle =$$

$$= |0, F(0)\rangle - |0, \overline{F(0)}\rangle + |1, F(1)\rangle - |1, \overline{F(1)}\rangle =$$

$$= (-1)^{F(0)} |0\rangle[|0\rangle - |1\rangle] + (-1)^{F(1)} |1\rangle[|0\rangle - |1\rangle] =$$

$$= [(-1)^{F(0)} |0\rangle + (-1)^{F(1)} |1\rangle][|0\rangle - |1\rangle]$$

$$|\varphi_2\rangle = \begin{cases} (\pm 1)[|0\rangle + |1\rangle][|0\rangle - |1\rangle] & \text{когда } F(0) = F(1) \\ (\pm 1)[|0\rangle - |1\rangle][|0\rangle - |1\rangle] & \text{когда } F(0) \neq F(1) \end{cases}$$

$$|\varphi_0\rangle = |0, 1\rangle$$

$$|\varphi_1\rangle = [|0\rangle + |1\rangle][|0\rangle - |1\rangle] = |0, 0\rangle - |0, 1\rangle + |1, 0\rangle - |1, 1\rangle$$

$$|\varphi_3\rangle = \begin{cases} (\pm 1)|0\rangle[|0\rangle - |1\rangle] & \text{когда } F(0) = F(1) \\ (\pm 1)|1\rangle[|0\rangle - |1\rangle] & \text{когда } F(0) \neq F(1) \end{cases}$$

1. Когда первый кубит выдает 0, это значит, что $F(0) = F(1)$.
2. Когда первый кубит выдает 1, это значит, что $F(0) \neq F(1)$.

Индивидуальные задания:

Построить функцию с использованием вентилях X, H и CNOT по заданному варианту. С помощью алгоритма Дойча проверить правильность построения схемы.

Построить схему. Привести теоретический расчет состояний кубитов на каждом этапе схемы. Проверить работоспособность схемы на квантовом компьютере с применением алгоритма Дойча.

Лабораторная работа № 3 Тема «Алгоритм Гровера, подготовка оракула»

Цель работы: научиться создавать оракул для поиска в алгоритме Гровера.

Теоретический материал

Задача заключается в поиске конкретной записи в неструктурированной базе данных. Например, в базе данных хранятся данные о цветах шаров, один из которых окрашен в красный цвет, а остальные – в зеленый. Пусть записи имеют значения от 1 до N .

Предположим, что при определении функции $F(x)$ может быть проверена запись. Когда $F(x)$ равен 0, то шарик зеленого цвета; когда $F(x)$ равен 1, то шарик красного цвета. Установим индекс x_0 красного шара, но при этом отсутствуют данные о его расположении. Тогда классическим алгоритмам необходимо поочередно проверить все записи.

В худшем случае классическим алгоритмам требуется N попыток, чтобы найти красный цвет. Сложность процесса составляет $\Theta(\sqrt{N})$.

Алгоритм Гровера способен ускорить процесс решения задачи.

Благодаря квантовой суперпозиции индексы N данных хранятся в одном квантовом состоянии из $\log_2 N$ кубитов. При использовании такого квантового состояния в качестве входа, одна проверка $F(x)$ позволяет получить выходы, соответствующие всем индексам N , то есть за один поиск алгоритм собирает всю информацию о цветах. Однако вся информация хранится в квантовом состоянии на выходе с равными вероятностями. При измерении $\log_2 N$ кубитов вероятность получения правильного ответа 0 составляет $1/N$. Следовательно, для увеличения вероятности получения x_0 необходимо провести дополнительные операции (см. рисунок ниже). При выполнении операции $\Theta(\sqrt{N})$ раз вероятность получить x_0 приближается к 1. Если значение является большим, то вероятность превышает $1 - 1/N$.

Квантовая схема алгоритма Гровера представлена на рисунке 10.

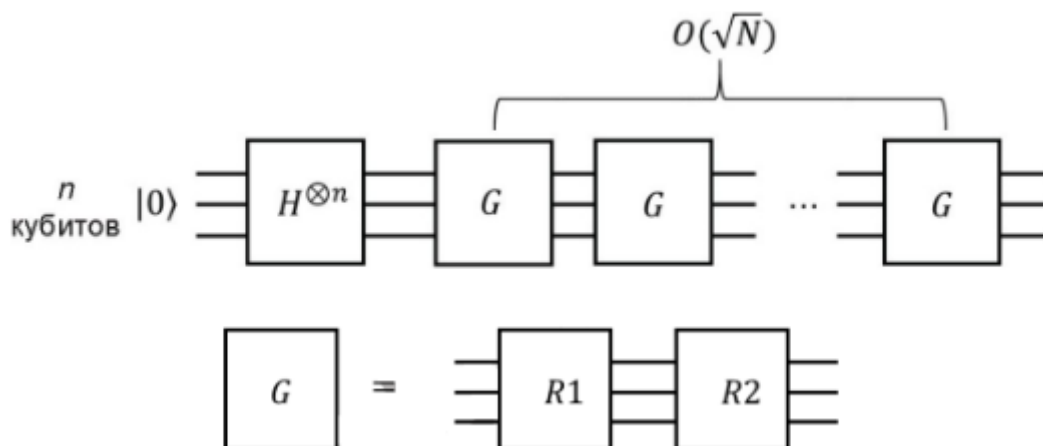


Рисунок 10 – Алгоритм Гровера

Здесь используется $n = \log_2 N$ кубитов. Первая операция $H^{\otimes n}$ – это операция Адамара над всеми кубитами, где индексы от 1 до N находятся в состоянии суперпозиции. Пусть $|\varphi\rangle$ – состояние после выполнения $H^{\otimes n}$, тогда

$$|\varphi\rangle = \frac{1}{\sqrt{N}}(|1\rangle + |2\rangle + \dots + |N\rangle) = \frac{1}{\sqrt{N}} \sum |x\rangle,$$

где $|x\rangle$ – базисное состояние системы из n кубитов, которое кодирует индекс x базы данных.

Вероятность всех базисных состояний N является одинаковой и равна $1/N$. Выполнение операции G повышает вероятность $|x_0\rangle$. G можно разделить на два этапа. $R1$ – операция, которая вычисляет функцию F для всех индексов и сохраняет результаты в состоянии суперпозиции:

$$|x\rangle = (-1)^{F(x)} |x\rangle.$$

Если зеленый цвет, то $F(x) = 0$ и $|x_0\rangle$ остается прежним; если красный цвет, то $F(x_0) = 1$, $|x_0\rangle$ получает знак "минус". Такая операция может быть выражена через оператор $R1 = I - 2|x_0\rangle\langle x_0|$. Дадим описание оператора: I – оператор идентичности и указывает на то, что ничего не происходит. За ним следует действие вычитания двух $|0\rangle$, в результате которого только состояние $|x_0\rangle$ меняет знак. Оператор $R2$ может быть выражен как $R2 = 2|\varphi\rangle\langle\varphi| - I$. I – указывает на то, что все базисные состояния меняют знаки, а при добавлении двух состояний $|\varphi\rangle$ только базис $|\varphi\rangle$ сохраняет исходный знак. Следующий рисунок демонстрирует необходимость выполнения операции $R2$.

Рассмотрим гильбертово пространство n кубитов, охватываемое двумя векторами $|\alpha\rangle$ и $|\beta\rangle$.

$|\beta\rangle$ – искомое значение, $|\beta\rangle = |x_0\rangle$, $|\alpha\rangle$ – суперпозиция всех базисных состояний,

кроме $|x_0\rangle$,
$$|\alpha\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x\rangle.$$

$|\alpha\rangle$ и $|\beta\rangle$ являются ортонормальными.

Начальное состояние суперпозиции в алгоритме Гровера может быть выражено как

$$|\varphi\rangle = \sqrt{\frac{N-1}{N}} |\alpha\rangle + \frac{1}{\sqrt{N}} |\beta\rangle.$$

$|\varphi\rangle$ имеет проекцию $\frac{1}{\sqrt{N}}$ на ось $|\beta\rangle$.

Соответствующие векторы $|\alpha\rangle$, $|\beta\rangle$ и $|\varphi\rangle$ изображены на следующем рисунке. После выполнения $R1$ $|x_0\rangle$ меняет знак и квантовое состояние переходит из $|\varphi\rangle$ в $\frac{\sqrt{N-1}}{\sqrt{N}} |\alpha\rangle - \frac{1}{\sqrt{N}} |\beta\rangle$ с проекцией $-\frac{1}{\sqrt{N}}$ на ось $|\beta\rangle$. Следовательно, $R1$ – операция, которая переворачивает вектор $|\varphi\rangle$ с $|\alpha\rangle$ в качестве оси симметрии. Из вышеприведенного анализа следует, что $R2$ сохраняет базис $|\varphi\rangle$ неизменным, при этом меняя знаки всех остальных базисов. Операция выполняет поворот квантового состояния с $|\varphi\rangle$ в качестве оси симметрии.

Результатом является поворот квантового состояния из $|\varphi\rangle$ в направление $|\beta\rangle$, а угол поворота удовлетворяет $\sin \theta = \frac{2N-1}{N}$. Когда значение N является большим, то $\theta \approx \sin \theta = \frac{2N-1}{N} \approx \frac{1}{\sqrt{N}}$.

Поэтому поворот квантового состояния около $\frac{\frac{\pi}{2}}{\frac{1}{\sqrt{N}}} = \frac{\pi\sqrt{N}}{4}$ раз позволяет получить

состояние $|\beta\rangle$ с большой вероятностью, при этом ошибка составляет менее $1/N$.

Индивидуальные задания

Создать оракул для поиска в алгоритме Гровера в соответствии с вариантом.

Схема оракула для схемы с двумя кубитами.

Теоретическая проверка работоспособности оракула в алгоритме Гровера для схемы с двумя кубитами.

Экспериментальная проверка работоспособности оракула в алгоритме Гровера для схемы с двумя кубитами.

Схема оракула для схемы с тремя кубитами.

Теоретическая проверка работоспособности оракула в алгоритме Гровера для схемы с тремя кубитами.

Экспериментальная проверка работоспособности оракула в алгоритме Гровера для схемы с тремя кубитами.

Вариант	
1	$ 00\rangle, 100\rangle$
2	$ 01\rangle, 011\rangle$
3	$ 10\rangle, 001\rangle$

Лабораторная работа № 4

Тема «Алгоритм Гровера, оператор диффузии Гровера»

Цель работы: научиться создавать оракул со вспомогательными кубитами и изучить оператор диффузии Гровера.

Теоретический материал

Квантовая схема алгоритма Гровера:

С n кубитами $n = \log_2 N$. Первая операция $H^{\otimes n}$ представляет вентиль Адамара, который применяется ко всем кубитам.

Данная операция хранит все порядковые номера от 1 до N в состояниях n кубитов. Состояние после выполнения операции записывается как

$$|\varphi\rangle, \text{ тогда } |\varphi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle.$$

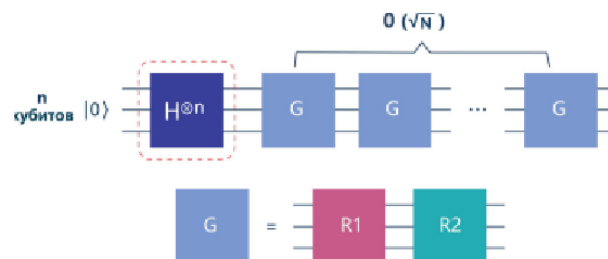


Рисунок 11 – Алгоритм Гровера

Операция G представляет квантовую операцию, которая увеличивает вероятность реализации состояния, соответствующего порядковому номеру красного шарика.

G состоит из двух этапов:

Первый этап операции $R1$ заключается в определении функций F всех порядковых номеров и их сохранении в квантовом состоянии

$$|x\rangle = (-1)^{F(x)}|x\rangle.$$

Второй этап операции $R2$ может быть представлен в виде

$$R2 = 2|\varphi\rangle\langle\varphi| - 1.$$

Пространство квантовых состояний можно представить как пространство, расширенное двумя векторами состояний $|\alpha\rangle$ и $|\beta\rangle$.

$|\beta\rangle$ – результат, который необходимо получить, $|\beta\rangle = |x_0\rangle$, $|\alpha\rangle$ – суперпозиция всех состояний порядковых чисел, за исключением

$$|x_0\rangle, |\alpha\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x\rangle, \text{ поэтому } |\varphi\rangle = \frac{\sqrt{N-1}}{\sqrt{N}} |\alpha\rangle + \frac{1}{\sqrt{N}} |\beta\rangle.$$

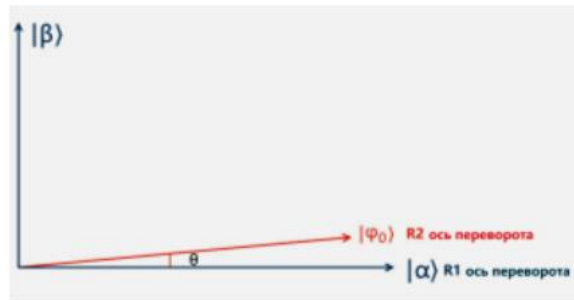


Рисунок 12 – График зависимости

Операция $R1$ представляет $|x\rangle = (-1)^{F(x)}|x\rangle$, $F(x \neq x_0) = 0, F(x_0) = 1$.

Таким образом, $R1$ преобразует

$$|\beta\rangle = |x_0\rangle = (-1)^{F(x_0)}|x_0\rangle = -|x_0\rangle, |\alpha\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x\rangle \text{ в постоянную величину. После выпол-}$$

нения операции $R1$,

$$|\varphi_0\rangle = \frac{\sqrt{N-1}}{\sqrt{N}} |\alpha\rangle + \frac{1}{\sqrt{N}} |\beta\rangle \text{ будет } |\varphi_0\rangle = \frac{\sqrt{N-1}}{\sqrt{N}} |\alpha\rangle - \frac{1}{\sqrt{N}} |\beta\rangle. \text{ Действие является}$$

эквивалентным переворачиванию вектора $|\varphi\rangle$ с $|\alpha\rangle$ в качестве оси симметрии.

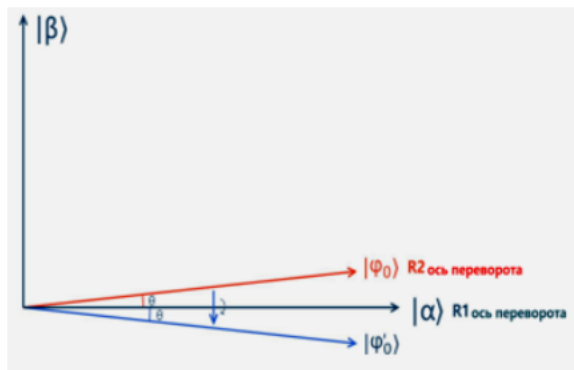


Рисунок 13 – Результат переворачивания Вектора

Операция R2 представляет $R2 = 2|\varphi\rangle\langle\varphi| - 1$. Проверните $|\varphi_0'\rangle = R1|\varphi_0\rangle$ с $|\varphi_0\rangle$ как ось, чтобы получить $|\varphi_1\rangle$.

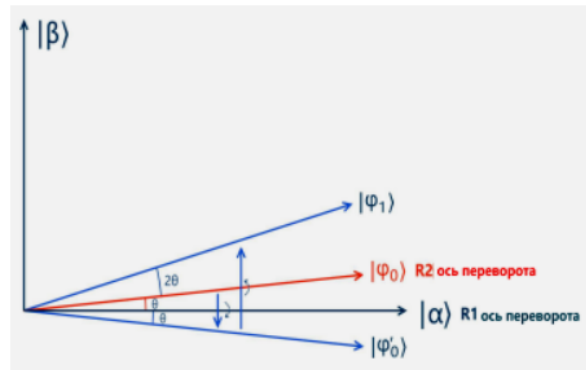


Рисунок 14 – Результат операции R2

На рисунке $|\varphi_0\rangle = \frac{\sqrt{N-1}}{\sqrt{N}}|\alpha\rangle + \frac{1}{\sqrt{N}}|\beta\rangle$, поэтому

$$\sin \theta = \frac{1}{\sqrt{N}}, \quad \cos \theta = \frac{\sqrt{N-1}}{\sqrt{N}}.$$

Тогда $\sin 2\theta = 2 \sin \theta \cos \theta = \frac{2\sqrt{N-1}}{N}$.

Конечный результат операции G - вращение $|\varphi_0\rangle$ в направлении

$|\beta\rangle$ к $|\varphi_1\rangle$ под углом 2θ , а $\sin 2\theta = \frac{2\sqrt{N-1}}{N}$.

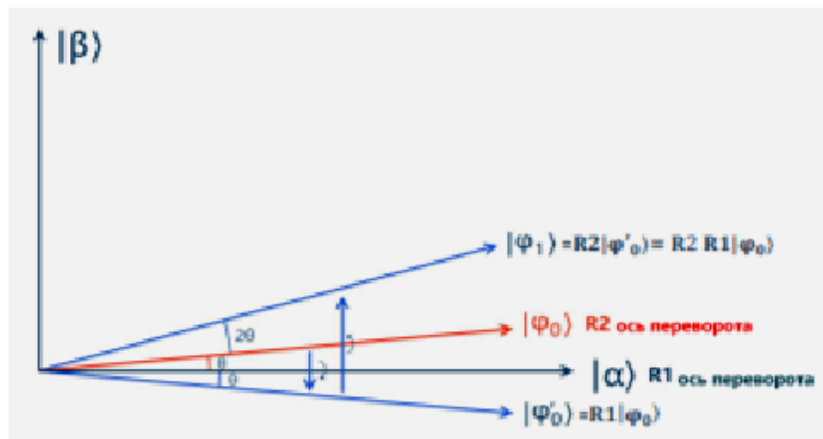


Рисунок 15 – Результат вращения

Тем же способом, при каждом выполнении операции R1, $|\varphi_n\rangle$ переворачивается с $|\alpha\rangle$ в качестве оси симметрии. Затем выполняется операция R2, где $|\varphi\rangle$ переворачивается в качестве оси симметрии. По сравнению с $|\varphi_n\rangle$ угол поворота $|\varphi_{n+1}\rangle$ увеличится на 2θ градуса по направлению оси.

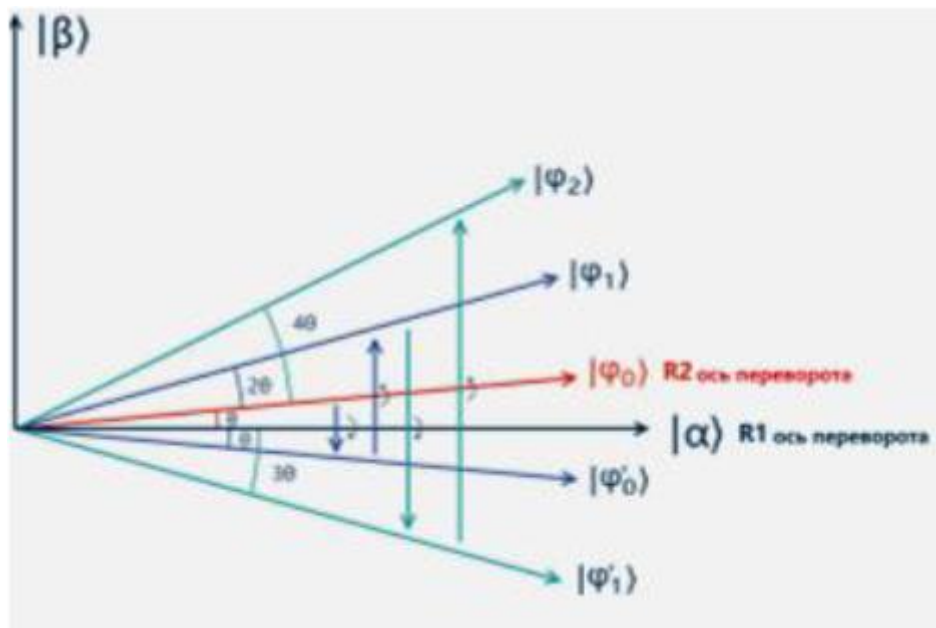


Рисунок 16 – Результат операций R_1 и R_2

Когда число N больше $N \gg 1$, $2\theta \approx \sin 2\theta = \frac{2\sqrt{N-1}}{N} \approx \frac{2}{\sqrt{N}}$.

Тогда вращения аппроксимируются до $\frac{\pi/2}{\frac{2}{\sqrt{N}}} = \frac{\pi\sqrt{N}}{4}$ раз и результат $|\beta\rangle$

будет достигнут с высокой вероятностью, а ошибка не будет превышать $1/N$. При этом, без учета коэффициента вычислительная сложность $O(\sqrt{N})$ составляет что значительно меньше среднего числа обычных запросов $N/2$.

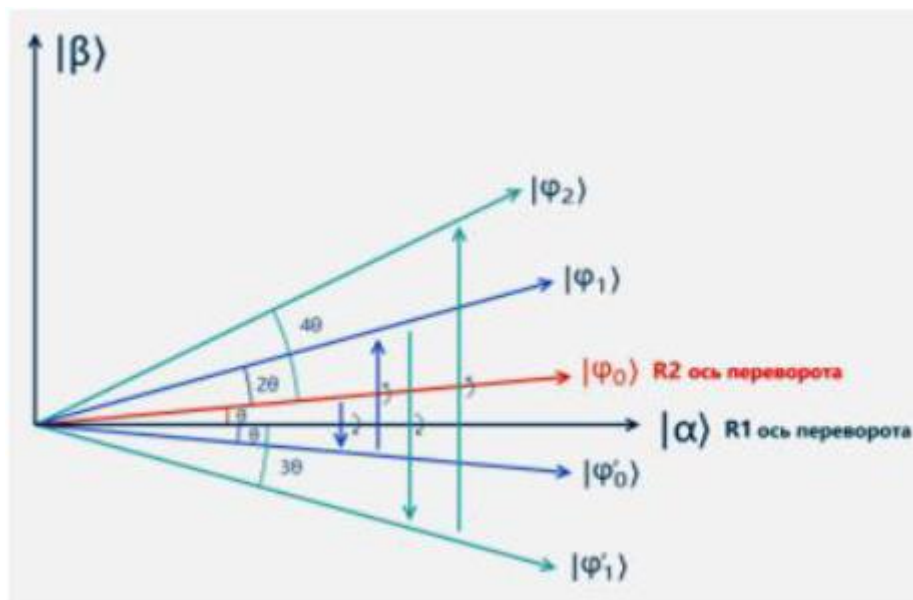


Рисунок 17 – Результат вращения

На рисунке, $|\varphi_0\rangle = \frac{\sqrt{N-1}}{\sqrt{N}}|\alpha\rangle + \frac{1}{\sqrt{N}}|\beta\rangle$,

поэтому $\sin \theta = \frac{1}{\sqrt{N}}$, $\cos \theta = \frac{\sqrt{N-1}}{\sqrt{N}}$,

тогда $\sin 2\theta = 2 \sin \theta \cos \theta = \frac{2\sqrt{N-1}}{N}$.

Конечный результат операции G – вращение $|\varphi_0\rangle$ в направлении $|\beta\rangle$

к $|\varphi_1\rangle$ под углом 2θ , а $\sin 2\theta = \frac{2\sqrt{N-1}}{N}$.

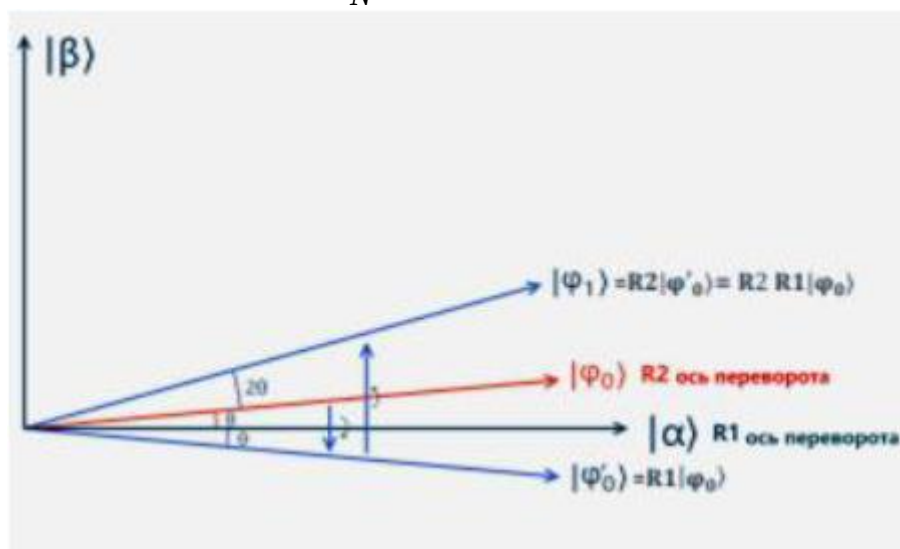


Рисунок 18 – Конечный результат G – вращение

Индивидуальное задание

Построить схему алгоритма Гровера со вспомогательными кубитами в соответствии с вариантами.

Привести схему алгоритма Гровера.

Привести расчеты состояний кубитов на каждом этапе схемы.

Выполнить теоретическую проверку работоспособности схемы.

Вариант	
1	$ 001\rangle$
2	$ 101\rangle$
3	$ 100\rangle$

Лабораторная работа № 5

Тема «Алгоритм Шора»

Цель работы: изучить работу алгоритма Шора.

Теоретический материал

Полный алгоритм имеет как классический, так и квантовый компоненты. Чтобы добраться до ответа, работа ведется на обоих видах машин. И это квантовая часть приводит нас к полиномиальной сложности по числу вентилей с помощью фазового оценивания, исчисления порядка, модульного возведения в степень и квантового преобразования Фурье.

Пусть нечетное M больше 3 и не кратно 3, 5, 7 и т. д. Также необходимо убедиться, что M не является степенью простого числа, и вы можете использовать метод Ньютона, чтобы это проверить.

Таким образом, M есть нечетное положительное число в $\mathbb{Z}$, которое не является степенью простого числа. С хорошей вероятностью оно окажется комплексным. Ниже приведен общий подход к алгоритму Шора с учетом M , как указано выше.

1. Выбрать случайное число a такое, что $1 < a < M$. Отслеживать эти значения, поскольку нам, возможно, придется повторить этот шаг еще раз.

2. Проверить, что $gcd(a, M) = 1$. Если не равно 1, то мы нашли делитель числа и все в порядке. Это маловероятно, но зато теперь мы знаем, что a и M являются взаимно простыми: у них нет общих целочисленных делителей.

3. Найти ненулевой порядок r для $\text{mod } M$. Это означает, что $a^r \equiv 1 \text{ mod } M$. Если r является нечетным, то вернуться к шагу 1 и повторить попытку с другим a .

4. Если r является четным, то мы имеем:

$$a^r \equiv 1 \text{ mod } M \rightarrow a^r - 1 \equiv 0 \text{ mod } M \rightarrow (a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1) \equiv 0 \text{ mod } M.$$

5. Теперь посмотреть на $gcd(a^{\frac{r}{2}} - 1, M)$ и, если необходимо,

$$gcd(a^{\frac{r}{2}} + 1, M).$$

Если ни один из них не равен 1, то мы нашли делитель числа M и добились успеха.

6. Если оба этих наибольших общих делителя равны 1, то мы повторяем все вышеизложенное с шага 1 с другим случайным a . Мы продолжаем делать это до тех пор, пока не найдем делитель.

Индивидуальные задания

С помощью алгоритма Шора необходимо факторизовать число 15.

Для этого необходимо построить схему для $a^x \text{ mod } N$, добавить QFT^{-1} для получения r – количества столбцов и выделить простые множители, входящие в число 15.

Построение схемы для $a^x \text{ mod } N$.

Построение полной схемы.

Проверка полученных результатов.

Вариант	
1	N=2
2	N=5
3	N=7

Список литературы

1. Роберт, С. Сатор. Танец с кубитами. Как на самом деле работают квантовые вычисления / С. Роберт. – СПб. : Питер, 2022. – 512 с.

2. Бернхард, К. Квантовые вычисления для настоящих айтишников / К. Бернхард. – СПб. : Питер, 2020. – 240 с.

3. Сысоев, С. С. Введение в квантовые вычисления. Квантовые алгоритмы: учеб. пособие / С. С. Сысоев. – СПб. : Изд-во С.-Петербург. ун-та, 2019. – 144 с.

4. Нильсен, М. Квантовые вычисления и квантовая информация / М. Нильсен, И. Чанг. – М. : Мир, 2006. – 824 с.

5. Попов, И. Ю. Квантовый компьютер и квантовые алгоритмы / И. Ю. Попов. – СПб : СПбГУ ИТМО, 2007. – 88 с.

6. Williams C. P. Explorations in quantum computing / C. P. Williams. – Santa Clara : Telos, 1998.

7. Gamel, O. Simplified Factoring Algorithms for Validating Small-Scale / O. Gamel, D. F. V. James // Quantum Information Processing Technologies. – 2013. – arXiv:1310.6446.

Учебное издание

Составители:

Хацкевич Мария Викторовна

Хацкевич Анна Сергеевна

Методические указания к лабораторным
и практическим занятиям по дисциплине

«Современные методы защиты компьютерных систем»

для специальности

6-05-0611-03 Искусственный интеллект

Ответственный за выпуск: Хацкевич М. В.

Редактор: Винник Н. С.

Компьютерная вёрстка: Соколюк А. П.

Корректор: Дударук С. А.

Подписано в печать 26.12.2024 г. Формат 60х84 ¹/₁₆. Бумага «Performer».
Гарнитура «Arial Narrow». Усл. печ. л. 1,4. Уч. изд. л. 1,5. Заказ № 1278. Тираж 30 экз.
Отпечатано на ризографе учреждения образования «Брестский государственный
технический университет». 224017, г. Брест, ул. Московская, 267.
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий № 3/1569 от 16.10.2017 г.