

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Национальный исследовательский Томский государственный университет

С.Н. Торгаев, И.Д. Шульга, Е.А. Юрченко, М.Л. Громов

ОСНОВЫ КВАНТОВЫХ ВЫЧИСЛЕНИЙ

*Рекомендовано в качестве учебного пособия
учебно-методической комиссией РФФ ТГУ*

Издательство STT
2020

УДК 681.3

ББК 32.971.3

T60

T60 С.Н. Торгаев, И.Д. Шульга, Е.А. Юрченко, М.Л. Громов
Основы квантовых вычислений : учебное пособие. – Томск : STT, 2020.
– 100 с.

Пособие содержит теоретический материал по основам квантовых вычислений. Приводится подробное описание квантовых гейтов и их воздействие на кубиты. Также в пособии представлен курс лабораторных работ, направленный на получение практических навыков по использованию квантовых гейтов и реализации простейших квантовых алгоритмов. Материал пособия предназначен для студентов ВУЗов, обучающихся на физико-математических и IT направлениях.

Рецензенты

кандидат технических наук, старший научный сотрудник

Института оптики атмосферы СО РАН

М.В. Тригуб

Доктор технических наук, профессор

профессор ОЭИ НИ ТПУ

А.И. Солдатов

Оглавление

ВВЕДЕНИЕ.....	4
ГЛАВА 1. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ.....	5
1.1. Математические основы квантовых вычислений.....	5
1.1.1. Комплексные числа	5
1.1.2. Линейные пространства	7
1.1.3. Линейные операторы.....	11
1.1.4. Эрмитовы и симметричные формы.....	16
1.2. Понятие квантового бита	19
1.3. Понятие квантовой системы.....	22
1.4. Измерение квантовой системы.....	23
1.5. Упражнения к Главе 1	26
ГЛАВА 2. КВАНТОВЫЕ ГЕЙТЫ	29
2.1. Гейт Адамара.....	29
2.2. Оператор <i>NOT</i> (Гейт <i>X</i>)	31
2.3. Гейт <i>Z</i>	32
2.4. Гейт <i>Y</i>	34
2.5. Гейт <i>S</i>	35
2.6. Гейт <i>T</i>	36
2.7. Гейты поворота <i>R_x</i> , <i>R_y</i> , <i>R_z</i>	37
2.8. Произвольные однокубитные унитарные гейты <i>U</i>	38
2.9. Контролируемые гейты	42
2.10. Упражнения к Главе 2	45
ГЛАВА 3. КВАНТОВЫЕ АЛГОРИТМЫ.....	47
3.1. Перепутанные состояния двух кубитов. Базис Белла	47
3.2. Сверхплотное кодирование	50
3.3. Квантовая телепортация.....	53
3.4. Алгоритм Дойча. Задача Дойча-Джозы.....	56
3.5. Алгоритм Гровера.....	63
3.6. Квантовое преобразование Фурье.....	67
3.7. Алгоритм Шора.....	69
3.8. Упражнения к Главе 3	73
ГЛАВА 4. ЛАБОРАТОРНЫЕ РАБОТЫ.....	74
Лабораторная работа №1	74
Лабораторная работа №2	85
Лабораторная работа №3	91
Лабораторная работа №4	96
СПИСОК ЛИТЕРАТУРЫ	99

Введение

Квантовые вычисления являются альтернативой классическим вычислениям. В основе квантовых вычислений лежит принцип квантовой суперпозиции – способность квантовой системы находиться в суперпозиции базовых (измеримых) состояний. Если у системы возможны 2 базовых состояний, то и любая суперпозиция (линейная комбинация) этих базовых состояний тоже возможное состояние системы. Из таких квантовых систем с двумя базовыми состояниями (их называют кубитами) и строят квантовые компьютеры: одно состояние моделирует константу 0, второе – 1.

Классический компьютер с памятью из n бит может одновременно выполнить некоторую операцию только над одним из 2^n возможных наборов. Чтобы вычислить значение некоторой Булевой функции от n аргументов для всех значений аргументов с помощью классического компьютера, придётся по очереди перебирать все 2^n наборов и вычислять значение функции на каждом наборе по отдельности. Благодаря квантовой суперпозиции, в квантовом компьютере с n кубитами можно одновременно представить все 2^n набора и выполнять операции над всеми наборами сразу. В результате мы можем вычислить значение функции сразу для всех 2^n комбинаций значений аргументов.

Такие возможности квантовых компьютеров могут значительно повысить эффективность решения ряда задач, в том числе, недостижимых для классических компьютеров. К таким задачам можно отнести обработку больших данных, разложение чисел на простые множители, генерирование случайных чисел, моделирование физических систем.

В данном пособии представлены теоретические материалы по основам квантовых вычислений. Теория проиллюстрирована на примерах простейших квантовых алгоритмов. Пособие предназначено для студентов высших учебных заведений, обучающихся на физико-математических и IT направлениях. Помимо теоретического материала, в пособии присутствует ряд лабораторных работ, позволяющих закрепить теоретический материал в системе *IBM Quantum Experience*.

ГЛАВА 1. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

1.1. Математические основы квантовых вычислений

1.1.1. Комплексные числа

\mathbb{N} \mathbb{Z} \mathbb{Q} \mathbb{R} \mathbb{C}

\mathbb{N} – множество натуральных чисел.

\mathbb{Z} – множество целых чисел.

\mathbb{Q} – множество рациональных чисел.

\mathbb{R} – множество вещественных чисел.

\mathbb{C} – множество комплексных чисел.

Определение 1

Комплексное число z – это упорядоченная пара вещественных чисел $z = (x, y)$, записанное в виде $z = x + i \cdot y$, где $i = \sqrt{-1}$, называемая мнимой единицей.

Определение 2

Функция комплексной переменной $z = (x, y)$ в общем случае имеет вид: $\omega = u(x, y) + i \cdot v(x, y)$, где $u(x, y)$ – вещественная часть функции ω , $v(x, y)$ – мнимая часть функции ω .

Примером функции комплексной переменной является показательная функция $\omega = e^z$, определяется сходящимся рядом:

$$e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}$$
$$e^{i\varphi} = \sum_{n=0}^{\infty} \frac{i^n \varphi^n}{n!} = \sum_{n=0}^{\infty} (-1)^n \frac{\varphi^{2n}}{(2n)!} + i \cdot \sum_{n=0}^{\infty} (-1)^n \frac{\varphi^{2n+1}}{(2n+1)!}$$
$$e^{i\varphi} = \cos(\varphi) + i \cdot \sin(\varphi)$$

Формулы Эйлера:

$$\cos(\varphi) = \frac{e^{i\varphi} + e^{-i\varphi}}{2}$$
$$\sin(\varphi) = \frac{e^{i\varphi} - e^{-i\varphi}}{2 \cdot i}$$

Алгебраическая форма записи: $z = x + i \cdot y$.

$x = \operatorname{Re}(z)$ – вещественная часть комплексного числа z .

$y = \operatorname{Im}(z)$ – мнимая часть комплексного числа z .

Тригонометрическая форма записи: $z = r \cdot (\cos(\varphi) + i \cdot \sin(\varphi))$, где $r = |z| = \sqrt{x^2 + y^2}$ – модуль комплексного числа, а $r = \text{Arg}(z) = \arg(z) + 2 \cdot \pi \cdot k$ – аргумент комплексного числа ($k = 0, \pm 1, \pm 2, \dots$).

Показательная форма записи: $z = r \cdot e^{i\varphi}$.

Определение 3

Комплексное число вида $\bar{z} = x - i \cdot y$ называется *комплексно-сопряжённым* комплексному числу вида $z = x + i \cdot y$.

Тогда можно записать:

$$\text{Re}(z) = \frac{1}{2}(z + \bar{z})$$

$$\text{Im}(z) = \frac{1}{2 \cdot i}(z - \bar{z}).$$

Определение 4

Комплексная плоскость \mathbb{C} – плоскость, на которой каждому комплексному числу $z = x + i \cdot y$ соответствует точка $z(x, y)$.

Операции над комплексными числами:

1. Равенство комплексных чисел z_1 и z_2 .

$$\text{Re}(z_1) = \text{Re}(z_2)$$

$$\text{Im}(z_1) = \text{Im}(z_2)$$

2. Сумма/разность комплексных чисел $z_1 = x_1 + i \cdot y_1$ и $z_2 = x_2 + i \cdot y_2$.

$$z = z_1 \pm z_2 = (x_1 \pm x_2) + i \cdot (y_1 \pm y_2)$$

3. Произведение комплексных чисел $z_1 = x_1 + i \cdot y_1$ и $z_2 = x_2 + i \cdot y_2$.

Алгебраическая запись:

$$z = z_1 \cdot z_2 = (x_1 \cdot x_2 - y_1 \cdot y_2) + i \cdot (x_1 \cdot y_2 + x_2 \cdot y_1)$$

Тригонометрическая запись:

$$z_1 = r_1 \cdot (\cos(\varphi_1) + i \cdot \sin(\varphi_1))$$

$$z_2 = r_2 \cdot (\cos(\varphi_2) + i \cdot \sin(\varphi_2))$$

$$z_1 \cdot z_2 = r_1 \cdot r_2 \cdot (\cos(\varphi_1 + \varphi_2) + i \cdot \sin(\varphi_1 + \varphi_2))$$

$$|z_1 \cdot z_2| = |z_1| \cdot |z_2|$$

$$\text{Arg}(z_1 \cdot z_2) = \text{Arg}(z_1) + \text{Arg}(z_2)$$

4. Деление комплексных чисел $z_1 = x_1 + i \cdot y_1$ и $z_2 = x_2 + i \cdot y_2$.

Алгебраическая запись (при $z_2 \neq 0$):

$$\frac{z_1}{z_2} = \frac{z_1 \cdot \bar{z}_2}{z_2 \cdot \bar{z}_2} = \frac{z_1 \cdot \bar{z}_2}{|z_2|^2}$$

Тригонометрическая запись:

$$z_1 = r_1 \cdot (\cos(\varphi_1) + i \cdot \sin(\varphi_1))$$

$$z_2 = r_2 \cdot (\cos(\varphi_2) + i \cdot \sin(\varphi_2))$$

$$\frac{z_1}{z_2} = \frac{r_1}{r_2} \cdot (\cos(\varphi_1 - \varphi_2) + i \cdot \sin(\varphi_1 - \varphi_2))$$

$$\left| \frac{z_1}{z_2} \right| = \frac{|z_1|}{|z_2|}$$

$$\text{Arg}\left(\frac{z_1}{z_2}\right) = \text{Arg}(z_1) - \text{Arg}(z_2)$$

5. Возведение в степень $z = x + i \cdot y$.

Формула Муавра – $z^n = r^n \cdot (\cos(n \cdot \varphi) + i \cdot \sin(n \cdot \varphi))$.

$$\sqrt[n]{z} = \sqrt[n]{r} \cdot \left(\cos\left(\frac{\varphi}{n} + \frac{2\pi k}{n}\right) + i \cdot \sin\left(\frac{\varphi}{n} + \frac{2\pi k}{n}\right) \right)$$

6. Обратный элемент комплексного числа z .

По сложению: $-z \rightarrow z + (-z) = 0$.

По умножению: $\forall z \neq 0 \exists z^{-1} \equiv \frac{1}{z}, z \cdot z^{-1} = 1$.

1.1.2. Линейные пространства

Определение 1

Линейное пространство (векторное пространство) – множество Φ элементов $\vec{a}, \vec{b}, \dots, \vec{c}$ (произвольной природы), определяемое следующими свойствами:

1. Для любых двух элементов $\vec{a}, \vec{b} \in \Phi$ определён элемент $\vec{a} + \vec{b} \in \Phi$, называемый суммой элементов \vec{a} и \vec{b} и обозначаемый $\vec{a} + \vec{b}$.

2. Для любого элемента $\vec{a} \in V$ и любого вещественного числа α определён элемент $\alpha \vec{a} \in V$, называемый произведением элемента \vec{a} на число α и обозначаемый $\alpha \vec{a}$.

3. Указанные два свойства подчинены следующим аксиомам:

3.1. Коммутативность сложения:

$$\vec{a} + \vec{b} = \vec{b} + \vec{a}.$$

3.2. Ассоциативность сложения:

$$(\vec{a} + \vec{b}) + \vec{c} = \vec{a} + (\vec{b} + \vec{c}).$$

3.3. Особая роль нулевого элемента:

$$\exists \text{ нулевой элемент } \vec{0} \text{ такой, что } \vec{a} + \vec{0} = \vec{a} \text{ и } \vec{0} + \vec{a} = \vec{a}.$$

3.4. Существование противоположного элемента:

$$\forall \vec{a} \in V \exists \vec{a}' \in V \text{ такой, что } \vec{a} + \vec{a}' = \vec{0} \text{ и } \vec{a}' + \vec{a} = \vec{0}.$$

3.5. Особая роль числового множителя на 1:

$$1 \oplus \vec{a} = \vec{a} \text{ и } \vec{a} \oplus 1 = \vec{a}.$$

3.6. Ассоциативность относительно числового множителя:

$$\alpha(\beta \vec{a}) = (\alpha\beta) \vec{a} \text{ и } (\alpha\beta) \vec{a} = \alpha(\beta \vec{a}).$$

3.7. Дистрибутивность относительно числового множителя:

$$(\alpha + \beta) \vec{a} = \alpha \vec{a} + \beta \vec{a} \text{ и } \alpha \vec{a} + \beta \vec{a} = (\alpha + \beta) \vec{a} \text{ для любых } \alpha, \beta \in \mathbb{R}.$$

3.8. Дистрибутивность относительно суммы элементов:

$$\alpha(\vec{a} + \vec{b}) = \alpha \vec{a} + \alpha \vec{b} \text{ и } \alpha \vec{a} + \alpha \vec{b} = \alpha(\vec{a} + \vec{b}) \text{ для любых } \alpha, \beta \in \mathbb{R}.$$

Определение 2

Линейное подпространство M линейного пространства Φ – подмножество $M \subset \Phi$ такое, что $\forall \vec{a}, \vec{b} \in M$ и любого числа α выполняются условия: $\vec{a} + \vec{b} \in M$ и $\alpha \vec{a} \in M$.

Определение 3

Линейная комбинация элементов $\vec{a}_1, \vec{a}_2, \dots, \vec{a}_n$ пространства Φ – сумма произведений элементов на произвольные вещественные числа: $\alpha_1 \vec{a}_1 + \alpha_2 \vec{a}_2 + \dots + \alpha_n \vec{a}_n$.

Определение 3.1

Тривиальная линейная комбинация элементов $\vec{a}_1, \vec{a}_2, \dots, \vec{a}_n$ – линейная комбинация $\alpha_1 \vec{a}_1 + \alpha_2 \vec{a}_2 + \dots + \alpha_n \vec{a}_n$, в которой все коэффициенты $\alpha, \beta, \dots, \gamma$ равны 0.

Определение 3.2

Множество векторов $\vec{a}_1, \vec{a}_2, \dots, \vec{a}_n$ называется линейно зависимым, если существует нетривиальная линейная комбинация этих векторов $\alpha_1 \vec{a}_1 + \alpha_2 \vec{a}_2 + \dots + \alpha_n \vec{a}_n$ равная 0.

Определение 3.3

Множество векторов $\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n$ называется *линейно независимым*, если никакая нетривиальная линейная комбинация этих векторов $\alpha_1 \vec{v}_1 + \alpha_2 \vec{v}_2 + \dots + \alpha_n \vec{v}_n$ не равна 0.

Определение 4

Базис в пространстве V – это множество n линейно независимых векторов $\{\vec{v}_1, \dots, \vec{v}_n\}$, а любые $n+1$ векторов линейно зависимы.

Определение 4.1

Размерность пространства V – число векторов базиса n , обозначаемое $\dim V$.

Определение 4.2

Конечномерное пространство V – пространство, в котором имеется конечный базис.

Определение 4.3

Бесконечномерное пространство V – пространство V , в котором можно найти системы линейно независимых векторов $\{\vec{v}_1, \dots, \vec{v}_n\}, \dots \in \mathbb{N}$.

Определение 4.4

В случае конечномерного пространства V любой $\vec{v} \in V$ является линейной комбинацией базисных векторов $\{\vec{v}_1, \dots, \vec{v}_n\}$, т.е. однозначно представляется в виде

$$\vec{v} = \alpha_1 \vec{v}_1 + \dots + \alpha_n \vec{v}_n = \sum_{i=1}^n \alpha_i \vec{v}_i.$$

Данное выражение является разложением вектора \vec{v} по базису $\{\vec{v}_1, \dots, \vec{v}_n\}$.

Определение 4.5

Компоненты (координаты) вектора \vec{v} в базисе $\{\vec{v}_1, \dots, \vec{v}_n\}$ – числовые коэффициенты $\alpha^i, i=1, \dots, n$ разложения этого вектора по базису.

Определение 4.6

Пусть $\{\vec{v}_1, \dots, \vec{v}_n\}$ и $\{\vec{w}_1, \dots, \vec{w}_n\}$ – два базиса в V . Пусть $\vec{v}_i \in \{\vec{w}_1, \dots, \vec{w}_n\}$ разложен по базису $\{\vec{w}_1, \dots, \vec{w}_n\}$:

$$\vec{v}_i = \alpha_{i1} \vec{w}_1 + \dots + \alpha_{in} \vec{w}_n = \sum_{j=1}^n \alpha_{ij} \vec{w}_j, \quad i=1, \dots, n,$$

где коэффициенты разложения $\alpha_{ij}, i=1, \dots, n$ – суть координаты i -го вектора базиса $\{\vec{v}_1, \dots, \vec{v}_n\}$ в базисе $\{\vec{w}_1, \dots, \vec{w}_n\}$.

Квадратная матрица n -го порядка $C = c_i^j$ – матрица перехода от базиса $\{\vec{c}_1, \dots, \vec{c}_n\}$ к базису $\{\vec{c}_1, \dots, \vec{c}_n\}$ в V .

Определение 5

Линейная оболочка множества $Ls\{U\}$ – это множество всех линейных комбинаций векторов, входящих в множество U .

Определение 6

Сумма $M+N$ линейных подпространств M и N линейного пространства V – это линейная оболочка векторов из $M \cup N$, т.е. множество всевозможных линейных комбинаций элементов из M и N :

$$M+N=Ls\{M \cup N\}.$$

Теорема 1

Пусть M и N – линейные пространства, дающие в сумме пространство V . Тогда для них эквивалентны следующие условия:

- $V=M+N$;
- всякий $\vec{v} \in V$ может быть однозначно представлен в виде $\vec{v} = \vec{m} + \vec{n}$, для некоторых $\vec{m} \in M, \vec{n} \in N$;
- если $\{\vec{c}_1, \dots, \vec{c}_a, \dots, \vec{c}_n\}$ – базис в M и $\{\vec{j}_1, \dots, \vec{j}_b, \dots, \vec{j}_n\}$ – базис в N , то множество $\{\vec{c}_1, \dots, \vec{c}_a, \dots, \vec{c}_n, \vec{j}_1, \dots, \vec{j}_b, \dots, \vec{j}_n\}$ образуют базис в V .

В результате: $\dim V = \dim M + \dim N$.

Теорема 2

Для любого подпространства M конечномерного линейного пространства V найдётся такое линейное подпространство N , что $V=M+N$.

Определение 7

Линейные пространства V и W называются *изоморфными*, если между их элементами установлено такое взаимно соответствие, при котором сумме любых двух элементов одного пространства отвечает сумма соответствующих элементов другого пространства, а произведению элемента одного пространства на некоторое число отвечает произведение на то же число соответствующего элемента другого пространства.

Обозначение: $V \cong W$.

Теорема 3

Все конечномерные комплексные (вещественные) линейные пространства одинаковой размерности n изоморфны.

1.1.3. Линейные операторы

Определение 1

Линейное преобразование (оператор) или эндоморфизм в линейном пространстве V – отображение $\hat{A}: V \rightarrow V$, линейное по аргументу, т.е. $\hat{A}(\alpha\vec{v}_1 + \beta\vec{v}_2) = \alpha\hat{A}\vec{v}_1 + \beta\hat{A}\vec{v}_2$, $\alpha, \beta \in \mathbb{R}$.

Обозначение: $\text{End } V$ – множество всех линейных операторов в линейном пространстве V .

Определение 1.1

Нулевой оператор – оператор $\hat{0}: V \rightarrow V$, т.е. оператор, отображающий все векторы пространства V в нуль.

Определение 1.2

Тождественный (единичный) оператор – оператор $\hat{1}: V \rightarrow V$, т.е. оператор, отображающий каждый вектор пространства V в самого себя.

Определение 2

Пусть $\{\vec{e}_1, \dots, \vec{e}_n\}$ – базис в V , а $\hat{A} \in \text{End } V$ – линейный оператор в V . Подействовав на каждый базисный вектор $\vec{e}_i, i = \overline{1, n}$, оператором \hat{A} , получим некоторые векторы $\hat{A}\vec{e}_i, i = \overline{1, n}$. Разложив каждый из полученных векторов по базису получим:

$$\hat{A}\vec{e}_i = \sum_{j=1}^n a_i^j \vec{e}_j, \quad i = \overline{1, n},$$

где коэффициенты $a_i^j, j = \overline{1, n}$ – суть координаты вектора $\hat{A}\vec{e}_i$ в базисе $\{\vec{e}_1, \dots, \vec{e}_n\}$.

Матрица линейного оператора \hat{A} в базисе $\{\vec{e}_1, \dots, \vec{e}_n\}$ – матрица A , матричными элементами которой являются коэффициенты $a_i^j, i, j = \overline{1, n}$, определяется как

$$A = (a_i^j) \in \text{Mat}(n, \mathbb{C}).$$

Матричный элемент линейного оператора \hat{A} в базисе $\{\vec{e}_1, \dots, \vec{e}_n\}$ – коэффициент a_i^j .

Формула, связывающая матрицы одного и того же линейного оператора \hat{A} в разных базисах

$$A' = C^{-1}AC,$$

где A и A' – матрицы одного и того же оператора \hat{A} в базисах $\{\vec{e}_1, \dots, \vec{e}_n\}$ и $\{\vec{e}'_1, \dots, \vec{e}'_n\}$ соответственно, C – матрица перехода от базиса $\{\vec{e}_1, \dots, \vec{e}_n\}$ к базису $\{\vec{e}'_1, \dots, \vec{e}'_n\}$, т.е.

$$C = (c_i^j),$$

$$\vec{e}'_i = \sum_{j=1}^n c_i^j \vec{e}_j,$$

$$\vec{e}'_i = \sum_{j=1}^n c_i^j \vec{e}_j, \dots$$

Определение 3

Определитель (детерминант) линейного оператора \hat{A} – определитель матрицы линейного оператора \hat{A} .

$$\det \hat{A} = \det A.$$

Обозначение: $\det \hat{A}$.

Определение 3.1

След линейного оператора \hat{A} – след матрица линейного оператора \hat{A} .

$$\text{Tr } \hat{A} = \text{Tr } A.$$

Обозначение: $\text{Tr } \hat{A}$.

Определение 4

Если определитель оператора \hat{A} не равен 0, то оператор называется *невырожденным линейным оператором \hat{A}* . В противном случае оператор \hat{A} называется *вырожденным линейным оператором \hat{A}* .

Алгебра линейных операторов

Пусть \hat{A} и \hat{B} – два линейных оператора в произвольном пространстве V , а α – вещественное число. Можно определить их сумму $\hat{A} + \hat{B} \in \text{End } V$, произведение $\hat{A} \cdot \hat{B} \in \text{End } V$, а также произведение $\alpha \hat{A}$ следующим образом:

1. $(\hat{A} + \hat{B}) \cdot \vec{e}_i = \hat{A} \cdot \vec{e}_i + \hat{B} \cdot \vec{e}_i$;
2. $\hat{A} \cdot \hat{B} \cdot \vec{e}_i = \hat{A} \cdot (\hat{B} \cdot \vec{e}_i)$;
3. $(\alpha \hat{A}) \cdot \vec{e}_i = \alpha (\hat{A} \cdot \vec{e}_i)$.

Свойства умножения операторов $\forall \hat{A}, \hat{B}, \hat{C} \in \text{End } V$ и \forall чисел α, β :

1. Дистрибутивность умножения операторов по сложению

$$\hat{A}(\alpha\hat{B} + \beta\hat{C}) = \alpha\hat{A}\hat{B} + \beta\hat{A}\hat{C},$$

$$(\alpha\hat{A} + \beta\hat{B})\hat{C} = \alpha\hat{A}\hat{C} + \beta\hat{B}\hat{C}.$$

2. Ассоциативность умножения операторов

$$\hat{A}(\hat{B}\hat{C}) = (\hat{A}\hat{B})\hat{C}.$$

3. Свойство единичного оператора

$$\hat{1}\hat{A} = \hat{A}\hat{1} = \hat{A}.$$

4. Некоммутативность умножения операторов

$$\hat{A}\hat{B} \neq \hat{B}\hat{A}.$$

Определение 5

Обратный оператор $\hat{B} \in \text{End } V$ к оператору $\hat{A} \in \text{End } V$ – оператор такой, что $\hat{A}\hat{B} = \hat{B}\hat{A} = \hat{1}$.

Обозначение: \hat{A}^{-1} .

Свойство обратного оператора: в конечномерном линейном пространстве матрица оператора \hat{A}^{-1} является обратной матрицей к матрице оператора \hat{A} , т.е.

$$\hat{A}\hat{A}^{-1} = \hat{A}^{-1}\hat{A} = 1_n.$$

Определение 6

k -ая степень оператора \hat{A} – оператор $\hat{A}^k = \hat{A}\hat{A}\dots\hat{A}$ (k -сомножителей, $k=1,2,3,\dots$).

Определение 7

Диагонализуемый (полупростой) оператор \hat{A} – оператор такой, что в некотором базисе $\{\vec{e}_1, \dots, \vec{e}_n\}$ матрица A оператора диагональная, т.е.

$$A = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix} = \text{diag}\{\lambda_1, \lambda_2, \dots, \lambda_n\}.$$

Определение 8

Собственное значение λ оператора $\hat{A} \in \text{End } V$ – такое число, что $\exists \hat{x} \neq 0$ такой, что $\hat{A}\hat{x} = \lambda\hat{x}$.

Определение 8.1

Собственный вектор оператора \hat{A} , отвечающий собственному значению λ – нетривиальное решение уравнения $\hat{A}\hat{x} = \lambda\hat{x}$.

Определение 8.2

Множество всех собственных векторов линейного оператора, соответствующих собственному числу λ , дополненное нулевым вектором, называется собственным подпространством этого оператора.

Определение 8.3

Геометрическая кратность собственного значения λ оператора \hat{A} – размерность M_λ , то есть $\dim M_\lambda$.

Определение 8.4

Спектр оператора \hat{A} – множество всех различных собственных значений оператора \hat{A} .

Теорема 1

Пусть $\vec{v}_1, \vec{v}_2, \dots, \vec{v}_k$ – собственные векторы оператора $\hat{A} \in \text{End } V$, отвечающие попарно различным собственным значениям $\lambda_1, \lambda_2, \dots, \lambda_k$ ($\lambda_i \neq \lambda_j$ при $i \neq j$). Тогда векторы $\vec{v}_1, \vec{v}_2, \dots, \vec{v}_k$ линейно независимы.

Теорема 2

Уравнение $(\hat{A} - \lambda \hat{I})\vec{v} = 0$ имеет ненулевые решения $\vec{v} \neq 0$ тогда и только тогда, когда $\det(\hat{A} - \lambda \hat{I}) = 0$.

Характеристические уравнения линейного оператора \hat{A} / матрицы A

$$f_{\hat{A}}(\lambda) = \det(\hat{A} - \lambda \hat{I}) = \begin{vmatrix} a_1^1 - \lambda & a_1^2 & a_1^3 & \dots & a_1^n \\ a_2^1 & a_2^2 - \lambda & a_2^3 & \dots & a_2^n \\ a_3^1 & a_3^2 & a_3^3 - \lambda & \dots & a_3^n \\ \dots & \dots & \dots & \dots & \dots \\ a_n^1 & a_n^2 & a_n^3 & \dots & a_n^n - \lambda \end{vmatrix} = 0,$$

где $A = (a_j^i)$ – матрица оператора \hat{A} в каком-либо базисе.

Многочлен n -ой степени имеет ровно n комплексных корней, если каждый корень учитывать столько раз, какова его алгебраическая кратность. Для характеристического многочлена это означает:

1. Характеристическое уравнение $f_{\hat{A}}(\lambda) = 0$ всегда имеет не менее одного, и не более n различных комплексных корней $\lambda_1, \lambda_2, \dots, \lambda_k$ для некоторого $k = \overline{1, n}$.

2. Характеристический многочлен представляется в виде

$$f_{\hat{A}}(\lambda) = (-1)^n (\lambda - \lambda_1)^{n_1} (\lambda - \lambda_2)^{n_2} \dots (\lambda - \lambda_k)^{n_k} = 0,$$

где n_1, n_2, \dots, n_k – целые положительные числа, причём $n_1 + n_2 + \dots + n_k = n$, n_i – алгебраическая кратность собственного значения λ_i .

Определение 9

Алгебраическая кратность n_i собственного значения λ_i – кратность λ_i как корня характеристического многочлена.

Определение 10

Собственное значение λ_i некоторого линейного оператора называется *простым*, если его алгебраическая кратность $n_i = 1$.

Определение 11

Собственное значение λ_i некоторого линейного оператора называется *вырожденным*, если его алгебраическая кратность $n_i > 1$.

Определение 11.1

Оператор $\hat{A} \in \text{End } V$ называется *оператором с простым спектром*, если все его собственные значения являются простыми.

Теорема 3

Пусть $\hat{A} \in \text{End } V$ – линейный оператор в конечном комплексном пространстве. Тогда справедливо:

1. \forall собственного значения λ_i геометрическая кратность не превосходит алгебраическую, т.е. $r_i \leq n_i$.
2. Оператор \hat{A} диагонализуем тогда и только тогда, когда $\forall \lambda_i r_i = n_i$.

Следствие: линейный оператор с простым спектром в конечномерном комплексном пространстве диагонализуется.

Определение 12

Нильпотентный оператор $\hat{A} \in \text{End } V$ – оператор, некоторая степень которого является нулевым оператором, т.е. $\hat{A}^k = \hat{0}$ для некоторого $k > 0$.

Теорема 4

Единственное собственное значение нильпотентного оператора \hat{A} равно 0. Характеристический многочлен любого нильпотентного оператора равен $f_{\hat{A}}(\lambda) = (-1)^n \lambda^n$, где $n = \dim V$.

Теорема 5

Если оператор \hat{A} в конечномерном линейном пространстве имеет единственное значение $\lambda_1 = 0$, то он нильпотентен.

Теорема 6

Ненулевой нильпотентный оператор не диагонализуем.

Теорема 7

Пусть $\alpha \in \mathbb{C}$ – некоторое комплексное число. Тогда:

1. Операторы \hat{A} и $\hat{A} + \alpha \hat{1}$ диагонализируемы и не диагонализируемы одновременно.
2. Если $\{\lambda_1, \lambda_2, \dots, \lambda_k\}$ – спектр оператора \hat{A} , то $\{\lambda_1 + \alpha, \lambda_2 + \alpha, \dots, \lambda_k + \alpha\}$ – спектр оператора $\hat{A} + \alpha \hat{1}$.
3. Каждое собственное пространство M_{λ_i} оператора \hat{A} , отвечающее собственному значению λ_i , является собственным пространством оператора $\hat{A} + \alpha \hat{1}$, отвечающим собственному значению $\lambda_i + \alpha$.
4. Характеристические многочлены операторов \hat{A} и $\hat{A} + \alpha \hat{1}$ связаны соотношением $f_{\hat{A}}(\lambda) = f_{\hat{A} + \alpha \hat{1}}(\lambda - \alpha)$.
5. Геометрическая и алгебраическая кратности каждого собственного значения λ_i оператора \hat{A} совпадают с геометрической и алгебраической кратностями соответственно собственного значения $\lambda_i + \alpha$ оператора $\hat{A} + \alpha \hat{1}$.

Следствие: пусть $\hat{A} \in \text{End } V$ – ненулевой нильпотентный оператор. Тогда оператор $\hat{A} + \alpha \hat{1}$ также не диагонализируем и имеет единственное вырожденное собственное значение α , для которого алгебраическая кратность равна n , а геометрическая кратность – 1. Характеристический многочлен оператора $\hat{A} + \alpha \hat{1}$ равен $f_{\hat{A} + \alpha \hat{1}}(\lambda) = f_{\hat{A}}(\alpha - \lambda)^n$.

1.1.4. Эрмитовы и симметричные формы

Определение 1

Эрмитова форма (эрмитово скалярное произведение) на комплексном линейном пространстве V – правило, которое каждой паре векторов $\vec{u}, \vec{v} \in V$ ставит в соответствие комплексное число, т.е. $\langle \vec{u}, \vec{v} \rangle \in \mathbb{C}$ причём выполняются следующие свойства $\forall \vec{u}, \vec{v}, \vec{w} \in V$ и $\forall \alpha, \beta \in \mathbb{C}$:

1. Линейность по второму аргументу

$$\langle \vec{u}, \alpha \vec{v} + \beta \vec{w} \rangle = \alpha \langle \vec{u}, \vec{v} \rangle + \beta \langle \vec{u}, \vec{w} \rangle.$$
2. Полулинейность по первому аргументу

$$\langle \alpha \vec{u} + \beta \vec{v}, \vec{w} \rangle = \alpha \langle \vec{u}, \vec{w} \rangle + \beta \langle \vec{v}, \vec{w} \rangle.$$
3. Эрмитовость

$$\langle \vec{u}, \vec{v} \rangle = \overline{\langle \vec{v}, \vec{u} \rangle}.$$

Определение 2

Матрица эрмитовой формы H в базисе $\{\vec{e}_1, \dots, \vec{e}_n\}$ – комплексная матрица n -го порядка, образованная попарным эрмитовым скалярным произведением базисных векторов, т.е.

$$h_{i,j} = \langle \vec{e}_i, \vec{e}_j \rangle, \quad i, j = \overline{1, n}$$

$$H = (h_{i,j}) \in \text{Mat}(n, \mathbb{C}).$$

Формула, связывающая матрицы одной и той же эрмитовой формы в разных базисах

$$H' = C^\dagger H C,$$

где H – матрица эрмитовой формы в базисе $\{\vec{e}_1, \dots, \vec{e}_n\}$, H' – матрица той же эрмитовой формы в базисе $\{\vec{e}'_1, \dots, \vec{e}'_n\}$, C – матрица перехода от базиса $\{\vec{e}_1, \dots, \vec{e}_n\}$ к базису $\{\vec{e}'_1, \dots, \vec{e}'_n\}$, $C^\dagger = \overline{C}^T$.

Определение 3

Ортогональные векторы $\vec{e}_1, \dots, \vec{e}_n$ – векторы такие, что $\langle \vec{e}_i, \vec{e}_j \rangle = \delta_{ij}$.

Определение 3.1

Изотропный вектор \vec{e} – вектор ортогональный сам себе, т.е. $\langle \vec{e}, \vec{e} \rangle = 0$.

Определение 4

В пространстве \mathbb{C}^n задан стандартный базис $\vec{e}_1 = (1, 0, \dots, 0)$, $\vec{e}_2 = (0, 1, \dots, 0)$, \dots , $\vec{e}_n = (0, \dots, 0, 1)$. В данном базисе зададим эрмитово скалярное произведение векторов $\vec{x} = (x^1, \dots, x^n) \in \mathbb{C}^n$ и $\vec{y} = (y^1, \dots, y^n) \in \mathbb{C}^n$ следующим образом:

$$\langle \vec{x}, \vec{y} \rangle = x^1 \overline{y^1} + \dots + x^p \overline{y^p} - \overline{x^{p+1}} y^{p+1} - \overline{x^{p+2}} y^{p+2} - \dots - \overline{x^{p+q}} y^{p+q},$$

где $p + q = r \leq n$.

Матрица этой эрмитовой формы в рассматриваемом базисе имеет вид

$$H = \text{diag}(1, 1, \dots, 1, -1, -1, \dots, -1, 0, 0, \dots, 0).$$

Ортонормированный базис – базис, в котором матрица эрмитовой формы имеет вид

$$H = \text{diag}(1, 1, \dots, 1, -1, -1, \dots, -1, 0, 0, \dots, 0).$$

Теорема 1

В любом конечномерном комплексном пространстве V с эрмитовой формой существует ортонормированный базис.

Определение 5

Эрмитово скалярное произведение на комплексном линейном пространстве V называется *невырожденным*, если в V нет ненулевых векторов, ортогональных векторам из V , т.е. $\langle \vec{v}, \vec{v} \rangle \neq 0, \forall \vec{v} \in V, \vec{v} \neq \vec{0}$.

Определение 5.1

Эрмитово скалярное произведение называется *положительно определённым*, если $\langle \vec{v}, \vec{v} \rangle > 0, \forall \vec{v} \in V, \vec{v} \neq \vec{0}$.

Теорема 2

Матрица положительно определённой эрмитовой формы в ортонормированном базисе равна единичной матрице.

Определение 6

Унитарное пространство (V, \langle, \rangle) – конечномерное комплексное линейное пространство V с положительно определённой эрмитовой формой \langle, \rangle .

Определение 6.1

Эрмитов (самосопряжённый) оператор $\hat{A} \in \text{End } V$ – оператор в унитарном пространстве (V, \langle, \rangle) такой, что $\langle \hat{A}\vec{v}, \vec{w} \rangle = \langle \vec{v}, \hat{A}\vec{w} \rangle, \forall \vec{v}, \vec{w} \in V$.

Теорема 3 (свойства эрмитова оператора)

1. Оператор \hat{A} эрмитов тогда и только тогда, когда матрица $A \in \text{Mat}(n, \mathbb{C})$ этого оператора в произвольном ортонормированном базисе эрмитова, т.е. $A = A^\dagger$.
2. Все собственные значения эрмитова оператора вещественные.
3. Собственные векторы эрмитова оператора, отвечающие различным собственным значениям, ортогональны друг другу.
4. Эрмитов оператор диагонализуем, а также в пространстве V существует ортонормированный базис, состоящий из собственных векторов эрмитова оператора \hat{A} .

Определение 7

Унитарный оператор $\hat{U} \in \text{End } V$ – оператор в унитарном пространстве (V, \langle, \rangle) такой, что $\langle \hat{U}\vec{v}, \hat{U}\vec{w} \rangle = \langle \vec{v}, \vec{w} \rangle, \forall \vec{v}, \vec{w} \in V$.

Теорема 4 (свойства унитарного оператора)

1. Оператор \hat{U} унитарен тогда и только тогда, когда $U \in \text{Mat}(n, \mathbb{C})$ этого оператора в произвольном ортонормированном базисе унитарна, т.е. $U^\dagger U = U U^\dagger = I_n$.
2. Все собственные значения унитарного оператора по модулю равны единице.

3. Собственные векторы унитарного оператора, отвечающие различным собственным значениям, ортогональны друг другу.
4. Унитарный оператор диагоналируем, а также в пространстве V существует ортонормированный базис, состоящий из собственных векторов унитарного оператора \hat{U} .

1.2. Понятие квантового бита

Единицей хранения информации является *бит*. Ячейка памяти классического компьютера объёмом в 1 бит может находиться в одном из двух различных состояниях. Эти состояния принято обозначать 0 и 1, саму такую ячейку также принято называть *битом*. Если бит находится в состоянии 0, то говорят, что он хранит значение 0, если же он находится в состоянии 1, то говорят, что он хранит значение 1.

При выполнении вычислений над битами можно совершать различные двоичные операции, например такие:

- отрицание (NOT): $y = \bar{x}$.

x	y
0	1
1	0

- конъюнкция («И», AND): $y = x_1 \wedge x_2$.

x_1	x_2	y
0	0	0
0	1	0
1	0	0
1	1	1

- дизъюнкция («ИЛИ», OR): $y = x_1 \vee x_2$.

x_1	x_2	y
0	0	0
0	1	1
1	0	1
1	1	1

Данные базовые операции являются основой любых дискретных вычислений. Любая более сложная логическая операция – это определённая комбинация базовых операций. С использованием набора базовых побитовых операций работает обычный компьютер.

Квантовый компьютер – это средство вычислительной техники в основе которого лежат законы квантовой механики [1-5]. В квантовых компьютерах для вычисления применяются так называемые квантовые

алгоритмы, которые используют эффекты квантовой механики, например, квантовый параллелизм и квантовая запутанность [1-5].

Квантовый компьютер оперирует так называемыми квантовыми битами. Можно определить квантовый бит, или сокращенно *q-бит* (*кубит*), как квантово-механическую систему, имеющую два состояния, обозначаемых, соответственно, как $|0\rangle$ и $|1\rangle$. Однако в отличие от классического случая в квантовой механике эти два состояния могут находиться в *состоянии суперпозиции*, то есть наиболее общее состояние квантового бита может быть записано как:

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

где α и β – комплексные коэффициенты. Другими словами, можно сказать, что законы квантовой механики допускают другие значения *кубита*, которые называются состояниями суперпозиции. Таким образом состояние суперпозиции представляют собой значения между экстремумами 0 и 1, а квантовый бит может принимать бесконечно много значений.

Для примера, проведем аналогию с выключателем света. Классический бит может принимать только одно из двух состояний – «включено» или «выключено» (рис. 1.1,а,б). Кубиты похожи на светильник с возможностью регулировки яркости (рис. 1.1,в) [6].

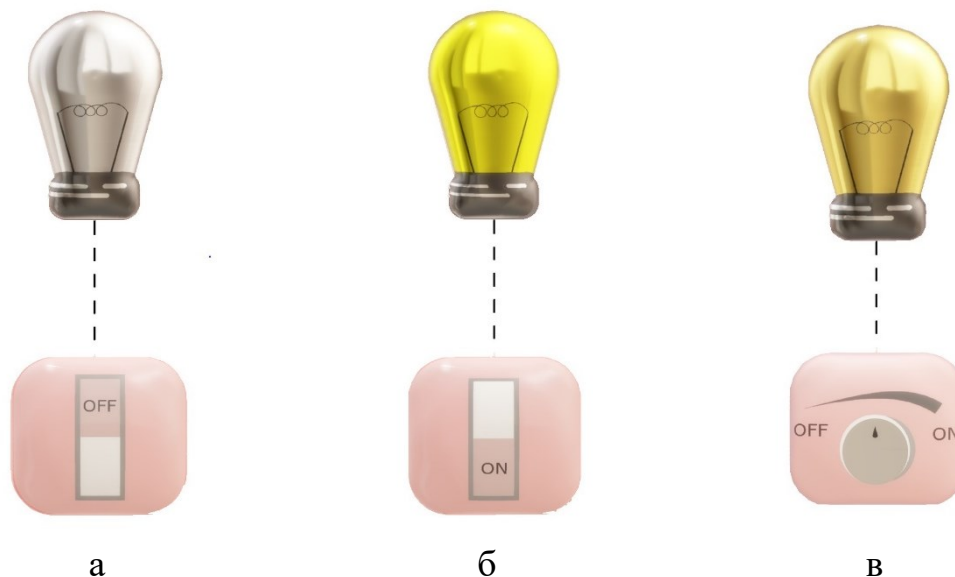


Рис. 1.1. Различие бита и кубита

Кубит можно определить, как вектор единичной длины в двумерном гильбертовом пространстве над полем комплексных чисел [1-4]. Состояния $|0\rangle$ и $|1\rangle$ вместе представляют собой базисные вектора. Как и все векторы, они указывают направление и имеют величину. Для записи

двух состояний кубитов можно использовать обозначения *бра* ($\langle |$ и *кет* ($| \rangle$) – обозначения Дирака. Векторы вида $| \rangle$ называются *кет*-векторами, а вида $\langle |$ *бра*-векторами. Обозначения *кет* соответствует следующим векторам: *Кет*-вектора, соответствующие нулевому и единичному состоянию кубита будут иметь следующий вид:

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

При измерении состояния системы с волновой функцией $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, вероятность обнаружить ее в состоянии $|0\rangle$ равна α^2 , а вероятность обнаружить ее в состоянии $|1\rangle$ равна β^2 . Сумма этих вероятностей равна единице:

$$|\alpha|^2 + |\beta|^2 = 1.$$

Данное соотношение называется *условием нормализации*.

То есть формула для волновой функции $|\Psi\rangle$ описывает, в какой пропорции бесконечное множество всех вариантов значений квантового состояния $|\Psi\rangle$ содержит варианты базисных состояний $|0\rangle$ и $|1\rangle$.

Визуализация состояния кубита возможна с помощью специального инструмента, называемого сферой Блоха. Сфера Блоха – это сфера с единичным радиусом, при этом точка на ее поверхности соответствует состоянию кубита.

Когда кубит находится в суперпозиции $|0\rangle$ и $|1\rangle$, вектор будет располагаться между двумя этими точками на сфере (угол θ). Вращение вокруг оси Z описывается углом φ , и отвечает за изменение фазы кубита. Сфера Блоха показана на рис. 1.2.

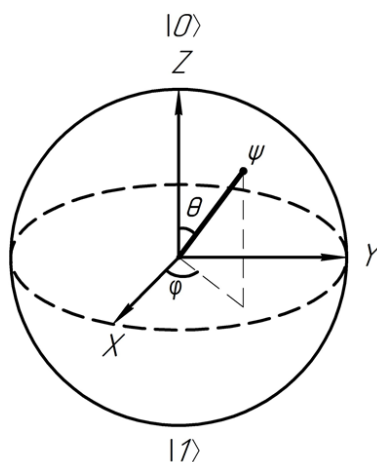


Рис. 1.2. Сфера Блоха. Состояние в верхней части сферы представляет $|0\rangle$, а состояние в нижней части сферы представляет $|1\rangle$

Физические реализации подобной системы с двумя состояниями могут быть разнообразными:

- электрон или ядро со спином $1/2$, ориентированным по или против направления магнитного поля;
- атом с двумя различными энергетическими состояниями;
- фотон с горизонтальной или вертикальной поляризацией;
- и т.д.

1.3. Понятие квантовой системы

Для квантовых вычислений как правило требуется больше одного кубита. Система, состоящая из нескольких кубитов, представляет собой тензорное произведение составляющих ее систем. Такая система называется *квантовой системой* [1-5].

Состояние квантовой системы, которая состоит из n кубитов можно представить следующим выражением:

$$|q_1\rangle \dots |q_n\rangle = (\alpha_0|0\rangle + \beta_0|1\rangle) \otimes (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes \dots \otimes (\alpha_{n-1}|0\rangle + \beta_{n-1}|1\rangle).$$

Приведем пример для системы двух кубитов. В данном случае мы имеем четырехмерный вектор единичной длины. Полностью смешанное состояние системы двух кубитов можно описать следующим образом:

$$|\psi\rangle = (\alpha_0|0\rangle + \beta_0|1\rangle) \otimes (\alpha_1|0\rangle + \beta_1|1\rangle) = \alpha_0\alpha_1|00\rangle + \alpha_0\beta_1|01\rangle + \beta_0\alpha_1|10\rangle + \beta_0\beta_1|11\rangle.$$

При этом сумма вероятностей нахождения в том или ином состоянии по-прежнему равна 1.

$$|\alpha_0\alpha_1|^2 + |\alpha_0\beta_1|^2 + |\beta_0\alpha_1|^2 + |\beta_0\beta_1|^2 = 1.$$

Как и в бинарном случае, этот набор возможных результатов называется измерительным базисом, а приводящие к ним комбинации значений – базисными состояниями. Тогда любое системное квантовое состояние мы можем записать как суперпозицию базисных состояний:

$$|\Psi\rangle = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle.$$

Физический смысл коэффициентов, стоящих в формуле перед базисными состояниями тот же, что и для одного кубита – это пропорция вариантов значений. Однако, в отличие от одного кубита, это значения не одиночного измерения, а комбинация двух измерений.

Таким образом, квантовая система из двух кубитов может находиться в одном из четырех состояний:

- $|00\rangle$ – оба кубита при измерении дают результат $|0\rangle$.

- $|01\rangle$ – первый кубит при измерении даёт $|0\rangle$, второй кубит даёт $|1\rangle$.
- $|10\rangle$ – первый кубит при измерении даёт $|1\rangle$, второй кубит даёт $|0\rangle$.
- $|11\rangle$ – оба кубита при измерении дают результат $|1\rangle$.

Другими словами, вектор состояния n -кубитной системы существует в 2^n -мерном комплексном пространстве и представляет собой сумму 2^n базисных векторов – базисных состояний.

Вероятностная природа квантовой механики проявляется в процессе измерений. Измерение является единственным способом извлечения данных, определяющих квантовое состояние. В результате измерения кубит немедленно коллапсирует. Допустим, одномерный кубит находится в состоянии суперпозиции. Если его измерить, то он примет одно конкретное значение – $|0\rangle$ или $|1\rangle$. После измерения кубита коэффициенты α и β , которыми характеризовалось его предыдущее состояние, будут утеряны.

Рассмотрим n -кубит:

$$|\Psi\rangle = \sum_{k=0}^{2^n-1} \alpha_k |k\rangle.$$

Так как длина вектора остается равной единицы, то можно записать

$$\sum_{k=0}^{2^n-1} |\alpha_k|^2 = 1.$$

Когда мы будем выполнять измерение состояния такого кубита, то получим одно из классических значений совокупности n битов от 000...0 до 111...1, где значение k (в двоичном представлении) появится с вероятностью $|\alpha_k|^2$. **Следует отметить, что для каких-то состояний вероятность может оказаться нулевой!**

1.4. Измерение квантовой системы

Чтобы получить информацию о состоянии квантовой системы необходимо выполнить его измерение. Для проведения измерений мы должны активно воздействовать на квантовую систему. В процессе измерения квантовой системы в выбранном базисе мы получим один из векторов этого базиса. В результате сразу же после измерения состояние квантовой системы разрушается, то есть система переходит в состояние, соответствующее наблюдаемому значению [1,2].

Приведем пример возможных исходов измерения для однокубитной системы:

- Если система находилась в состоянии $|0\rangle$, то при ее измерении мы получим тоже $|0\rangle$.
- Если система находилась в состоянии $|1\rangle$, то при ее измерении мы получим тоже $|1\rangle$.
- Если система находилась в состоянии суперпозиции $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, то в результате ее измерения мы получим вектор $|0\rangle$ с вероятностью $|\alpha|^2$, а вектор $|1\rangle$, с вероятностью $|\beta|^2$.

Следует отметить, что вероятность получения в процессе измерения конкретного вектора выбранного базиса ($|0\rangle$ или $|1\rangle$) равна квадрату модуля скалярного произведения вектора данной системы на этот вектор [1].

При этом, в результате измерений невозможно определить значения α и β , а также невозможно измерить повторно ту же самую систему, потому что, после измерения состояние квантовой системы разрушается. Таким образом, для получения максимально достоверной информации о состоянии системы при ее измерении необходимо выбирать базис, один из векторов которого наиболее близок к измеряемому кубиту [1-4].

В общем случае, вероятностный процесс измерения квантовой системы происходит следующим образом:

- Пусть у нас имеется квантовое состояние системы из n кубитов $|\psi\rangle$ и стандартный базис пространства состояний системы $k = \{|0\rangle, \dots, |2^n - 1\rangle\}$

$$|\Psi\rangle = \sum_{k=0}^{2^n-1} \alpha_k |k\rangle.$$

- При измерении состояния системы по отношению к базису k с вероятностью $|\alpha_i|^2$ результат измерения будет – $|i\rangle$.
- После измерения квантовая система будет находиться в состоянии – $|i\rangle$.
- После измерений амплитуды состояний отличных от $|i\rangle$ будут равны нулю: $\alpha_k = 0$ для $k \neq i$.

Рассмотрим пример измерения 2-кубита.

Пример 1.1: Выполним измерение следующего 2-кубита

$$|\Psi\rangle = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle$$

$$\alpha_0 = 0.3; \alpha_1 = 0.1; \alpha_2 = 0.9; \alpha_3 = 0.3$$

При измерении данного 2-кубита возможны четыре варианта:

•С вероятностью 0.09 получится значение 00 и 2-кубит перейдет в состояние $|00\rangle$.

•С вероятностью 0.01 получится значение 01 и 2-кубит перейдет в состояние $|01\rangle$.

•С вероятностью 0.81 получится значение 10 и 2-кубит перейдет в состояние $|10\rangle$.

•С вероятностью 0.09 получится значение 11 и 2-кубит перейдет в состояние $|11\rangle$.

В некоторых задачах требуется измерить состояние лишь некоторых кубитов в большом n -кубите. Приведем пример подобной ситуации для 3-кубита.

Пример 1.2: Выполним измерение первых двух битов кубита, но не будем трогать третий бит.

$$|\Psi\rangle = \alpha_0|000\rangle + \alpha_1|001\rangle + \alpha_2|010\rangle + \alpha_3|011\rangle + \alpha_5|101\rangle + \alpha_6|110\rangle$$

$$\alpha_0 = 0.3; \alpha_1 = -0.6; \alpha_2 = -0.1; \alpha_3 = -0.7; \alpha_5 = 0.1; \alpha_6 = -0.2$$

Видно, что в заданном нами примере отсутствуют состояния $|100\rangle$ и $|111\rangle$, то есть их коэффициенты α_4 и α_7 равны 0.

Так как нам необходимо измерить только два первых кубита, то возможны четыре варианта исхода: 00, 01, 10, 11. После измерения первые два кубита получают определенные значения, а значение третьего кубита не будет фиксировано.

•Вероятность наблюдения значения 00 будет определяться как $\alpha_0^2 + \alpha_1^2 = 0.09 + 0.36 = 0.45$, при этом новое состояние системы будет следующим:

$$|\Psi\rangle = \frac{1}{\sqrt{\alpha_0^2 + \alpha_1^2}} (\alpha_0|000\rangle + \alpha_1|001\rangle)$$

$$\alpha_0 = 0.3; \alpha_1 = -0.6$$

•Вероятность наблюдения значения 01 будет определяться как $\alpha_2^2 + \alpha_3^2 = 0.01 + 0.49 = 0.5$, при этом новое состояние системы будет следующим:

$$|\Psi\rangle = \frac{1}{\sqrt{\alpha_2^2 + \alpha_3^2}} (\alpha_2|010\rangle + \alpha_3|011\rangle)$$

$$\alpha_2 = -0.1; \alpha_3 = -0.7$$

Стоит отметить, что для нормализации состояния третьего не наблюдаемого кубита необходимо коэффициенты этих двух состояний

разделить на корень квадратный из вероятности появления данного исхода.

- Вероятность наблюдения значения 10 будет определяться как $\alpha_5^2 = 0.01$, при этом новое состояние системы будет $|101\rangle$.

- Вероятность наблюдения значения 11 будет определяться как $\alpha_6^2 = 0.04$, при этом новое состояние системы будет $|110\rangle$.

Заметьте, учитывая особенности нашего 3-кубита (отсутствие состояний $|101\rangle$ и $|110\rangle$), в последних двух случаях вероятность того, что третий бит соответственно принимает значения 1 и 0, равна 1.

Пример 1.3: Выполним измерение последних двух кубитов, но не будем трогать первый кубит.

$$|\Psi\rangle = \alpha_0|000\rangle + \alpha_1|001\rangle + \alpha_2|010\rangle + \alpha_3|011\rangle + \alpha_5|101\rangle + \alpha_6|110\rangle$$

$$\alpha_0 = 0.3; \alpha_1 = -0.6; \alpha_2 = -0.1; \alpha_3 = -0.7; \alpha_5 = 0.1; \alpha_6 = -0.2$$

- Вероятность наблюдения значения 00 будет определяться как $|\alpha_0|^2 = 0.09$, при этом новое состояние системы будет $|000\rangle$.

- Вероятность наблюдения значения 01 будет определяться как $\alpha_1^2 + \alpha_5^2 = 0.36 + 0.01 = 0.37$, при этом новое состояние системы будет следующим:

$$|\Psi\rangle = \frac{1}{\sqrt{\alpha_1^2 + \alpha_5^2}}(\alpha_1|001\rangle + \alpha_5|101\rangle)$$

$$\alpha_5 = 0.1; \alpha_1 = -0.6$$

- Вероятность наблюдения значения 10 будет определяться как $\alpha_2^2 + \alpha_6^2 = 0.01 + 0.04 = 0.05$, при этом новое состояние системы будет следующим:

$$|\Psi\rangle = \frac{1}{\sqrt{\alpha_2^2 + \alpha_6^2}}(\alpha_2|010\rangle + \alpha_6|110\rangle)$$

$$\alpha_2 = 0.1; \alpha_6 = -0.2$$

- Вероятность наблюдения значения 11 будет определяться как $\alpha_6^2 = 0.04$, при этом новое состояние системы будет $|011\rangle$.

1.5. Упражнения к Главе 1

1. Для квантовой системы $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ определите значение коэффициента β , если $\alpha = \frac{1}{\sqrt{2}}$.

2. Для квантовой системы $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ определите значение коэффициента α , если $\beta = 0.9$.

3. Докажите, что сумма вероятностей полностью смешанного состояния системы двух кубитов $|\alpha_0\alpha_1|^2 + |\alpha_0\beta_1|^2 + |\beta_0\alpha_1|^2 + |\beta_0\beta_1|^2$ равна 1.

4. Опишите возможные значения и их вероятности при измерении следующего 2-кубита:

$$|\Psi\rangle = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle$$

$$\alpha_0 = 0.3; \alpha_1 = 0.1; \alpha_2 = 0.64; \alpha_3 = 0.7$$

5. Опишите возможные значения и их вероятности при измерении следующего 3-кубита:

$$|\Psi\rangle = \alpha_0|000\rangle + \alpha_1|001\rangle + \alpha_2|010\rangle + \alpha_3|011\rangle + \alpha_4|100\rangle + \alpha_5|101\rangle + \alpha_6|110\rangle + \alpha_7|111\rangle$$

$$\alpha_0 = 0.3; \alpha_1 = -0.6; \alpha_2 = -0.1; \alpha_3 = -0.6; \alpha_4 = 0.1; \alpha_5 = -0.2; \alpha_6 = 0.2; \alpha_7 = -0.3$$

6. Опишите возможные результаты измерения первых двух бит 3-кубита:

$$|\Psi\rangle = \alpha_0|000\rangle + \alpha_1|001\rangle + \alpha_2|010\rangle + \alpha_3|011\rangle + \alpha_4|100\rangle + \alpha_5|101\rangle + \alpha_6|110\rangle + \alpha_7|111\rangle$$

$$\alpha_0 = 0.3; \alpha_1 = -0.6; \alpha_2 = -0.1; \alpha_3 = -0.6; \alpha_4 = 0.1; \alpha_5 = -0.2; \alpha_6 = 0.2; \alpha_7 = -0.3$$

7. Опишите возможные результаты измерения последних двух бит 3-кубита:

$$|\Psi\rangle = \alpha_0|000\rangle + \alpha_1|001\rangle + \alpha_2|010\rangle + \alpha_3|011\rangle + \alpha_4|100\rangle + \alpha_5|101\rangle + \alpha_6|110\rangle + \alpha_7|111\rangle$$

$$\alpha_0 = 0.3; \alpha_1 = -0.6; \alpha_2 = -0.1; \alpha_3 = -0.6; \alpha_4 = 0.1; \alpha_5 = -0.2; \alpha_6 = 0.2; \alpha_7 = -0.3$$

8. Запишите разложение Шмидта для следующих состояний 2-кубитовой системы:

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

9. Запишите разложение Шмидта для следующих состояний 2-кубитовой системы:

$$\frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

10. Покажите, что любые две диаметрально противоположные точки на сфере Блоха соответствуют двум ортогональным состояниям.

11. Проверьте унитарность следующих матриц:

$$a) \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$b) \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$e) \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

$$z) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$d) \frac{1}{2} \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}.$$

ГЛАВА 2. КВАНТОВЫЕ ГЕЙТЫ

Классические дискретные цепи представляют собой совокупность проводников и набора логических гейтов (совокупности полупроводниковых приборов). Логические гейты осуществляют преобразование информации, поступающей на их входы. В квантовых компьютерах преобразование информации осуществляется с использованием, так называемых, квантовых гейтов [1,2].

2.1. Гейт Адамара

Одиночный кубит, по определению, является суперпозицией двух квантовых состояний $|0\rangle$ и $|1\rangle$ каждое из которых может рассматриваться как носитель одного бита классической информации $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Чтобы создать состояния суперпозиции, используется гейт, называемый *гейт Адамара (H)*. *Гейт Адамара* является одним из наиболее полезных квантовых гейтов. Он задается матрицей:

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

Учитывая, что состояния кубита могут быть представлены в виде:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}; |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}; |\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix},$$

запишем выражения показывающие действия оператора Адамара на кубиты.

$$\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \\ H|1\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \\ H|\psi\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix} = \frac{\alpha + \beta}{\sqrt{2}}|0\rangle + \frac{\alpha - \beta}{\sqrt{2}}|1\rangle. \end{aligned}$$

Таким образом, действие оператора H на произвольный кубит можно описать формулой:

$$H|\psi\rangle = \frac{\alpha + \beta}{\sqrt{2}}|0\rangle + \frac{\alpha - \beta}{\sqrt{2}}|1\rangle.$$

В геометрической интерпретации кубита на сфере Блоха можно заметить, что в результате действия *гейта Адамара* на кубит в состоянии $|0\rangle$ переводит его в положение между состояниями $|0\rangle$ и $|1\rangle$, т.е. в

состояние $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. Соответственно в результате действия *гейта Адамара* состояние кубита $|1\rangle$ переводит его в положение между состояниями $|0\rangle$ и $|1\rangle$, только в другой полусфере, т.е. в состоянии $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$. Действие *гейта Адамара* на сфере Блоха показано на рис. 2.1.

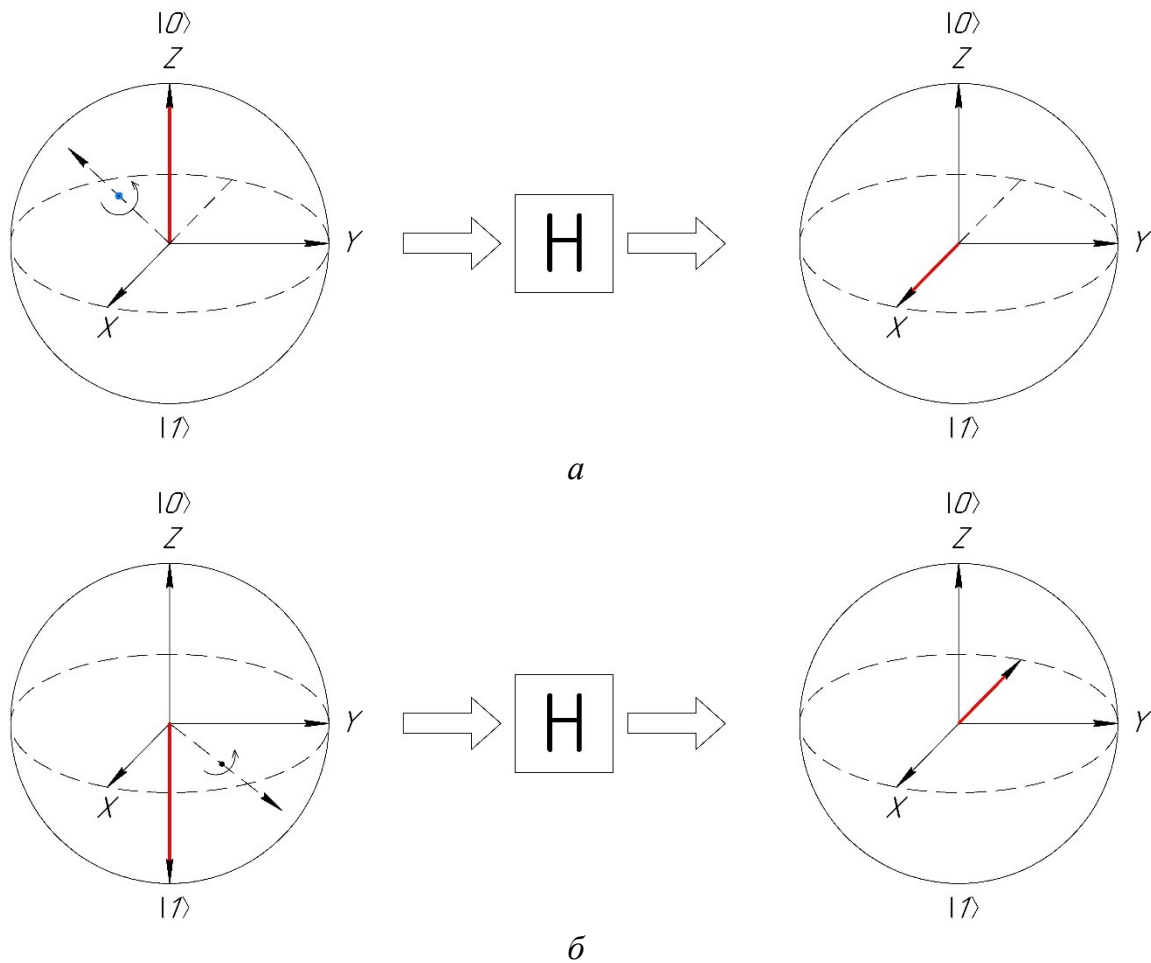


Рис. 2.1. Действие *гейта Адамара*: а) начальное состояние кубита $|0\rangle$ б) начальное состояние кубита $|1\rangle$

Оператор H является самосопряженным, а, следовательно, обратным к себе самому, то его повторное применение к базису Адамара вернет нам обычный базис. Другими словами, алгебраические вычисления дают $H^2=I$. То есть двукратное применение гейта H возвращает систему в исходное положение. Покажем самосопряженность *гейта Адамара* на примерах:

Пример 2.1. Для кубита в состоянии $|0\rangle$:

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle,$$

$$HH|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \left(\frac{1}{\sqrt{2}}\right)^2 \begin{pmatrix} 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle.$$

Пример 2.2. Для кубита в состоянии $|1\rangle$:

$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle,$$

$$HH|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \left(\frac{1}{\sqrt{2}}\right)^2 \begin{pmatrix} 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle.$$

Пример 2.3. Для кубита в состоянии $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$:

$$H|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix} = \frac{\alpha + \beta}{\sqrt{2}}|0\rangle + \frac{\alpha - \beta}{\sqrt{2}}|1\rangle,$$

$$HH|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix} = \left(\frac{1}{\sqrt{2}}\right)^2 \begin{pmatrix} 2\alpha \\ 2\beta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle + \beta|1\rangle.$$

Если у нас имеется система из n кубитов то применив **оператор Адамара** ко всем кубитам индивидуально, мы получим суперпозицию всех 2^n состояний:

$$(H \otimes H \otimes H \otimes H \dots \otimes H \otimes H)|0000\dots 00\rangle =$$

$$= \frac{1}{\sqrt{2^n}} ((|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \dots \otimes (|0\rangle + |1\rangle)) = \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} |z\rangle.$$

2.2. Оператор NOT (Гейт X)

В классических дискретных вычислениях оператор *NOT* – это оператор инверсии. В соответствии с этим определением классического оператора *NOT*, квантовый **гейт X** (т.е. гейт преобразующий информацию внутри кубита) может быть определен по аналогии:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \Rightarrow NOT |\Psi\rangle = \alpha|1\rangle + \beta|0\rangle.$$

Квантовым аналогом классического оператора *NOT* является матрица вида:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Покажем действия **гейта X** на кубит в различных состояниях.

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$X|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \beta|0\rangle + \alpha|1\rangle$$

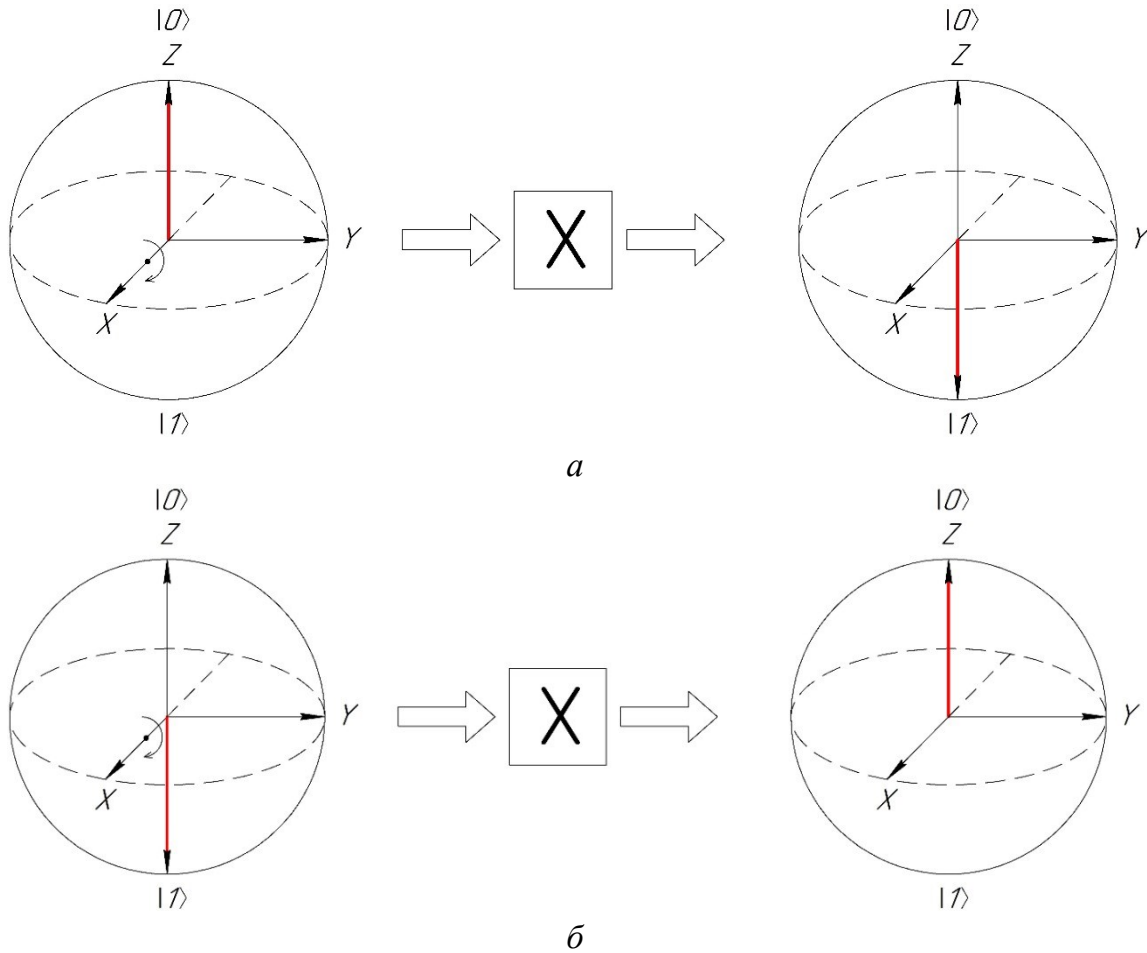


Рис. 2.2. Действие гейта X : а) начальное состояние кубита $|0\rangle$ б) начальное состояние кубита $|1\rangle$

С точки зрения интерпретации действия данного гейта на состояние кубита с помощью сферы Блоха, можно заметить, что происходит поворот вектора состояния на 180 градусов вокруг оси X (рис. 2.2).

2.3. Гейт Z

Определим сначала действие гейта Z на базисные вектора. Потребуем, чтобы он не изменял 0, а 1 переводил в -1:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \Rightarrow Z|\Psi\rangle = \alpha|0\rangle - \beta|1\rangle.$$

Тогда действию данного *гейта Z* отвечает матрица:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Покажем действия *гейта Z* на кубит в различных состояниях.

$$Z|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$Z|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix} = -|1\rangle$$

$$Z|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ -\beta \end{pmatrix} = \alpha|0\rangle - \beta|1\rangle$$

На сфере Блоха действие *гейта Z* соответствует повороту вектора вокруг оси *Z* на угол π (рис. 2.3).

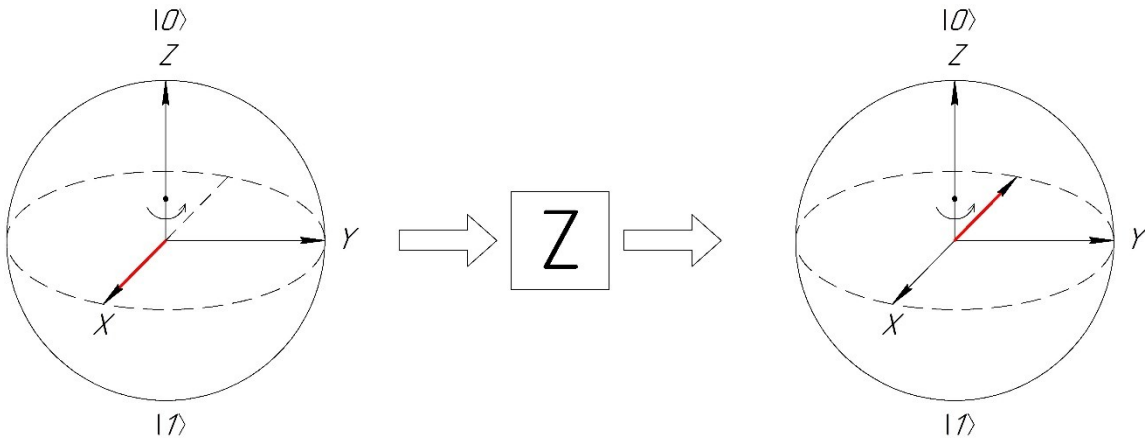


Рис. 2.3. Действие *гейта Z*

Отметим следующие два свойства *гейтов X* и *Z*:

$$HXH = Z,$$

$$HZH = X.$$

Приведем примеры показывающие данные свойства.

Пример 2.4. Для кубита в состоянии $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ применим операции *HXH*.

$$H|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix} = \frac{\alpha + \beta}{\sqrt{2}}|0\rangle + \frac{\alpha - \beta}{\sqrt{2}}|1\rangle$$

$$XH|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha - \beta \\ \alpha + \beta \end{pmatrix} = \frac{\alpha - \beta}{\sqrt{2}}|0\rangle + \frac{\alpha + \beta}{\sqrt{2}}|1\rangle$$

$$HXH|\psi\rangle = \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha - \beta \\ \alpha + \beta \end{pmatrix} = \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} \begin{pmatrix} 2\alpha \\ -2\beta \end{pmatrix} = \alpha|0\rangle - \beta|1\rangle$$

Как было показано ранее $Z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$, а, следовательно, можно заметить, что $HXH = Z$.

Пример 2.5. Для кубита в состоянии $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ применим операции HZH .

$$H|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix} = \frac{\alpha + \beta}{\sqrt{2}}|0\rangle + \frac{\alpha - \beta}{\sqrt{2}}|1\rangle$$

$$ZH|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha + \beta \\ \beta - \alpha \end{pmatrix} = \frac{\alpha + \beta}{\sqrt{2}}|0\rangle + \frac{\beta - \alpha}{\sqrt{2}}|1\rangle$$

$$HZH|\psi\rangle = \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha + \beta \\ \beta - \alpha \end{pmatrix} = \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} \begin{pmatrix} 2\beta \\ 2\alpha \end{pmatrix} = \beta|0\rangle + \alpha|1\rangle$$

Как было показано ранее $X|\psi\rangle = \beta|0\rangle + \alpha|1\rangle$, а, следовательно, можно заметить, что $HZH = X$.

2.4. Гейт Y

Гейт Y задается матрицей:

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

В отличие от предыдущих рассмотренных нами элементов, **гейт Y** является комплексным. Покажем действия **гейта Y** на кубит в различных состояниях.

$$Y|0\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ i \end{pmatrix} = i|1\rangle$$

$$Y|1\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -i \\ 0 \end{pmatrix} = -i|0\rangle$$

$$Y|\psi\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} -i\beta \\ i\alpha \end{pmatrix} = -i\beta|0\rangle + i\alpha|1\rangle$$

На сфере Блоха действие **гейта Y** соответствует повороту вектора вокруг оси Y на угол π (рис. 2.4).

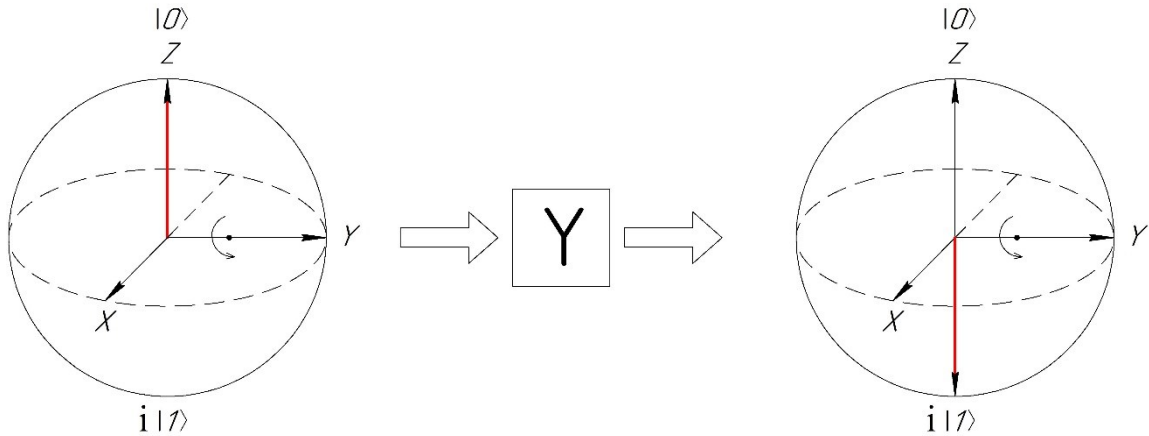


Рис. 2.4. Действие гейта Y

Отметим следующие свойства гейта Y :

$$YH = -Y.$$

Приведем пример показывающие данное свойство.

Пример 2.6. Для кубита в состоянии $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ применим операции YH .

$$H|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix} = \frac{\alpha + \beta}{\sqrt{2}}|0\rangle + \frac{\alpha - \beta}{\sqrt{2}}|1\rangle$$

$$YH|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} -i(\alpha - \beta) \\ i(\alpha + \beta) \end{pmatrix} = \frac{-i(\alpha - \beta)}{\sqrt{2}}|0\rangle + \frac{i(\alpha + \beta)}{\sqrt{2}}|1\rangle$$

$$HYH|\psi\rangle = \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} -i(\alpha - \beta) \\ i(\alpha + \beta) \end{pmatrix} = \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} \begin{pmatrix} 2i\beta \\ -2i\alpha \end{pmatrix} = i\beta|0\rangle - i\alpha|1\rangle$$

Как было показано ранее $Y|\psi\rangle = -i\beta|0\rangle + i\alpha|1\rangle$, а, следовательно, можно заметить, что $HYH = -Y$.

2.5. Гейт S

Гейт S задается матрицей:

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

Покажем действия гейта S на кубит в различных состояниях.

$$S|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$S|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ i \end{pmatrix} = i|1\rangle$$

$$S|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ i\beta \end{pmatrix} = \alpha|0\rangle + i\beta|1\rangle$$

Покажем действие *гейта S* на сфере Блоха (рис.2.5).

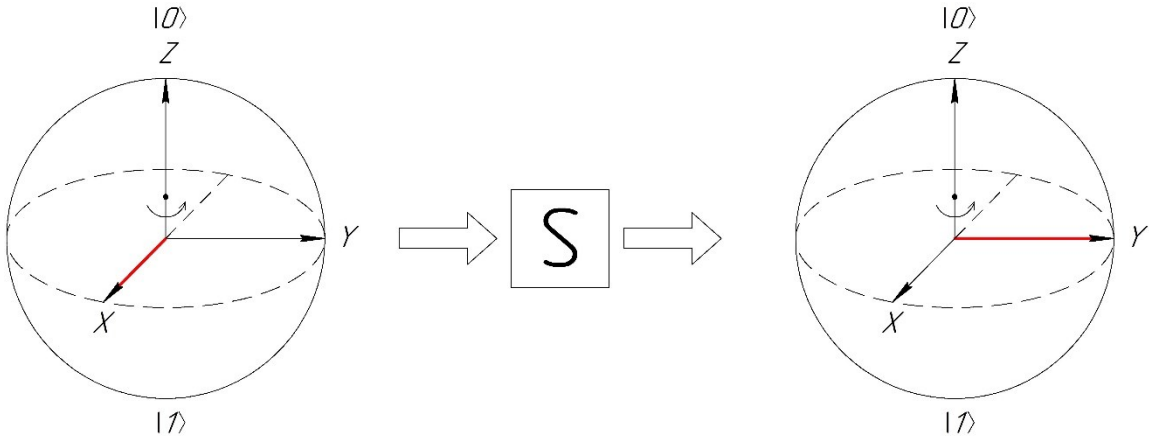


Рис. 2.5 Действие гейта *S*

2.6. Гейт *T*

Рассмотрим еще один комплексный логический *гейт T*, который часто обозначается как $\pi/4$. *Гейт T* задается матрицей:

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}.$$

Название *гейта T* определяется исторической возможностью представления матрицы этого гейта с точностью до общего фазового множителя $e^{i\frac{\pi}{8}}$ в виде:

$$T = e^{i\frac{\pi}{8}} \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix}.$$

Покажем действия *гейта T* на *кубит* в различных состояниях.

$$T|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$T|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ e^{i\frac{\pi}{4}} \end{pmatrix} = e^{i\frac{\pi}{4}}|1\rangle$$

$$T|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ e^{i\frac{\pi}{4}}\beta \end{pmatrix} = \alpha|0\rangle + e^{i\frac{\pi}{4}}\beta|1\rangle$$

Покажем действие **гейта T** на сфере Блоха (рис. 2.6).

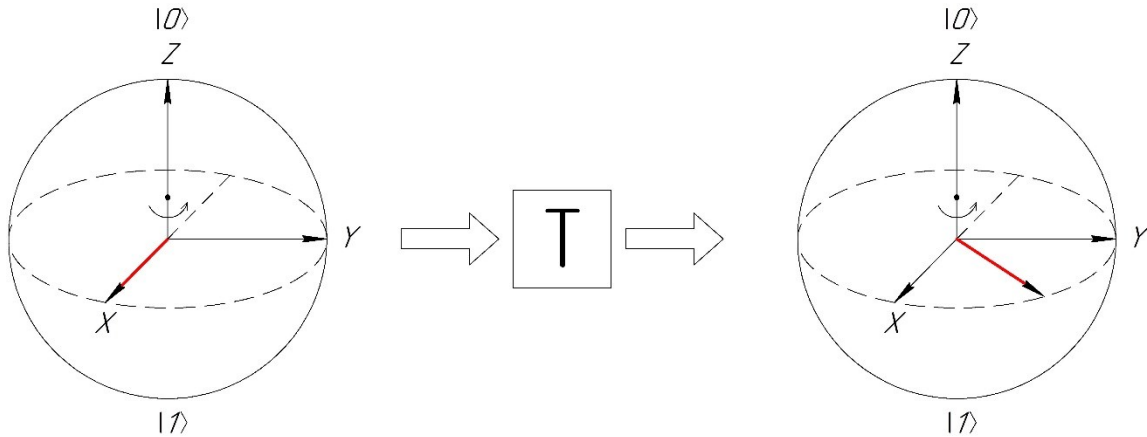


Рис. 2.6. Действие **гейта T**

Таким образом, **гейт T** не изменяет коэффициент при базисном векторе 0 и меняет фазу коэффициента при базисном векторе 1.

2.7. Гейты поворота R_x , R_y , R_z

Гейт R_x на сфере Блоха соответствует вращению кубита вокруг оси X на заданный угол. В матричном виде данный гейт можно записать как [1,2,6]:

$$R_x(\theta) = e^{-i\frac{\theta}{2}X} = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -i \cdot \sin\left(\frac{\theta}{2}\right) \\ -i \cdot \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}.$$

По аналогии с **гейтом R_x** , **гейты R_y** и **R_z** соответствуют вращению **кубита** вокруг осей Y и Z . При этом их можно определить как:

$$R_y(\theta) = e^{-i\frac{\theta}{2}Y} = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix},$$

$$R_z(\theta) = e^{-i\frac{\theta}{2}Z} = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix}.$$

2.8. Произвольные однокубитные унитарные гейты U

Произвольный однокубитный унитарный оператор может быть записан в виде [1,2,6]:

$$U = e^{i\alpha} R_{\vec{n}}(\theta),$$

где $R_{\vec{n}}(\theta)$ – оператор поворота на угол θ вокруг оси, определенной единичным вектором \vec{n} , α и θ – действительные числа.

Гейт $U1$ осуществляет вращение одного кубита вокруг оси Z . В матричном виде данный гейт можно записать как:

$$U1(\lambda) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\lambda} \end{pmatrix}.$$

В зависимости от значения угла λ данный гейт является эквивалентом других гейтов:

$$U1(\pi) = Z,$$

$$U1\left(\frac{\pi}{2}\right) = S,$$

$$U1\left(\frac{\pi}{4}\right) = T.$$

Гейт $U2$ осуществляет вращение одного кубита вокруг $X+Y$ осей. Согласно теореме $X-Y$ разложения для однокубитового гейта данный оператор определяется как:

$$U2(\varphi, \lambda) = R_z\left(\varphi + \frac{\pi}{2}\right) R_x\left(\frac{\pi}{2}\right) R_z\left(\lambda - \frac{\pi}{2}\right).$$

В матричном виде данный гейт можно записать как:

$$U2(\varphi, \lambda) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -e^{i\lambda} \\ e^{i\varphi} & e^{i(\varphi+\lambda)} \end{pmatrix}.$$

Можно заметить, что $U2(0, \pi) = H$.

Гейт $U3$ – это универсальный однокубитный поворотный затвор с тремя углами Эйлера. Данный гейт определяется как:


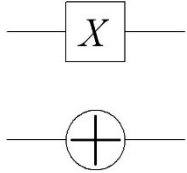





$$U3(\theta, \varphi, \lambda) = Rz\left(\varphi - \frac{\pi}{2}\right) Rx\left(\frac{\pi}{2}\right) Rz(\pi - \theta) Rx\left(\frac{\pi}{2}\right) Rz\left(\lambda - \frac{\pi}{2}\right),$$

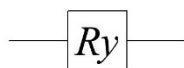
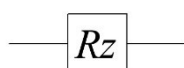
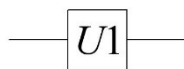
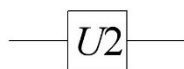
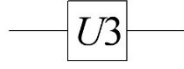
$$U3(\theta, \varphi, \lambda) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -e^{i\lambda} \sin\left(\frac{\theta}{2}\right) \\ e^{i\varphi} \sin\left(\frac{\theta}{2}\right) & e^{i(\varphi+\lambda)} \cos\left(\frac{\theta}{2}\right) \end{pmatrix}.$$

Можно заметить, что $U3\left(\theta, -\frac{\pi}{2}, \frac{\pi}{2}\right) = Rx(\theta)$ и $U3(\theta, 0, 0) = Ry(\theta)$.

В таблице 2.1 представлены графические обозначение однобитовых гейтов и результат их воздействия на произвольный кубит $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

Таблица 2.1. Однокубитные гейты

Название	Графическое обозначение	Матрица	Результат воздействия
Гейт H		$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	$\frac{\alpha + \beta}{\sqrt{2}} 0\rangle + \frac{\alpha - \beta}{\sqrt{2}} 1\rangle$
Гейт X		$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\beta 0\rangle + \alpha 1\rangle$
Гейт Z		$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\alpha 0\rangle - \beta 1\rangle$
Гейт Y		$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$-i\beta 0\rangle + i\alpha 1\rangle$
Гейт S		$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$	$\alpha 0\rangle + i\beta 1\rangle$
Гейт T		$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$	$\alpha 0\rangle + e^{i\frac{\pi}{4}}\beta 1\rangle$
Гейт Rx		$Rx(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -i \cdot \sin\left(\frac{\theta}{2}\right) \\ -i \cdot \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$	$\left(\alpha \cos\left(\frac{\theta}{2}\right) - i\beta \sin\left(\frac{\theta}{2}\right)\right) 0\rangle + \left(\beta \cos\left(\frac{\theta}{2}\right) - i\alpha \sin\left(\frac{\theta}{2}\right)\right) 1\rangle$

Гейт R_y		$R_y(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$	$\left(\alpha \cos\left(\frac{\theta}{2}\right) - \beta \sin\left(\frac{\theta}{2}\right)\right) 0\rangle + \left(\alpha \sin\left(\frac{\theta}{2}\right) + \beta \cos\left(\frac{\theta}{2}\right)\right) 1\rangle$
Гейт R_z		$R_z(\theta) = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix}$	$\alpha e^{-i\frac{\theta}{2}} 0\rangle + \beta e^{i\frac{\theta}{2}} 1\rangle$
Гейт U_1		$U_1(\lambda) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\lambda} \end{pmatrix}$	$\alpha 0\rangle + \beta e^{i\lambda} 1\rangle$
Гейт U_2		$U_2(\varphi, \lambda) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -e^{i\lambda} \\ e^{i\varphi} & e^{i(\varphi+\lambda)} \end{pmatrix}$	$\frac{(\alpha - \beta e^{i\lambda})}{\sqrt{2}} 0\rangle + \frac{(\alpha e^{i\varphi} + \beta e^{i(\varphi+\lambda)})}{\sqrt{2}} 1\rangle$
Гейт U_3		$U_3(\theta, \varphi, \lambda) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -e^{i\lambda} \sin\left(\frac{\theta}{2}\right) \\ e^{i\varphi} \sin\left(\frac{\theta}{2}\right) & e^{i(\varphi+\lambda)} \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$	$\left(\alpha \cos\left(\frac{\theta}{2}\right) - \beta e^{i\lambda} \sin\left(\frac{\theta}{2}\right)\right) 0\rangle + \left(\alpha e^{i\varphi} \sin\left(\frac{\theta}{2}\right) + \beta e^{i(\varphi+\lambda)} \cos\left(\frac{\theta}{2}\right)\right) 1\rangle$

Используя гейты поворота R и унитарные гейты U , можно получать произвольные состояния суперпозиции $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Приведем примеры получения различных состояний суперпозиции кубита.

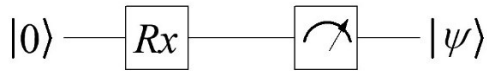
Пример 2.7: Получим кубит в состоянии суперпозиции $|\psi\rangle = \sqrt{0.8}|0\rangle + \sqrt{0.2}|1\rangle$, применив воздействие гейта R_x к кубиту, который находится в исходном состоянии $|0\rangle$

$$R_x(\theta)|0\rangle = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -i \cdot \sin\left(\frac{\theta}{2}\right) \\ -i \cdot \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ -i \cdot \sin\left(\frac{\theta}{2}\right) \end{pmatrix} = \cos\left(\frac{\theta}{2}\right)|0\rangle - i \cdot \sin\left(\frac{\theta}{2}\right)|1\rangle.$$

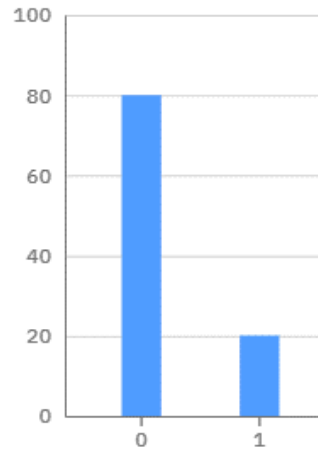
Таким образом для получения необходимого состояния нужно рассчитать правильный угол поворота θ . Для этого решим уравнение:

$$\cos\left(\frac{\theta}{2}\right)^2 = 0.8 \Rightarrow \theta \approx 0.93 \text{ рад.}$$

На рис. 2.7 представлена квантовая схема, реализующая подобное состояние суперпозиции и результат измерений состояния кубита с использованием системы *IBM Quantum Experience*.



а



б

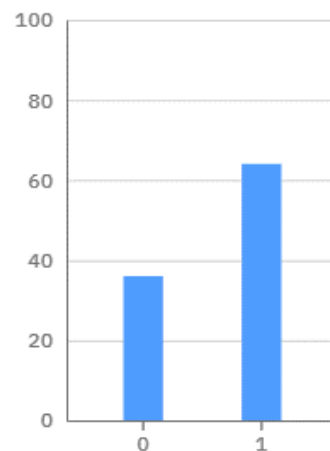
Рис. 2.7. Квантовая схема получения кубита в состоянии суперпозиции $|\psi\rangle = \sqrt{0.8}|0\rangle + \sqrt{0.2}|1\rangle$ (а) и результат симуляции (б)

Пример 2.8: Получим кубит в состоянии суперпозиции $|\psi\rangle = 0.6|0\rangle + 0.8|1\rangle$, применив воздействие гейта **Rx** к кубиту, который находится в исходном состоянии $|0\rangle$. Состояние $|\psi\rangle = 0.6|0\rangle + 0.8|1\rangle$ соответствует тому, что данный кубит будет принимать значение $|0\rangle$ с вероятностью 36% и значение $|1\rangle$ с вероятностью 64%.

Решим уравнение:

$$\cos\left(\frac{\theta}{2}\right)^2 = 0.36 \Rightarrow \theta \approx 1.85 \text{ рад.}$$

На рис. 2.8 представлена квантовая схема, реализующая подобное состояние суперпозиции и результат измерений состояния **кубита** с использованием системы *IBM Quantum Experience*.



а

б

Рис. 2.8. Квантовая схема получения кубита в состоянии суперпозиции $|\psi\rangle = 0.6|0\rangle + 0.8|1\rangle$ (а) и результат симуляции (б)

2.9. Контролируемые гейты

Для квантовых вычислений как правило требуется больше одного **кубита**:

$$|q_1\rangle \dots |q_n\rangle = (\alpha_0|0\rangle + \beta_0|1\rangle) \otimes (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes \dots \otimes (\alpha_{n-1}|0\rangle + \beta_{n-1}|1\rangle).$$

Например, система двух кубитов описывается как:

$$\begin{aligned} |\psi\rangle &= |\psi_0\rangle \otimes |\psi_1\rangle = (\alpha_0|0\rangle + \beta_0|1\rangle) \otimes (\alpha_1|0\rangle + \beta_1|1\rangle) = \\ &= \alpha_0\alpha_1|00\rangle + \alpha_0\beta_1|01\rangle + \beta_0\alpha_1|10\rangle + \beta_0\beta_1|11\rangle, \\ |\psi\rangle &= \alpha|00\rangle + \beta|01\rangle + \lambda|10\rangle + \delta|11\rangle. \end{aligned}$$

Простейшим двухкубитным контролируемым гейтом является **гейт CNOT**. Данный гейт имеет два кубита на входе и два кубита на выходе. При этом один из кубитов называется контролирующим, а второй – контролируемым. Процесс выполнения **гейта CNOT** является следующим: если контролирующий кубит находится в состоянии $|1\rangle$, тогда контролируемый кубит подвергается квантовой операции **NOT**, если контролирующий кубит находится в состоянии $|0\rangle$, тогда контролируемый кубит остается без изменения. Графическое обозначение квантового **гейта CNOT** представлено на рис. 2.9.

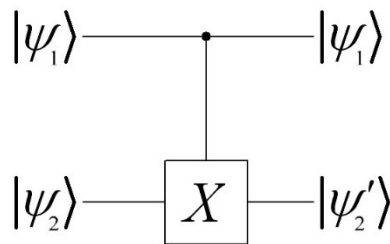


Рис. 2.9. Графическое обозначение квантового **гейта CNOT**

Для пары кубитов $|\psi_1\rangle$ и $|\psi_2\rangle$ в качестве базисных можно выбрать вектора, являющиеся произведением базисных векторов отдельных кубитов [1,2]:

$$\begin{aligned}
|00\rangle &= |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} & |01\rangle &= |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \\
|10\rangle &= |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} & |11\rangle &= |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.
\end{aligned}$$

В общем случае можно записать:

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \lambda|10\rangle + \delta|11\rangle = \begin{pmatrix} \alpha \\ \beta \\ \lambda \\ \delta \end{pmatrix}.$$

Исходя из этого можно определить матрицу **гейта CNOT**:

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

В данном случае для состояния $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \lambda|10\rangle + \delta|11\rangle$ первый (слева) кубит будет контролирующим, а второй кубит контролируемым. При этом действия **гейта CNOT** будет следующим:

$$CNOT|00\rangle \Rightarrow |00\rangle,$$

$$CNOT|01\rangle \Rightarrow |01\rangle,$$

$$CNOT|10\rangle \Rightarrow |11\rangle,$$

$$CNOT|11\rangle \Rightarrow |10\rangle.$$

Аналогичным образом может быть определен произвольный контролируемый унитарный оператор (таблица 2).

Таблица 2.2. Контролируемые квантовые гейты

Название	Графическое обозначение	Матрица
----------	-------------------------	---------

<p>CXgate CNOT</p>		$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
<p>CYgate</p>		$CY = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{pmatrix}$
<p>CZgate</p>		$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$
<p>CRxgate</p>		$CRx = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos\left(\frac{\theta}{2}\right) & -i \cdot \sin\left(\frac{\theta}{2}\right) \\ 0 & 0 & -i \cdot \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$

CRygate		$CRy = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ 0 & 0 & \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$
CRzgate		$CRz = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{-i\frac{\lambda}{2}} & 0 \\ 0 & 0 & 0 & e^{i\frac{\lambda}{2}} \end{pmatrix}$
CU1gate		$CU1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\lambda} \end{pmatrix}$
CU3gate		$CU3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos\left(\frac{\theta}{2}\right) & -e^{i\lambda} \sin\left(\frac{\theta}{2}\right) \\ 0 & 0 & e^{i\varphi} \sin\left(\frac{\theta}{2}\right) & e^{i(\varphi+\lambda)} \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$

2.10. Упражнения к Главе 2

1. Покажите воздействие *гейта Адамара* на кубит в состоянии $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.
2. Докажите, что $HYH = -Y$.
3. Покажите, что гейты R_x , R_y и R_z унитарны.
4. Выполните доказательство следующих соотношений:
 - a) $U1(\pi) = Z$;
 - б) $U1\left(\frac{\pi}{2}\right) = S$;

$$в) U1\left(\frac{\pi}{4}\right) = T;$$

$$з) U2(\varphi, \lambda) = R_z\left(\varphi + \frac{\pi}{2}\right) R_x\left(\frac{\pi}{2}\right) R_z\left(\lambda - \frac{\pi}{2}\right);$$

$$д) U2(0, \pi) = H; .$$

$$е) U3(\theta, \varphi, \lambda) = R_z\left(\varphi - \frac{\pi}{2}\right) R_x\left(\frac{\pi}{2}\right) R_z(\pi - \theta) R_x\left(\frac{\pi}{2}\right) R_z\left(\lambda - \frac{\pi}{2}\right);$$

$$жс) U3\left(\theta, -\frac{\pi}{2}, \frac{\pi}{2}\right) = R_x(\theta);$$

$$з) U3(\theta, 0, 0) = R_y(\theta).$$

5. Запишите состояние кубита на выходе следующих схем:

$$\alpha|0\rangle + \beta|1\rangle \text{---} [H] \text{---} [X] \text{---} |y\rangle$$

a

$$\alpha|0\rangle + \beta|1\rangle \text{---} [H] \text{---} [T] \text{---} |y\rangle$$

б

$$|0\rangle \text{---} [X] \text{---} [H] \text{---} |y\rangle$$

в

$$|1\rangle \text{---} [X] \text{---} [H] \text{---} |y\rangle$$

г

$$\alpha|0\rangle + \beta|1\rangle \text{---} [X] \text{---} [H] \text{---} |y\rangle$$

д

$$|1\rangle \text{---} [H] \text{---} [Z] \text{---} |y\rangle$$

е

6. Покажите, что гейты *CXgate*, *CYgate* и *CZgate* унитарны.

ГЛАВА 3. КВАНТОВЫЕ АЛГОРИТМЫ

Квантовый параллелизм – это фундаментальное свойство квантовых вычислений. Данное свойство позволяет квантовым компьютерам вычислять функцию $f(x)$ для различных значений x одновременно. Как отмечалось ранее, в классических компьютер состояние бита представляется либо 0, либо 1. В квантовом же компьютере состояние кубита можно представить не только как 0 или 1, а как комбинацию двух этих значений. Поэтому применение какой-либо операции кубиту происходит сразу со всеми его значениями одновременно. В качестве примера рассмотрим действие *гейта* X . Допустим изначально кубит находился в состоянии $|\psi\rangle = 0.8|1\rangle + 0.6|0\rangle$, после действия гейта инверсии кубит будет находиться в состоянии $|\psi\rangle = 0.6|1\rangle + 0.8|0\rangle$. Таким образом, одна операция повлияла сразу на оба значения кубита. Это и есть квантовый параллелизм. Однако, для получения информации, которая хранится в суперпозиционном состоянии, нужно выполнить операцию измерения состояний кубитов. При этом измерение кубита всегда дает только один вариант из всего множества возможных вариантов.

Квантовый параллелизм лежит в основе всех квантовых алгоритмов. Благодаря возможности воздействовать сразу на все состояния кубитов системы эффективность квантовых алгоритмов значительно выше, чем у классических компьютерных алгоритмов.

3.1. Перепутанные состояния двух кубитов. Базис Белла

Рассмотрим два незапутанных кубита. Незапутанность двух кубитов подразумевает, что измерение первого кубита не влияет на результат измерения второго кубита. Зададим их состояния:

$$\begin{aligned} |\Psi_1\rangle &= \alpha_0|0\rangle + \alpha_1|1\rangle, \\ |\Psi_2\rangle &= \beta_0|0\rangle + \beta_1|1\rangle. \end{aligned}$$

Состояние пары кубитов получается перемножением одиночных состояний:

$$\begin{aligned} |\Psi\rangle &= |\Psi_1\Psi_2\rangle = |\Psi_1\rangle|\Psi_2\rangle = (\alpha_0|0\rangle + \alpha_1|1\rangle)(\beta_0|0\rangle + \beta_1|1\rangle), \\ |\Psi\rangle &= |\Psi_1\Psi_2\rangle = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle, \\ |\Psi\rangle &= |\Psi_1\Psi_2\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle. \end{aligned}$$

В данном случае, как отмечалось в Главе 1, вероятность событий $|00\rangle$, $|01\rangle$, $|10\rangle$ и $|11\rangle$ равна произведению вероятностей его составляющих – $\alpha_0\beta_0$, $\alpha_0\beta_1$, $\alpha_1\beta_0$ и $\alpha_1\beta_1$, соответственно.

Перепутанное состояние двух кубитов – это состояние, при котором измерение одного из кубитов однозначно определяет состояние второго кубита. Например, если в результате измерения одного кубита получилось, состояние $|0\rangle$, то измерение другого кубита однозначно даст значение $|0\rangle$, а если в результате измерения одного кубита получилось, состояние $|1\rangle$, то измерение другого кубита также даст значение $|1\rangle$. В данном примере амплитуды вероятности групп $|01\rangle$ и $|10\rangle$ равны нулю. Такое состояние системы двух кубитов можно записать следующим образом [1,2]:

$$|\Psi\rangle = |\Psi_1\Psi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

$$|\Psi\rangle = |\Psi_1\Psi_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$

$$|\Psi\rangle = |\Psi_1\Psi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$

$$|\Psi\rangle = |\Psi_1\Psi_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

Для понимания специфики подобных состояний можно подробно рассмотреть процессы измерения, например, для состояний:

$$|\Psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle,$$

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle).$$

Сначала рассмотрим процесс измерения двухкубитного состояния $|\Psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$. Допустим, что сначала мы проводим измерение первого кубита. В ходе проведения измерения первого кубита мы получим состояние $|0\rangle$ в том случае если мы попадем в группы $|00\rangle$ и $|01\rangle$. Вероятность такого события будет составлять $|\alpha_{00}|^2 + |\alpha_{01}|^2$. При этом первый кубит перешел в состояние $|0\rangle$, а состояния $|10\rangle$ и $|11\rangle$ становятся нереализуемы.

После получения этого результата двухкубитное состояние выглядит так:

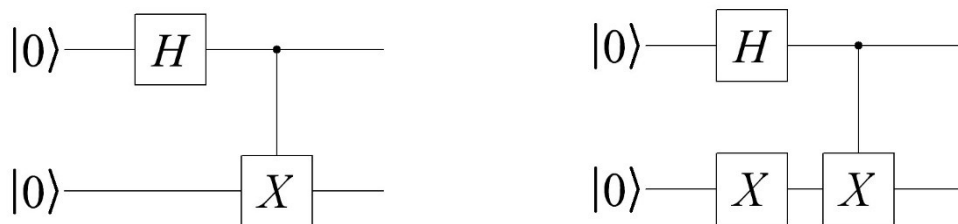
$$|\Psi\rangle = \frac{\alpha_{00}}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}|00\rangle + \frac{\alpha_{01}}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}|01\rangle,$$

$$|\Psi_1\rangle = |0\rangle; |\Psi_2\rangle = \frac{\alpha_{00}}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}|0\rangle + \frac{\alpha_{01}}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}|1\rangle.$$

Теперь рассмотрим процесс измерения двухкубитного состояния $|\Psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. В данном случае при измерении реализуемы только два состояния: $|01\rangle$ и $|10\rangle$. Если мы проведем измерение первого кубита, то реализуемой остается только одна группа: $|01\rangle$ или $|10\rangle$. Отсюда следует, что состояние второго кубита тоже определится, хотя его мы пока не провели его измерение. Например, если при измерении первого кубита мы получим состояние $|\Psi_1\rangle = |0\rangle$ тогда реализуемой остаётся только группа $|01\rangle$, то есть второй кубит переходит в определенное состояние — $|\Psi_2\rangle = |1\rangle$. Если же при измерении первого кубита мы получим состояние $|\Psi_1\rangle = |1\rangle$ тогда реализуемой остаётся только группа $|10\rangle$, то есть второй кубит переходит в определенное состояние — $|\Psi_2\rangle = |0\rangle$. Также можно описать процессы измерения других перепутанных состояний.

Аналогично обстоит дело и с более сложными системами: трёхкубитными, четырёхкубитными и так далее. Измерение одного кубита всегда выводит его из запутанности с остальными кубитами и приводит в одно из двух чистых базисных состояний. Квантовое состояние оставшейся части системы кубитов скачкообразно изменяется строго определённым образом. Если же измеряемый кубит не запутан с прочими кубитами системы, то при его измерении с остальными кубитами ничего не происходит.

На рис. 3.1 представлены способы реализации состояний Белла системы двух кубитов.



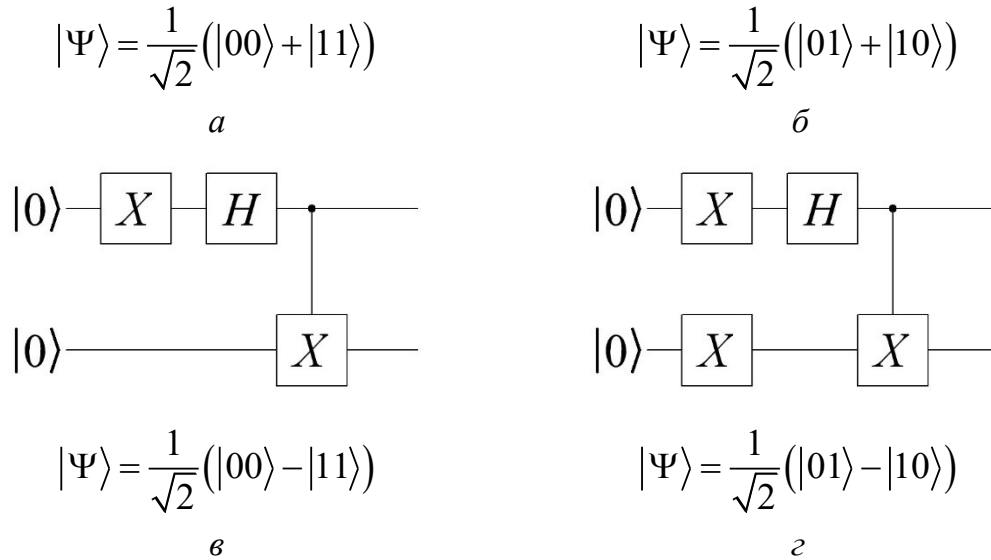


Рис. 3.1. Примеры реализации состояний Белла

3.2. Сверхплотное кодирование

Приведем пример применения перепутанности квантовых состояний. Допустим Алиса хочет передать бобу одну из цифр от 0 до 3. Для организации передачи информации между Бобом и Алисой каждому из них пересылается один из двух кубитов приготовленных в запутанном состоянии, например, $|\psi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Пусть Алиса получает первый кубит, а Боб второй. При этом Алиса может осуществлять преобразование на своем кубите, а Боб на своем [2].

Алгоритм обмена информации будет следующим:

1. Алиса получает извне два классических бита, которые кодируют цифры от 0 до 3. В зависимости от значения числа Алиса совершает одно из преобразований **I**, **X**, **Y** или **Z**:

Для цифры 0:

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix};$$

$$\begin{aligned}
0 \Rightarrow (I \otimes I)|\psi_0\rangle &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix} = \\
&= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}.
\end{aligned}$$

Таким образом, получаем: $0 \Rightarrow (I \otimes I)|\psi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Для цифры 1:

$$\begin{aligned}
1 \Rightarrow (X \otimes I)|\psi_0\rangle &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix} = \\
&= \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 0 \end{pmatrix}.
\end{aligned}$$

Таким образом, получаем: $1 \Rightarrow (X \otimes I)|\psi_0\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$.

Аналогично можно получить преобразования для цифр 2 и 3:

$$2 \Rightarrow (Y \otimes I)|\psi_0\rangle = \frac{1}{\sqrt{2}}(-|10\rangle + |01\rangle);$$

$$3 \Rightarrow (Z \otimes I)|\psi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle).$$

2. Далее Алиса передает свой кубит Бобу.
3. Боб применяет *гейт CNOT* к двум запутанным кубитам:

$$0 \Rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \Rightarrow CNOT \Rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle);$$

$$1 \Rightarrow \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \Rightarrow CNOT \Rightarrow \frac{1}{\sqrt{2}}(|11\rangle + |01\rangle);$$

$$2 \Rightarrow \frac{1}{\sqrt{2}}(-|10\rangle + |01\rangle) \Rightarrow CNOT \Rightarrow \frac{1}{\sqrt{2}}(-|11\rangle + |01\rangle);$$

$$3 \Rightarrow \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \Rightarrow CNOT \Rightarrow \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle).$$

4. Далее Боб производит измерение второго кубита. В результате измерений он получит состояние $|0\rangle$ для цифр 0 и 3, состояние $|1\rangle$ для цифр 1 и 2:

$$0 \Rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \Rightarrow \begin{cases} \text{Первый кубит } \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle); \\ \text{Второй кубит } |0\rangle \end{cases};$$

$$1 \Rightarrow \frac{1}{\sqrt{2}}(|11\rangle + |01\rangle) \Rightarrow \begin{cases} \text{Первый кубит } \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle); \\ \text{Второй кубит } |1\rangle \end{cases};$$

$$2 \Rightarrow \frac{1}{\sqrt{2}}(-|11\rangle + |01\rangle) \Rightarrow \begin{cases} \text{Первый кубит } \frac{1}{\sqrt{2}}(-|1\rangle + |0\rangle); \\ \text{Второй кубит } |1\rangle \end{cases};$$

$$3 \Rightarrow \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) \Rightarrow \begin{cases} \text{Первый кубит } \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle); \\ \text{Второй кубит } |0\rangle \end{cases}.$$

Результат измерения второго кубита:

$$|0\rangle \Rightarrow \begin{cases} \text{Либо } 0 \\ \text{Либо } 3 \end{cases} \quad |1\rangle \Rightarrow \begin{cases} \text{Либо } 1 \\ \text{Либо } 2 \end{cases}$$

5. Далее Боб применяет **преобразование Адамара** к первому кубиту и измеряет его:

$$0 \Rightarrow \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) = |0\rangle;$$

$$1 \Rightarrow \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) = |0\rangle;$$

$$2 \Rightarrow \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) = |1\rangle;$$

$$3 \Rightarrow \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle)\right) = |1\rangle.$$

6. Таким образом, выполнив преобразования и измерив два кубита, Боб понимает какую цифру передавала Алиса:

$$\left. \begin{array}{l} \text{Первый кубит} \rightarrow |0\rangle \\ \text{Второй кубит} \rightarrow |0\rangle \end{array} \right\} \rightarrow \text{цифра } 0;$$

$$\left. \begin{array}{l} \text{Первый кубит} \rightarrow |0\rangle \\ \text{Второй кубит} \rightarrow |1\rangle \end{array} \right\} \rightarrow \text{цифра } 1;$$

$$\left. \begin{array}{l} \text{Первый кубит} \rightarrow |1\rangle \\ \text{Второй кубит} \rightarrow |1\rangle \end{array} \right\} \rightarrow \text{цифра } 2;$$

$$\left. \begin{array}{l} \text{Первый кубит} \rightarrow |1\rangle \\ \text{Второй кубит} \rightarrow |0\rangle \end{array} \right\} \rightarrow \text{цифра } 3.$$

Исходя из представленного выше описания свехплотного кодирования можно построить квантовую схему (рис. 3.2).

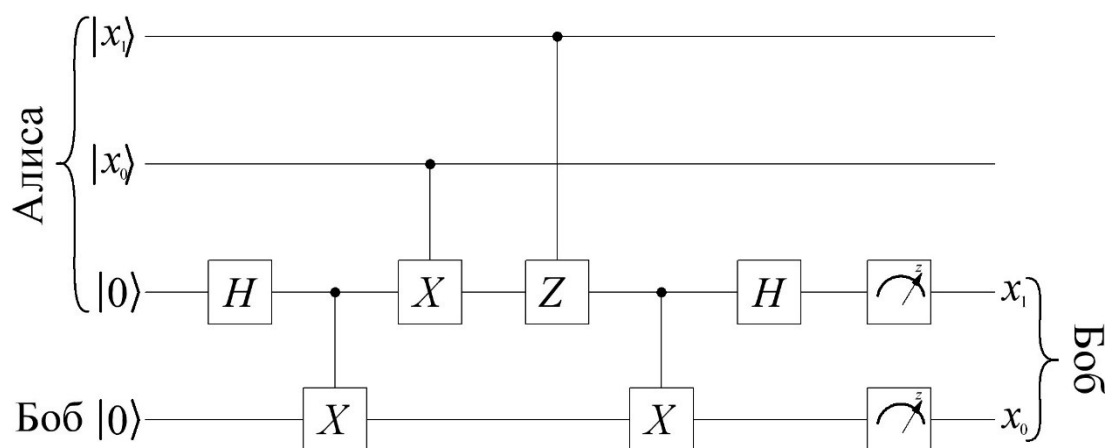


Рис. 3.2. Квантовая схема свехплотного кодирования

На схеме, представленной на рис. 3.2, передаваемая цифра кодируется в двоичном коде x_1x_0 . При этом один из запутанных **кубитов** принадлежит Алисе и в зависимости от передаваемой цифры Алиса применяет к нему соответствующее преобразование. После преобразования своего кубита Боб применяет операцию распутывания кубитов посредством операции контролируемого **NOT** и гейта Адамара **H**. После этого производится операция измерения двух кубитов.

3.3. Квантовая телепортация

Задача квантовой телепортации заключается в переносе неизвестного квантового состояния с одной системы на другую с

использованием квантового канала связи. Так как квантовое состояние не может быть скопировано (теорема о неклонированности), то в процессе передачи исходное состояние кубита будет утеряно. При осуществлении квантовой телепортации исходное состояние кубита будет утеряно, но при этом оно будет воссоздано у получателя [1,2,6].

Рассмотрим пример квантовой телепортации. Допустим Алиса хочет передать Бобу кубит в состоянии суперпозиции $|\Psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$. Кубит в данном состоянии находится у Алисы.

Для организации передачи информации между Бобом и Алисой каждому из них пересылается один из двух кубитов приготовленных в запутанном состоянии, например, $|\Psi_{23}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. На рис. 3.3 показано распределение кубитов между Бобом и Алисой.

$$|\Psi_1\rangle = \alpha|0\rangle + \beta|1\rangle \longrightarrow \text{Первый бит} - \text{Алиса}$$

Второй бит - Алиса

$$|\Psi_{23}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Третий бит - Боб

Рис. 3.3 Кубиты Алисы и Боба для квантовой телепортации

Таким образом можно говорить, что мы имеем трехкубитовую систему:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle).$$

Далее Алиса применяет операцию контролируемой инверсии, причем передаваемый кубит $|\Psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$ будет являться контролирующим. Тогда трехбитовая система будет иметь вид:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle).$$

После операции **CNOT** Алиса выполняет преобразование Адамара с передаваемым кубитом. Для дальнейшего описания системы вспомним, что $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ и $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Следовательно, состояние системы после преобразования Адамара можно представить в виде:

$$\alpha|000\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|100\rangle),$$

$$\alpha|011\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(\alpha|011\rangle + \alpha|111\rangle),$$

$$\beta|110\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(\beta|010\rangle - \beta|110\rangle),$$

$$\beta|101\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(\beta|001\rangle - \beta|101\rangle),$$

$$|\Psi\rangle = \frac{1}{2}(\alpha|000\rangle + \alpha|100\rangle + \alpha|011\rangle + \alpha|111\rangle + \beta|010\rangle - \beta|110\rangle + \beta|001\rangle - \beta|101\rangle).$$

Напомним, что в данной системе два кубита принадлежат Алисе и один кубит – Бобу. Если выделить в волновой функции системы кубиты Алисы, то ее можно записать следующим образом:

$$|\Psi\rangle = \frac{1}{2}(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)).$$

Из представленной выше функции можно заметить, что кубит, который принадлежит Бобу, может быть преобразован в исходный (передаваемый) кубит. Причем необходимое преобразование зависит от значений двух кубитов Алисы. Распишем необходимые преобразования для получения Бобом исходного кубита:

1. Если кубиты Алисы при измерении принимают значения $|00\rangle$, то в данном случае Бобу не нужно выполнять никаких преобразований и его кубит будет иметь волновую функцию $\alpha|0\rangle + \beta|1\rangle$.

2. Если кубиты Алисы при измерении принимают значения $|01\rangle$, то в данном случае кубит, который принадлежит Бобу находится в состоянии $\alpha|1\rangle + \beta|0\rangle$. Можно заметить, что для получения исходного кубита Бобу необходимо выполнить операцию инверсии:

$$\alpha|1\rangle + \beta|0\rangle \xrightarrow{X} \alpha|0\rangle + \beta|1\rangle.$$

3. Если кубиты Алисы при измерении принимают значения $|10\rangle$, то в данном случае кубит, который принадлежит Бобу находится в состоянии $\alpha|0\rangle - \beta|1\rangle$. Можно заметить, что для получения исходного кубита Бобу необходимо применить гейт Z :

$$\alpha|0\rangle - \beta|1\rangle \xrightarrow{Z} \alpha|0\rangle + \beta|1\rangle.$$

4. Если кубиты Алисы при измерении принимают значения $|11\rangle$, то в данном случае кубит, который принадлежит Бобу находится в состоянии $\alpha|1\rangle - \beta|0\rangle$. Можно заметить, что для получения исходного кубита Бобу необходимо применить гейты Z и X :

$$\alpha|1\rangle - \beta|0\rangle \xrightarrow{X} \alpha|0\rangle - \beta|1\rangle,$$

$$\alpha|0\rangle - \beta|1\rangle \xrightarrow{Z} \alpha|0\rangle + \beta|1\rangle.$$

Исходя из алгоритма телепортации можно построить квантовые схемы ее реализующие (рис. 3.4).

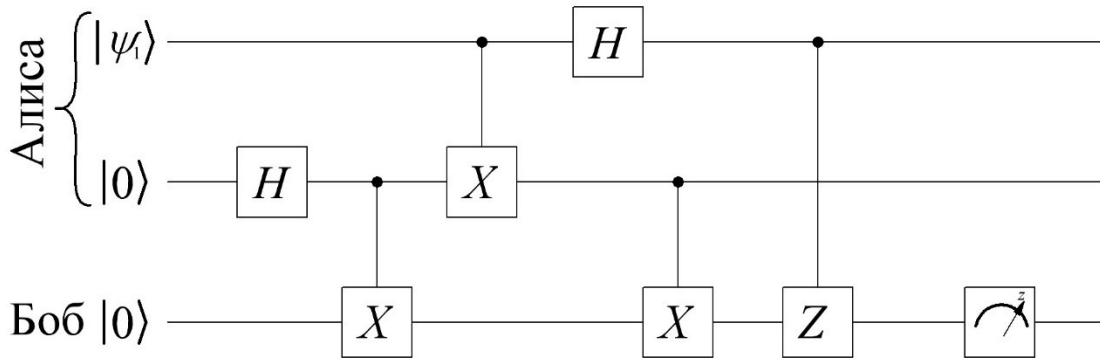


Рис. 3.4. Схема алгоритма квантовой телепортации

В представленной на рис. 3.4 схеме передаваемым кубитом является $|\Psi_1\rangle$. При разработке схемы телепортации данный кубит должен находиться в состоянии суперпозиции. Получить подобное состояние можно с использованием гейтов поворота U или R .

3.4. Алгоритм Дойча. Задача Дойча-Джозы

Принцип работы квантового компьютера и преимущества квантовых вычислений наиболее просто показать на примере простейшего квантового алгоритма – алгоритма Дойча [1,2,6]. Опишем задачу, которую решает данный алгоритм. Предположим, что у нас имеется «черный ящик», который вычисляет неизвестную нам функцию одной переменной – $f(x)$. Так как это функция одной переменной, то на вход можно подать 0 или 1 и на выходе также можно получить или 0, или 1. Функции одной переменной можно разделить на две группы: константный и сбалансированные. На выходе первых мы всегда будем получать постоянное значение 0 или 1 не зависимо от того, что подано на вход. Константных функций одной переменной являются функции вида: $f(x) = 0$ и $f(x) = 1$. Сбалансированными функциями одной переменной являются функции тождественного равенства и инверсии: $f(x) = x$ и $f(x) = \bar{x}$.

Задача Дойча состоит в том, чтобы определить к какой из двух групп (константная или сбалансированная) относится функция, реализуемая

«черным ящиком». Решение подобной задачи с использованием классического компьютера сводится к тому, что необходимо на вход схемы подать сначала 0, а потом 1. Т.е. на классическом компьютере нам необходимо будет два раза вызвать функцию и измерить выходную реакцию. После двух данных операций мы однозначно можем идентифицировать не только к какой группе относится функция, но и вид данной функции. Если же мы на классическом компьютере вызовем функцию один раз, то не сможем определить даже группу, к которой она относится. Однако использование квантового компьютера позволит определить группу за один вызов функции.

В квантовой системе в качестве функции в «черном ящике» должен быть реализован унитарный оператор U_f . Данный оператор называется квантовым оракулом. Квантовый оракул – это многокубитный гейт, который соответствует бинарной функции, содержит в себе информацию о функции $f(x)$ и позволяет одновременно вызвать её на всех возможных аргументах. Квантовый оракул определяется как преобразование $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$, где, в общем случае, множество кубитов $|x\rangle$ несут в себе информацию об аргументах функции (остаются неизменными), а кубит $|y\rangle$ – результат. При этом размерность квантового оракула будет составлять $n+1$ при размерности функции $f(x) - n$.

Определив квантовый оракул как преобразование $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$ можно показать его воздействие на состояние $\frac{1}{\sqrt{2}}|x\rangle(|0\rangle - |1\rangle)$:

$$U_f \frac{1}{\sqrt{2}}|x\rangle(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}|x\rangle(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle) = \frac{1}{\sqrt{2}}(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle).$$

Давайте получим матрицы и схемы оракулов для всех бинарных функций одной переменной: $f(x) = 0$, $f(x) = 1$, $f(x) = x$ и $f(x) = \bar{x}$.

1. Функция $f(x) = 0$. В соответствии с воздействием $|x\rangle|y \oplus f(x)\rangle$ рассмотрим в какие состояния должны перейти все возможные базисные состояния регистра:

$$|00\rangle = |0\rangle|0\rangle \xrightarrow{U_f} |0\rangle|0 \oplus f(0)\rangle = |0\rangle|0 \oplus 0\rangle = |00\rangle,$$

$$|01\rangle = |0\rangle|1\rangle \xrightarrow{U_f} |0\rangle|1 \oplus f(0)\rangle = |0\rangle|1 \oplus 0\rangle = |01\rangle,$$

$$|10\rangle = |1\rangle|0\rangle \xrightarrow{U_f} |1\rangle|0 \oplus f(1)\rangle = |1\rangle|0 \oplus 0\rangle = |10\rangle,$$

$$|11\rangle = |1\rangle|1\rangle \xrightarrow{U_f} |1\rangle|1 \oplus f(0)\rangle = |1\rangle|1 \oplus 0\rangle = |11\rangle.$$

Таким образом матрицу оракула U_f можно представить в виде:

$$U_f = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Исходя из полученной матрицы оракула можно представить его квантовую схему (рис. 3.5).

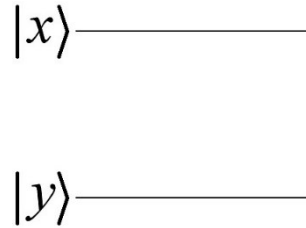


Рис. 3.5. Квантовая схема оракула функции $f(x) = 0$

2. Функция $f(x) = 1$. Рассмотрим в какие состояния должны перейти все возможные базисные состояния регистра:

$$|00\rangle = |0\rangle|0\rangle \xrightarrow{U_f} |0\rangle|0 \oplus f(0)\rangle = |0\rangle|0 \oplus 1\rangle = |01\rangle,$$

$$|01\rangle = |0\rangle|1\rangle \xrightarrow{U_f} |0\rangle|1 \oplus f(0)\rangle = |0\rangle|1 \oplus 1\rangle = |00\rangle,$$

$$|10\rangle = |1\rangle|0\rangle \xrightarrow{U_f} |1\rangle|0 \oplus f(1)\rangle = |1\rangle|0 \oplus 1\rangle = |11\rangle,$$

$$|11\rangle = |1\rangle|1\rangle \xrightarrow{U_f} |1\rangle|1 \oplus f(0)\rangle = |1\rangle|1 \oplus 1\rangle = |10\rangle.$$

Таким образом матрицу оракула U_f можно представить в виде:

$$U_f = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Как видно из полученной матрицы оракула можно заметить, что в данном случае схема будет представлять собой инверсию $|y\rangle$ (рис. 3.6).

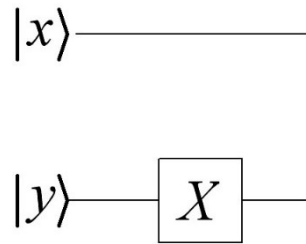


Рис. 3.6. Квантовая схема оракула функции $f(x)=1$

3. Функция $f(x)=x$. Рассмотрим в какие состояния должны перейти все возможные базисные состояния регистра:

$$|00\rangle = |0\rangle|0\rangle \xrightarrow{U_f} |0\rangle|0 \oplus f(0)\rangle = |0\rangle|0 \oplus 0\rangle = |00\rangle,$$

$$|01\rangle = |0\rangle|1\rangle \xrightarrow{U_f} |0\rangle|1 \oplus f(0)\rangle = |0\rangle|1 \oplus 0\rangle = |01\rangle,$$

$$|10\rangle = |1\rangle|0\rangle \xrightarrow{U_f} |1\rangle|0 \oplus f(1)\rangle = |1\rangle|0 \oplus 1\rangle = |11\rangle,$$

$$|11\rangle = |1\rangle|1\rangle \xrightarrow{U_f} |1\rangle|1 \oplus f(1)\rangle = |1\rangle|1 \oplus 1\rangle = |10\rangle.$$

Таким образом матрицу оракула U_f можно представить в виде:

$$U_f = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

В данном случае квантовый оракул представляет собой контролируемый гейт X , причем кубит $|x\rangle$ является контролирующим (рис. 3.7).

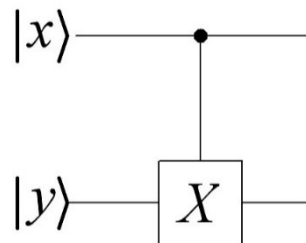


Рис. 3.7. Квантовая схема оракула функции $f(x)=x$

4. Функция $f(x)=\bar{x}$. Рассмотрим в какие состояния должны перейти все возможные базисные состояния регистра:

$$\begin{aligned}
|00\rangle &= |0\rangle|0\rangle \xrightarrow{U_f} |0\rangle|0 \oplus f(0)\rangle = |0\rangle|0 \oplus 1\rangle = |01\rangle, \\
|01\rangle &= |0\rangle|1\rangle \xrightarrow{U_f} |0\rangle|1 \oplus f(0)\rangle = |0\rangle|1 \oplus 1\rangle = |00\rangle, \\
|10\rangle &= |1\rangle|0\rangle \xrightarrow{U_f} |1\rangle|0 \oplus f(1)\rangle = |1\rangle|0 \oplus 0\rangle = |10\rangle, \\
|11\rangle &= |1\rangle|1\rangle \xrightarrow{U_f} |1\rangle|1 \oplus f(1)\rangle = |1\rangle|1 \oplus 0\rangle = |11\rangle.
\end{aligned}$$

Таким образом матрицу оракула U_f можно представить в виде:

$$U_f = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Подобный оператор можно реализовать различными схемами (рис. 3.8).

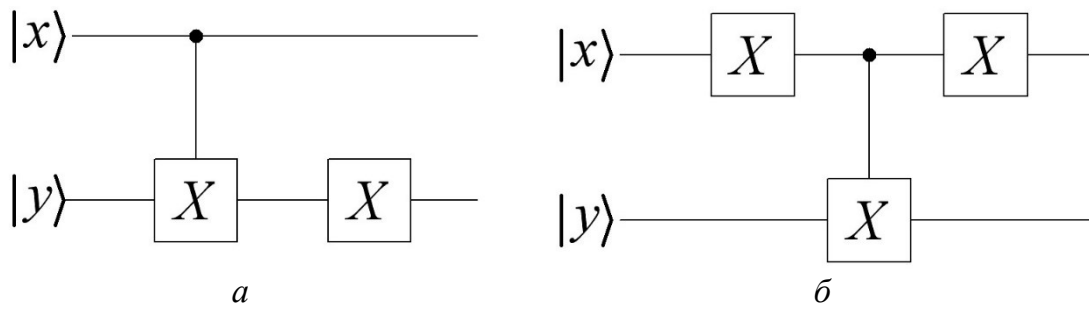


Рис. 3.8. Квантовая схема оракула функции $f(x) = \bar{x}$

Итак, описав оракулы мы можем вернуться к разработке алгоритма, реализующего задачу Дойча. Схема данного алгоритма представлена на рис. 3.9.

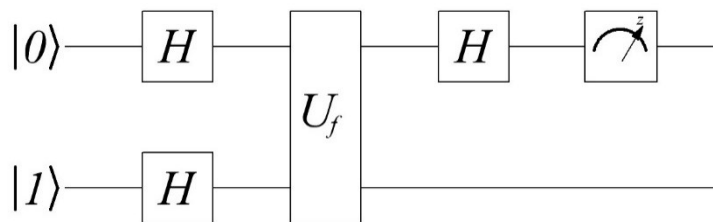


Рис. 3.9. Схема алгоритма Дойча

Приведем описание как данная схема работает. Применим преобразование Адамара к каждому кубиту двухкубитовой системы:

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

$$|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle);$$

$$|xy\rangle = |01\rangle \xrightarrow{H} \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = \frac{1}{2}|0\rangle(|0\rangle - |1\rangle) + \frac{1}{2}|1\rangle(|0\rangle - |1\rangle).$$

Далее на систему действует оператор U_f :

$$U_f \frac{1}{\sqrt{2}}|x\rangle(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle);$$

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

Далее по алгоритму применяется преобразование Адамара к первому кубиту, и после этого производится его измерение. Рассмотрим оба случая, т.е. когда функция является константной или сбалансированной.

• В случае если функция является константной, то $f(0) = f(1)$. В данном случае после воздействия оператора U_f первый кубит будет находиться либо в состоянии $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, либо в состоянии $-\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. При этом воздействие оператора Адамара приведет его в состояния $|0\rangle$ или $-|0\rangle$, соответственно. В любом случае измерение покажет, что кубит находится в нулевом состоянии.

• В случае если функция является сбалансированной, то $f(0) \neq f(1)$. После воздействия оператора U_f первый кубит будет находиться либо в состоянии $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, либо в состоянии $-\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Последующее воздействие оператора Адамара приведет его в состояния $|1\rangle$ или $-|1\rangle$, соответственно, и измерение покажет, что кубит находится в единичном состоянии.

Далее рассмотрим с вами решения задачи Дойча-Джозы, которая является обобщенной задачей Дойча. Данная задача формулируется следующим образом: пусть имеется бинарная функция $f: \{0,1\}^n \rightarrow \{0,1\}$, и известно, что данная функция может быть константной или сбалансированной. Функция с n входными переменными будет сбалансированной если она принимает значение 0 на 2^{n-1} входных наборах и значение 1 на 2^{n-1} входных наборах. Задача Дойча-Джозы, как и задача Дойча, заключается в том, что необходимо определить, является

ли функция в «черном ящике» сбалансированной или константной. По аналогии с предыдущей задачей, схема алгоритма Дойча-Джозы будет иметь вид, представленный на рис. 3.10.

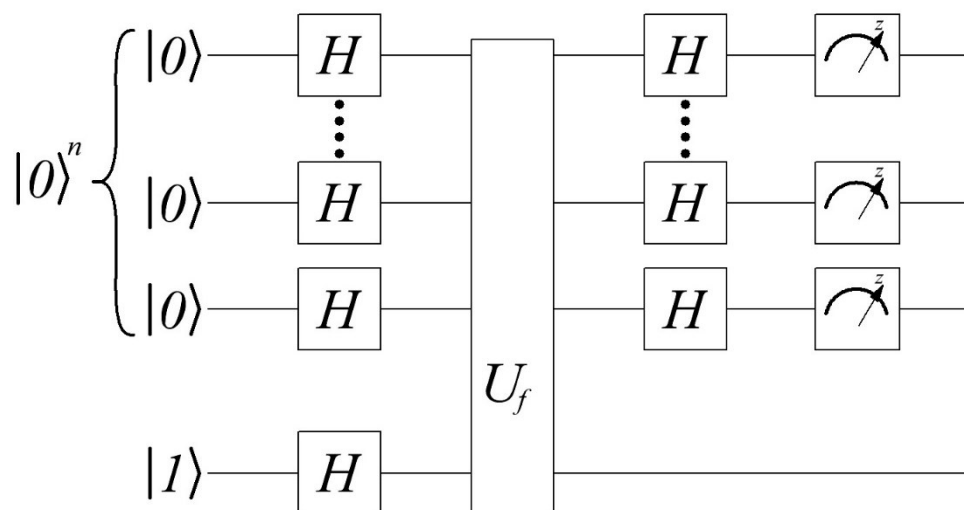


Рис. 3.10. Схема алгоритма Дойча-Джозы

Выполним описание данного алгоритма. Для этого рассмотрим действие оператора Адамара на произвольный квантовый регистр $|x\rangle^n$:

$$\begin{aligned} |x\rangle^n &\rightarrow |x_1 x_2 \dots x_n\rangle \xrightarrow{H_n} H|x_1\rangle \otimes H|x_2\rangle \otimes \dots \otimes H|x_n\rangle = \\ &= \frac{1}{\sqrt{2^n}} \left(\sum_{y_1 \in \{0,1\}} (-1)^{x_1 y_1} |y_1\rangle \otimes \sum_{y_2 \in \{0,1\}} (-1)^{x_2 y_2} |y_2\rangle \otimes \dots \otimes \sum_{y_n \in \{0,1\}} (-1)^{x_n y_n} |y_n\rangle \right) = \\ &= \frac{1}{\sqrt{2^n}} \sum_{y \in B_n} (-1)^{x_1 y_1 \otimes x_2 y_2 \otimes \dots \otimes x_n y_n} |y\rangle^n. \end{aligned}$$

В начальный момент времени система (рис. 3.10) находится в состоянии $|0\rangle^n |1\rangle$. Если применить операцию H_n к состоянию $|0\rangle^n$, то мы получим следующий результат $H_n |0\rangle^n = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$, следовательно, для состояния $|0\rangle^n |1\rangle$ получим:

$$|0\rangle^n |1\rangle \xrightarrow{H_{n+1}} = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle (|0\rangle - |1\rangle).$$

Воздействие оракула U_f переведет систему в состояние:

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle (|0\rangle - |1\rangle) \xrightarrow{U_f} \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle (|0\rangle - |1\rangle).$$

Если функция $f(x)$ является константной и, учитывая, что

$$H_n |0\rangle^n = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle, \text{ то первые } n \text{ кубитов находятся в состоянии}$$

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle = (-1)^{f(x)} H_n |0\rangle^n.$$

Повторное применение оператора Адамара к состоянию $H_n |0\rangle^n$ приведет к тому, что при измерении (рис. 3.10) с вероятностью 100% будет получено состояние $|0\rangle^n$.

Если же функция $f(x)$ является сбалансированной, то $(-1)^{f(x)}$ нельзя вынести из под суммы и состояние первых n кубитов можно представить как [1]

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle = \frac{1}{\sqrt{2^n}} \left(\sum_{x:f(x)=0} |x\rangle - \sum_{x:f(x)=1} |x\rangle \right).$$

Отметим, что

$$H_n |x\rangle^n = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x_1 y_1 \oplus x_2 y_2 \oplus \dots \oplus x_n y_n} |y\rangle = \frac{1}{\sqrt{2^n}} \left(|0\rangle^n + \sum_{y=1}^{2^n-1} (-1)^{x_1 y_1 \oplus x_2 y_2 \oplus \dots \oplus x_n y_n} |y\rangle \right).$$

Если функция $f(x)$ сбалансирована, то число слагаемых в суммах выражения $\frac{1}{\sqrt{2^n}} \left(\sum_{x:f(x)=0} |x\rangle - \sum_{x:f(x)=1} |x\rangle \right)$ одинаково, и при повторно применении оператора Адамара векторы $|0\rangle^n$ будут отсутствовать. Таким образом в случае сбалансированной функции при измерении системы (рис. 3.10) вероятность получения состояния $|0\rangle^n$ будет равно нулю.

3.5. Алгоритм Гровера

Алгоритм Гровера направлен на решение следующей задачи: в базе неупорядоченных данных, состоящей из n элементов, требуется найти элемент с заданными свойствами [1,2,6]. Для решения данной задачи на классическом компьютере в среднем потребуется перебрать $\frac{n}{2}$ элементов базы, а в наихудшем случае – $n-1$ элементов. Квантовый алгоритм Гровера позволит выполнить данную задачу всего за \sqrt{n} операций [2].

Задачу поиска можно сформулировать следующим образом: пусть имеется бинарная функция $f : \{0,1\}^n \rightarrow \{0,1\}$, и известно, что данная функция принимает значение 0 на всех входных наборах, кроме x_0 , и задача состоит в том, чтобы найти x_0 . Очевидно, что для реализации алгоритма поиска необходимо получить оракул данной функции:

$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle,$$

$|x\rangle$ – входной регистр,
 $|y\rangle$ – выходной регистр.

Вычисление функции $f(x)$ для всевозможных входных наборов $|x\rangle$ за счет применения оператора U_f , при начальном значении выходного регистра равному 0, приведет к суперпозиции $\frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$. Для входного набора x_0 , при котором $f(x_0) = 1$, состояние $|x_0\rangle |1\rangle$ будет иметь вероятность 2^{-n} . Суть алгоритма Гровера состоит в том, чтобы максимально повысить амплитуду состояния $|x_0\rangle |1\rangle$ и уменьшить амплитуды состояний $|x_0\rangle |0\rangle$. [2] Представим последовательность реализации алгоритма Гровера:

1. Подготавливаем входной регистр $|x\rangle^n$, который будет содержать суперпозицию всех возможных значений входных наборов.
2. Вычисляем функцию $f(x)$.
3. Изменяем знак коэффициентов для тех значений x при которых функция $f(x)$ равна 1.
4. Далее необходимо увеличить амплитуду коэффициентов тех значений x при которых функция $f(x)$ равна 1. Увеличение амплитуд возможно за счет применения операции, которая носит название «инверсия относительно среднего». После применения данной операции амплитуды входных значений, при которых функция равна 1 вырастут, а амплитуды входных значений, при которых функция равно 0 – уменьшатся.

5. Далее пункты 2-4 повторяются $\frac{\pi}{4} \sqrt{2^n}$ раз.

Изменение знака коэффициентов выполняется следующим образом. Возьмем значение выходного регистра равным 1 и применим преобразование Адамара:

$$|0\rangle^n |1\rangle \xrightarrow{H_{n+1}} = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle (|0\rangle - |1\rangle).$$

Затем к полученному состоянию суперпозиции применяется преобразование U_f и, как и в алгоритме Дойча, это приводит к следующему результату:

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle (|0\rangle - |1\rangle) \xrightarrow{U_f} \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle (|0\rangle - |1\rangle).$$

Отсюда можно заметить, что в полученном состоянии суперпозиции амплитуды значений, при которых функция равна 1, будут иметь отрицательное значение.

Инверсия относительно среднего – это унитарное преобразование, которое воздействует на систему следующим образом:

$$\sum_i \alpha_i |x_i\rangle \rightarrow \sum_{x=0}^{2^n-1} (2A - \alpha_i) |x_i\rangle,$$

где A – среднее значение амплитуды. По сути амплитуды, осуществляется путем переворачивания вероятностей относительно их среднего. Если число выше среднего, оно переворачивается и становится ниже среднего и наоборот.

Преобразование инверсии относительно среднего описывается матрицей:

$$D = \begin{pmatrix} \frac{2}{N} - 1 & \frac{2}{N} & \dots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} - 1 & \dots & \frac{2}{N} \\ \dots & \dots & \dots & \dots \\ \frac{2}{N} & \frac{2}{N} & \dots & \frac{2}{N} - 1 \end{pmatrix},$$

где $N = 2^n$.

Пример матрицы преобразования «инверсия относительно среднего» для $N = 4$, т.е. для $n = 2$, будет выглядеть следующим образом:

$$D = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \end{pmatrix} = \frac{1}{2} \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}.$$

Пример схемы, реализующей данное преобразование представлен на рис. 3.11 [1,2].

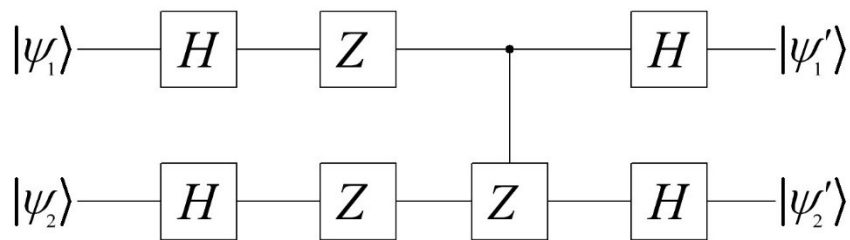


Рис. 3.11. Квантовая схема инверсии относительно среднего

Покажем, что данная схема реализует преобразование «инверсия относительно среднего»:

$$H \otimes H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix},$$

$$Z \otimes Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$(H \otimes H)(Z \otimes Z) = \frac{1}{2} \begin{pmatrix} 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 \end{pmatrix},$$

$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix},$$

$$(H \otimes H)(Z \otimes Z)CZ = \frac{1}{2} \begin{pmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix},$$

$$(H \otimes H)(Z \otimes Z)CZ(H \otimes H) = \frac{1}{4} \begin{pmatrix} -2 & 2 & 2 & 2 \\ 2 & -2 & 2 & 2 \\ 2 & 2 & -2 & 2 \\ 2 & 2 & 2 & -2 \end{pmatrix} = \frac{1}{4} \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}.$$

В общем виде пример схемы алгоритма Гровера можно представить, как показано на рис. 3.12 [1].

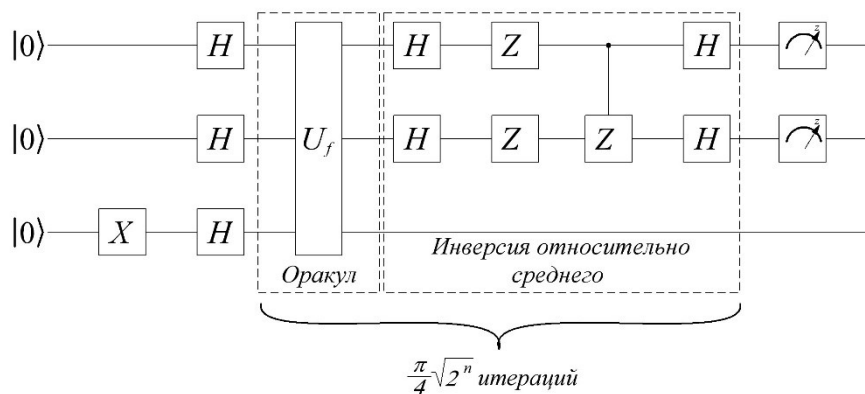


Рис 3.12 Схема алгоритма Гровера

3.6. Квантовое преобразование Фурье

Квантовое преобразование Фурье (КПФ) – это аналог дискретного преобразования Фурье (ДПФ), которое применяется к вектору амплитуд квантовых состояний. Квантовое преобразование Фурье широко применяется во многих квантовых алгоритмах, в частности, в алгоритме Шора.

Квантовое преобразование Фурье осуществляет преобразование квантового состояния следующим образом:

$$\sum_x f(x)|x\rangle = \sum_y F(y)|y\rangle.$$

При измерении состояния после преобразования Фурье с вероятностью $|F(y)|^2$ мы получим состояние $|y\rangle$. ДПФ осуществляет преобразование функции с периодом r в функцию, которая имеет нулевые значения на всех частотах не кратных $\frac{1}{r}$. Применив квантовое преобразование Фурье к функции $f(x)$ с периодом r мы получим функцию $F(y)$, которая будет равно нулю, кроме значений кратных $\frac{N}{r}$. Т.е. проведя измерение мы получим результат кратный $\frac{N}{r}$. [2]

Квантовое преобразование Фурье определяется следующим образом:

$$|x\rangle \xrightarrow{QFT} \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{\frac{2\pi i y x}{2^n}} |y\rangle.$$

В общем случае квантовая схема квантового преобразования Фурье представлена на рис. 3.13.

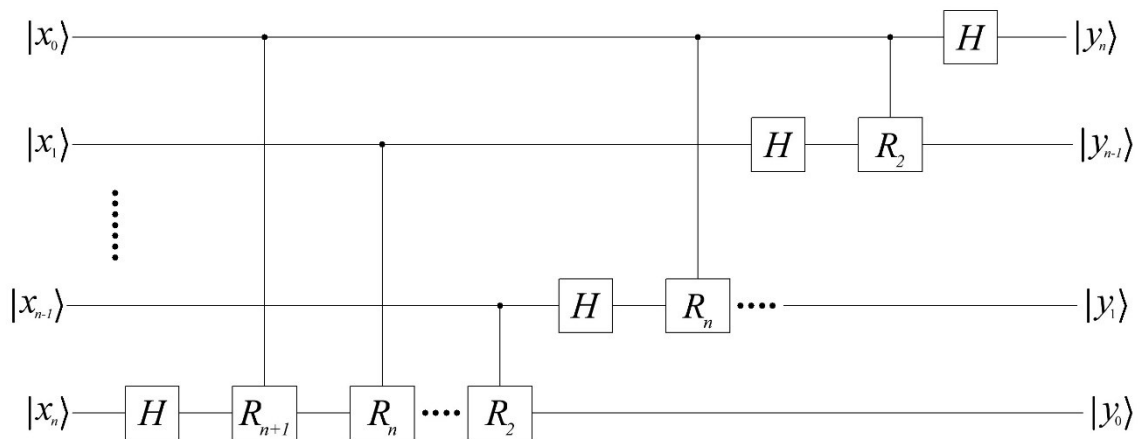


Рис. 3.13. Схема квантового преобразования Фурье

Следует отметить, что схема меняет порядок кубитов. В схеме, представленной на рис. 3.13 используются унитарные операторы поворота R_k , которые можно определить как:

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix}.$$

В общем случае выражение для n-ой линии можно выразить выражением [1]:

$$|x_n\rangle \xrightarrow{QFT} \frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i \left(\frac{x_n}{2} + \dots + \frac{x_1}{2^n} + \frac{x_0}{2^{n+1}} \right)} |1\rangle \right).$$

3.7. Алгоритм Шора

Алгоритм Шора является одним из наиболее распространенных алгоритмов и направлен на решение задачи факторизации. Факторизация – это разложение чисел на множители. Факторизация широко применяется в современной теории чисел и криптоанализа. Следует отметить, что эта задача весьма сложная, так как трудоемкость классических алгоритмов растет экспоненциально с увеличением размера факторизуемых чисел. Так, при факторизации числа N путем простого перебора необходимо будет перебрать все варианты от 2 до \sqrt{N} , а это весьма сложно если мы имеем дело с очень большими числами [1,2,6].

Пример использования факторизации – это алгоритмы шифрования с открытым ключом (*RSA*, *El Gamal* и т.д.). В данном случае ключ представляет собой пару больших чисел, а взлом шифра, который заключается в нахождении по открытому ключу приватного и наоборот, требует решения задачи факторизации.

Алгоритм Шора позволяет выполнить решение задачи факторизации за полиномиальное время. Это осуществляется за счет использования свойства квантового параллелизма и сведения задачи к поиску периода функции.

Допустим нам необходимо разложить на множители некоторое число N . Изначально выберем произвольное число $a < N$ и рассматриваем функцию $f_a(x) = a^x \bmod N$.

Функция $f_a(x)$ является периодической с периодом r . Период r является порядком числа a : $a^r = 1 \bmod N$ и $\forall r_1 < r \rightarrow a^{r_1} \neq 1 \bmod N$. Если число N простое, то период r будет равно $N-1$. Этот случай весьма простой и легко реализуется проверкой на простоту классическими методами. В общем случае $f_a(x+r) = f_a(x)$. Если период r известен, то разложение на множители числа N легко можно определить классическими методами. В частности, если период r является четным числом, то из соотношения $a^r - 1 = 0 \bmod N$ можно записать:

$$\left(a^{\frac{r}{2}} - 1 \right) \left(a^{\frac{r}{2}} + 1 \right) = 0 \bmod N.$$

Так как $\left(a^{\frac{r}{2}} - 1\right)\left(a^{\frac{r}{2}} + 1\right)$ делится на N , то оба сомножителя имеют общие с N делители. Эти делители можно определить классическим алгоритмом Евклида по поиску наибольшего общего делителя. Если же период r является нечетным или $\left(a^{\frac{r}{2}} - 1\right)\left(a^{\frac{r}{2}} + 1\right)$ вырождается в ноль, то следует выбрать другое число a . Для больших чисел N это случается редко.

Квантовый алгоритм Шора предназначен для быстрого поиска периода r . Для реализации алгоритма необходимо использовать квантовый компьютер с двумя квантовыми регистрами размера n . Причем размер должен быть таким, что $M = 2^n > N$, $M \approx N^2$. Алгоритм определения периода r будет следующим:

1. На первом этапе необходимо приготовить два входных регистра в состоянии $|0\rangle$.

2. Далее воздействием на каждый кубит входного регистра преобразованием Адамара:

$$|0\rangle^n |0\rangle^n \xrightarrow{H_n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |0\rangle^n.$$

3. Применим к обоим регистрам квантовую схему, реализующую функцию $f_a(x)$. Теперь регистры перейдут в состояние:

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |0\rangle^n \xrightarrow{f_a(x)} \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |f_a(x)\rangle.$$

Таким образом, в выходном регистре будет суперпозиция всех возможных значений функции $f_a(x)$.

4. Далее производится измерение выходного регистра. В результате измерений мы получим

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |f_a(x)\rangle \xrightarrow{\text{измерение}} \frac{1}{\sqrt{M}} \sum_{i=0}^{M-1} |k + jr\rangle |f_a(k)\rangle.$$

После измерения мы получим значение функции $f_a(k)$ при некотором случайном значении k , а выходной регистр перейдет в состояние $|f_a(k)\rangle$. Измеренное значение выходного регистра нас не интересует, но важно, что состояние входного регистра редуцируется до комбинации только тех состояний, которые совместимы с измеренным на выходе значением: $f_a(x) = f_a(k)$, $x = k$, $x = k + r$, $x = k + 2r$ и т.д.

5. Для извлечения периодичности в выходном регистре необходимо выполнить квантовое преобразование Фурье и измерение результата преобразования.

$$\frac{1}{\sqrt{M}} \sum_{i=0}^{M-1} |k + jr\rangle \xrightarrow{QFT} \frac{1}{\sqrt{MN}} \sum_{i=0}^{M-1} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{ky}{N}} e^{2\pi i \frac{jry}{N}} |y\rangle = \frac{1}{\sqrt{MN}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{ky}{N}} \sum_{y=0}^{M-1} e^{2\pi i \frac{jry}{N}} |y\rangle.$$

При преобразовании Фурье период r будет преобразован в $\frac{M}{r}$ и измерение приведет к тому, что с высокой долей вероятности мы получим $\frac{jM}{r}$ для $j=1,2,\dots$. Далее, применив классический алгоритм разложения в непрерывную дробь (алгоритм Евклида) можно извлечь из полученного результата период r .

На рис. 3.14 представлена структурная схема алгоритма Шора [1].

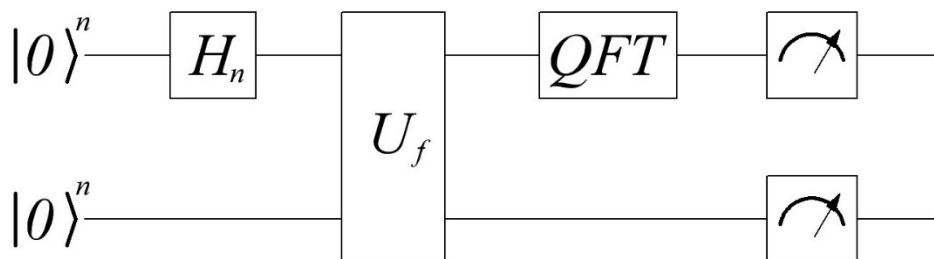


Рис. 3.14. Схема алгоритма Шора

Приведем классический пример реализации алгоритма Шора [1].

Пример 3.1: Допустим нам необходимо выполнить факторизацию числа $N = pq = 3 \cdot 5 = 15$. Используя функцию Эйлера можно определить функцию $f_a(x)$:

$$\Phi(N) = (q-1)(p-1) = (5-1)(3-1) = 8 \rightarrow a = 7 \rightarrow f_a(x) = 7^x \text{ mod } 15.$$

Функцию $f_a(x)$ можно записать в следующем виде:

$$f_a(x) = (7^8)^{x_3} \cdot (7^4)^{x_2} \cdot (7^2)^{x_1} \cdot (7^1)^{x_0} \text{ mod } 15.$$

Поскольку $(7^8)^{x_3} \text{ mod } 15 = 1$, $(7^4)^{x_2} \text{ mod } 15 = 1$ и $(7^2)^{x_1} \text{ mod } 15 = (4)^{x_1} \text{ mod } 15$ то можно переопределить функцию как:

$$f_a(x) = (4)^{x_1} \cdot (7)^{x_0} \text{ mod } 15.$$

На рис. 3.15 представлена квантовая схема, реализующая алгоритм Шора для данного примера.

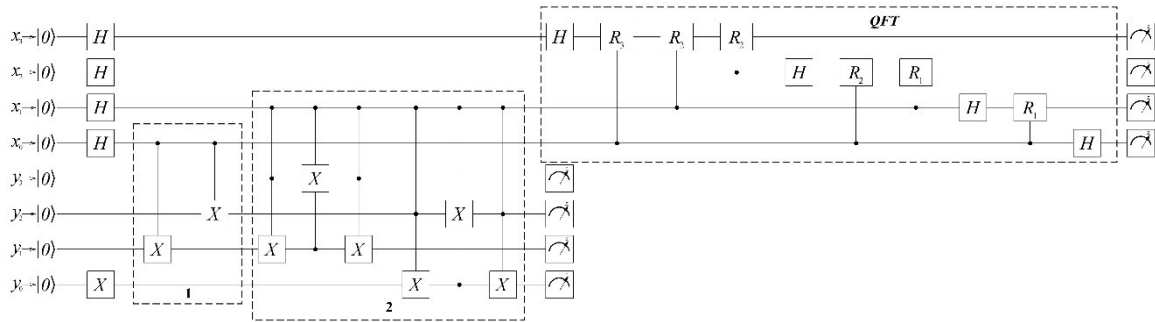


Рис. 3.15. Квантовая схема алгоритма Шора для $N=15$

На рис. 3.15 блок под номером **1** реализует умножение регистра $|y\rangle$ на 7, а блок под номером **2** – умножение на 4. Далее выполняется квантовое преобразование Фурье (блок QFT) и измерение результата преобразования.

Выполним моделирование данной схемы в системе *IBM Quantum Experience*. Результаты серии измерений представлены на рис. 3.16.

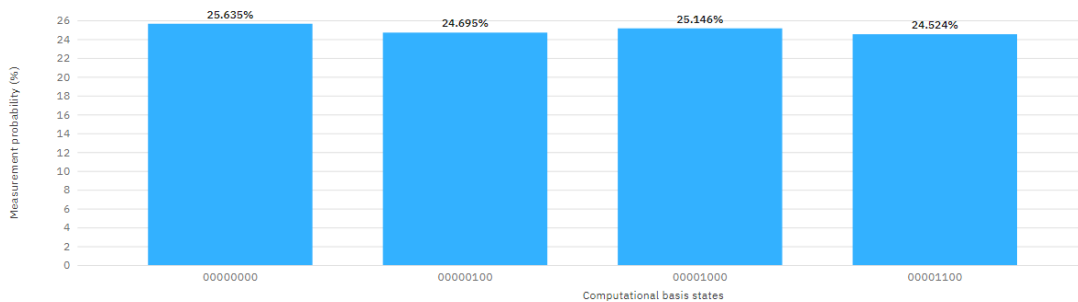


Рис. 3.16. Результаты симуляции алгоритма Шора для $N=15$

Из рис. 3.16 видно, что в результате измерений мы получили 0, 4, 8 и 12. Отбросив нулевой результат и вспомнив, что преобразование Фурье приведут к тому, что с высокой долей вероятности мы получим $\frac{jM}{r}$ для $j=1,2,\dots$ можно вычислить период r :

$$\frac{jM}{r} \rightarrow \frac{j2^n}{r} \rightarrow \begin{cases} j=1 \rightarrow \frac{2^4}{r} = 4 \rightarrow r=4 \\ j=2 \rightarrow \frac{2 \cdot 2^4}{r} = 8 \rightarrow r=4 \\ j=3 \rightarrow \frac{3 \cdot 2^4}{r} = 4 \rightarrow r=4 \end{cases}$$

Таким образом, мы определили период $r=4$. Зная период, мы можем определить числа p и q :

$$\text{НОД}\left(7^{\frac{r}{2}} + 1, 15\right) = \text{НОД}(50, 15) = 5,$$

$$\text{НОД}\left(7^{\frac{r}{2}} - 1, 15\right) = \text{НОД}(49, 15) = 3.$$

3.8. Упражнения к Главе 3

1. Покажите квантовые схемы для всех состояний Белла.
2. Запишите матрицы оракулов следующих функций:
 - a) $f(x_1, x_2) = x_1 \wedge x_2$;
 - б) $f(x_1, x_2) = x_1 \vee x_2$;
 - в) $f(x_1, x_2) = \overline{x_1} \vee x_2$;
 - г) $f(x_1, x_2) = \overline{x_1} \vee \overline{x_2}$;
 - д) $f(x_1, x_2) = x_1 \oplus x_2$.
3. Реализуйте **CZgate**, используя геты Адамара и **CXgate**.
4. Покажите схему квантового преобразования Фурье для системы пяти **кубитов**.
5. Запишите матрицу преобразования «инверсия относительно среднего» для $n=3$.
6. Запишите матрицу преобразования «инверсия относительно среднего» для $n=4$.

Глава 4. Лабораторные работы

Лабораторная работа №1

Основы работы в системе IBM Quantum Experience

1. Цель работы

Целью работы является знакомство с системой *IBM Quantum Experience*.

2. Реализация квантовых схем в системе IBM Quantum Experience

Реализация квантовых алгоритмов в лабораторных работах будет осуществляться с использованием системы *IBM Quantum Experience* [7]. Первым этапом работы с данной системой является регистрация на сайте <https://quantum-computing.ibm.com/>.

После прохождения регистрации страница сайта системы будет иметь следующий вид (рис. 4.1):

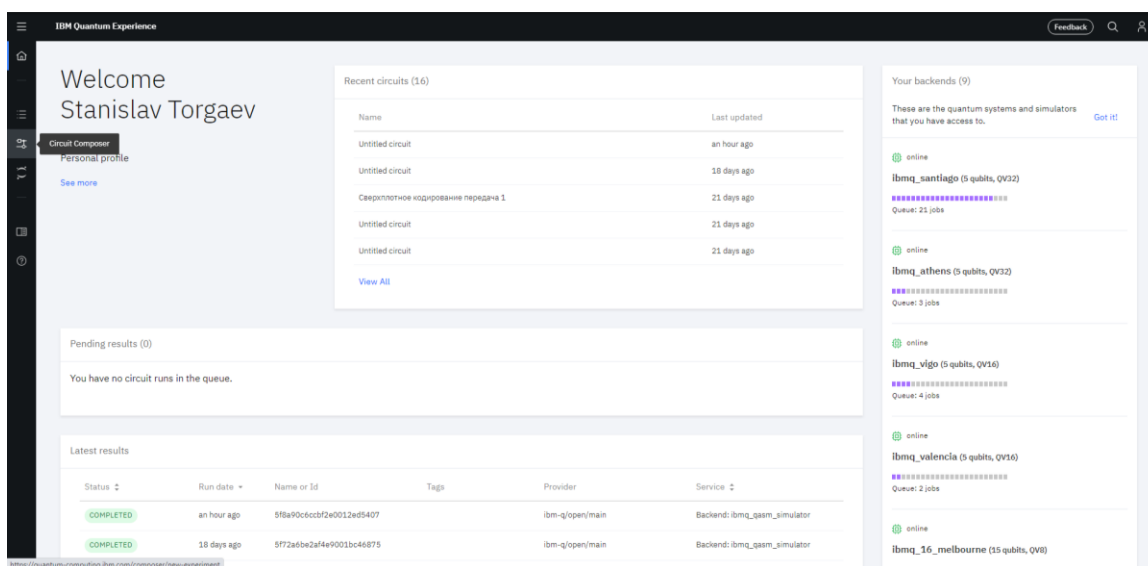


Рис. 4.1. Интерфейс страницы в системе IBM Quantum Experience

Для разработки квантовой схемы и проведения моделирования ее работы необходимо перейти на страницу «*Circuit Composer*». Переход осуществляется посредством соответствующей кнопки (рис. 4.1). Окно страницы «*Circuit Composer*» представлено на рис. 4.2.

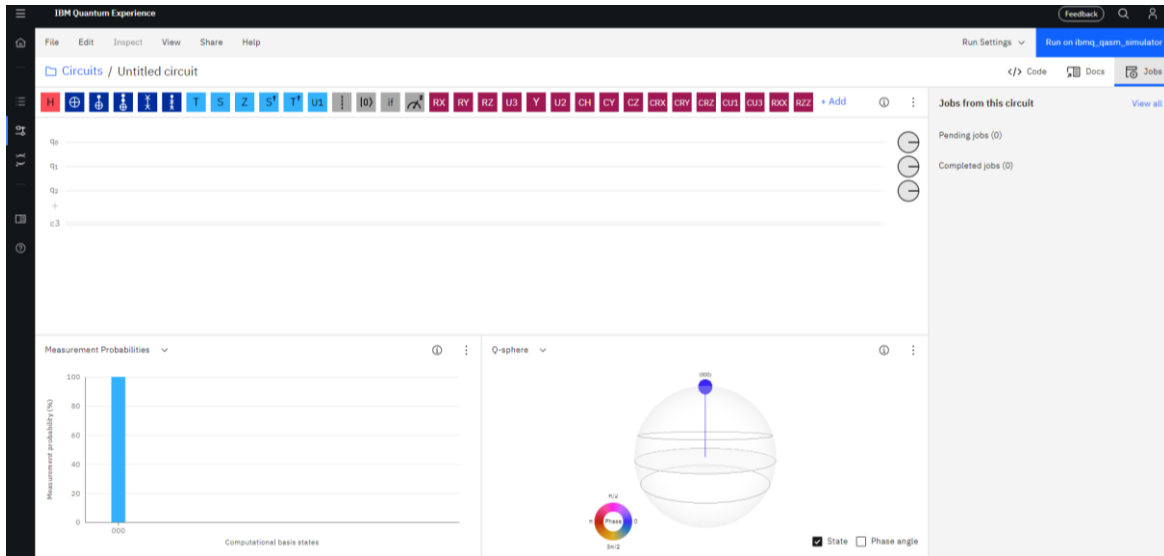


Рис. 4.2. Интерфейс страницы «Circuit Composer» в системе IBM Quantum Experience

Разработка квантовой схемы осуществляется посредством встроенного набора гейтов (рис. 4.3).



Рис. 4.3. Набор квантовых гейтов в системе IBM Quantum Experience

На рис. 4.4 представлено фрагменты области в которой производится сборка квантовой схемы. Система IBM Quantum Experience позволяет увеличивать и уменьшать количество используемых **кубитов**. Нарращивание количества **кубитов** осуществляется нажатием знака «+» (рис. 4.4), а удаление **кубитов** посредством нажатия на сам **кубит** (q_0 , q_1 , q_2 на рис. 4.4).



Рис. 4.4. Область сборки квантовой схемы в системе IBM Quantum Experience

Разработка квантовой схемы осуществляется посредством перемещения необходимых гейтов в область схемы и подключением их к соответствующим *кубитам*. На рис. 4.5 представлены примеры включения в схему различных гейтов.

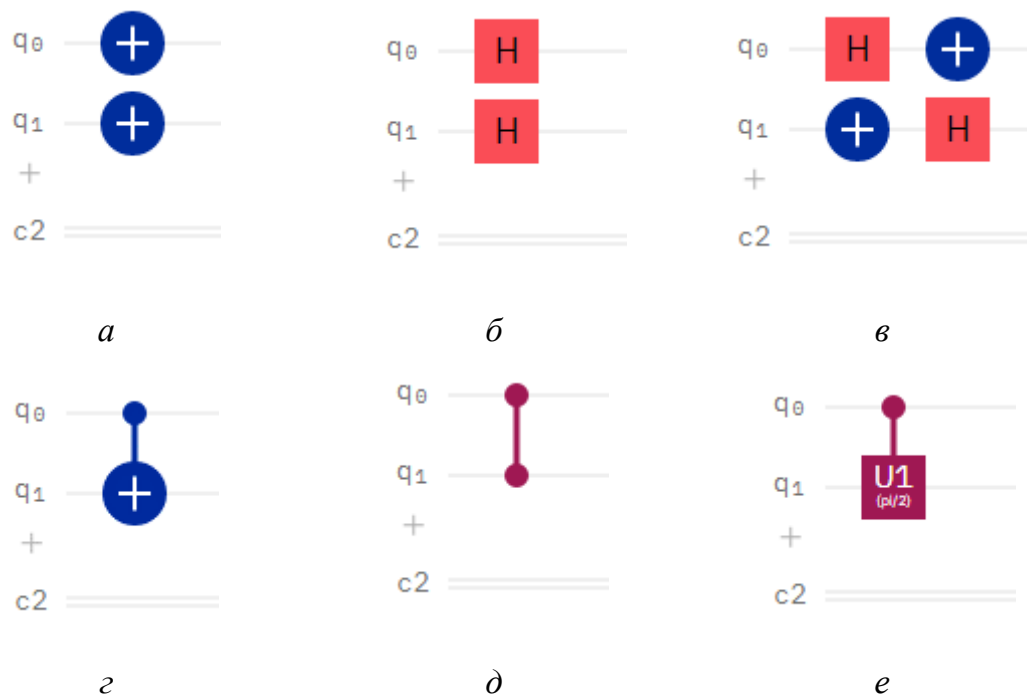


Рис. 4.5. Примеры подключения гейтов в системе IBM Quantum Experience

При нажатии на установленный в схеме гейт можно удалить его или внести изменения в его параметры и конфигурацию. Изменение конфигурации необходимо при смене контролируемого и контролирующих *кубитов* для контролируемых гейтов. Пример удаления гейта показан на рис. 4.6.

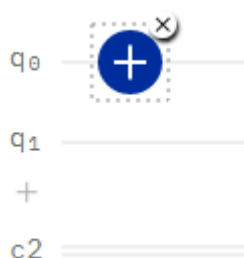


Рис. 4.6. Примеры удаления гейтов в системе IBM Quantum Experience

Для некоторых гейтов в системе IBM Quantum Experience предусмотрена возможность редактирования их параметров. В

частности, можно изменять углы в гейтах поворота R_x , R_y , R_z и гейтах $U1$, $U2$, $U3$, а также в соответствующих им контролируемых гейтах. Примеры изменения параметров показаны на рис. 4.7.

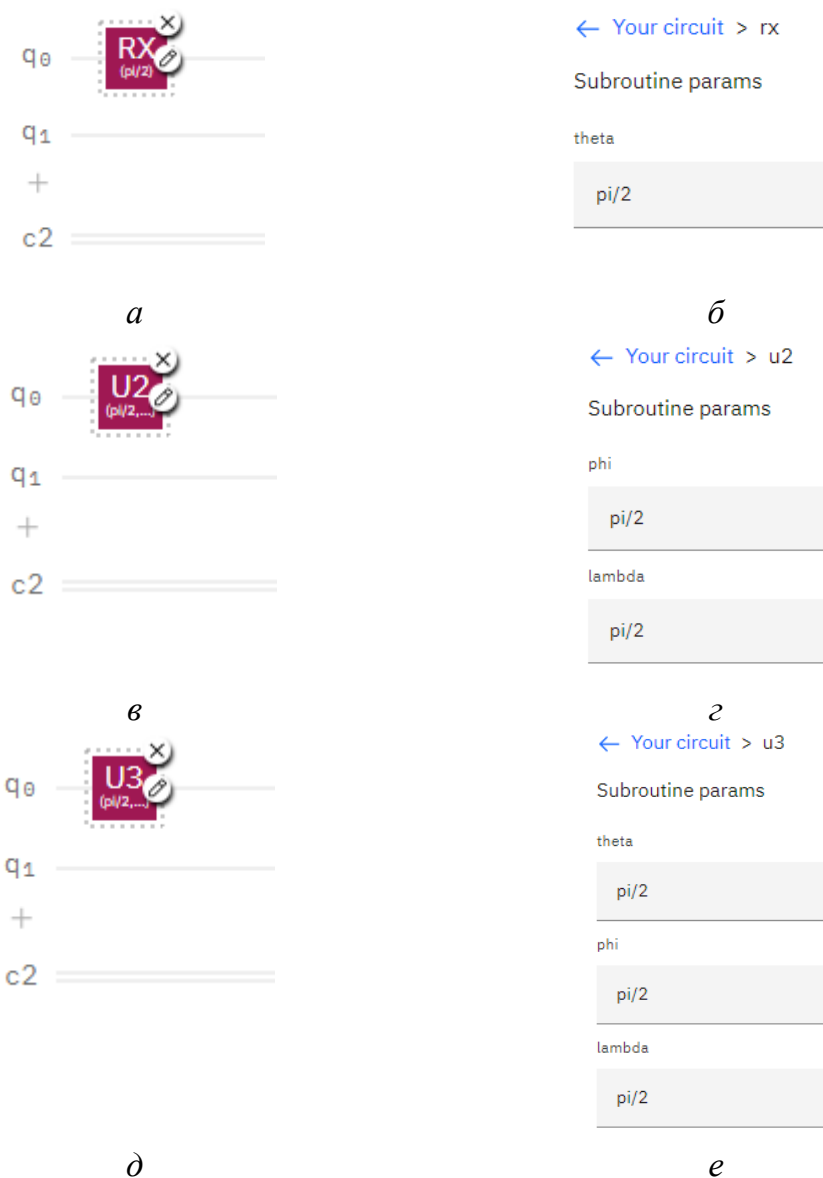


Рис. 4.7. Примеры контролируемых гейтов в системе IBM Quantum Experience

В случае использования в схеме контролируемых гейтов система предполагает возможность выбора контролирующего и контролируемого **кубита** (рис. 4.8). Изменение можно выполнить также в области редактирования.

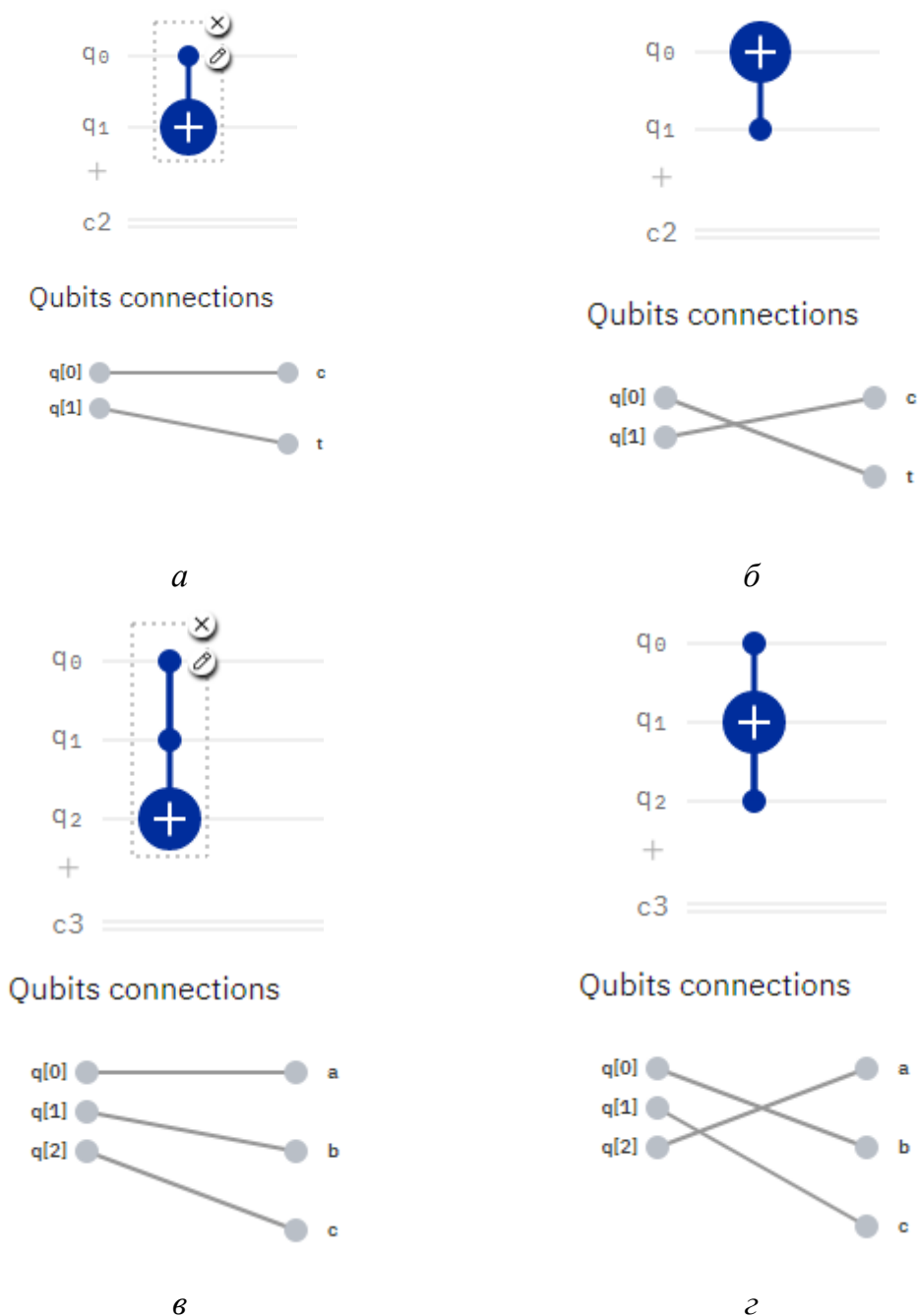


Рис. 4.8. Примеры выбора контролирующего и контролируемого кубита в системе IBM Quantum Experience

При разработке квантовой схемы система *IBM Quantum Experience* в режиме реального времени показывает расчетные (теоретические) значения вероятностей всех состояний кубитов квантовой системы, состояние векторов и их положение на сфере Блоха (рис. 4.9).

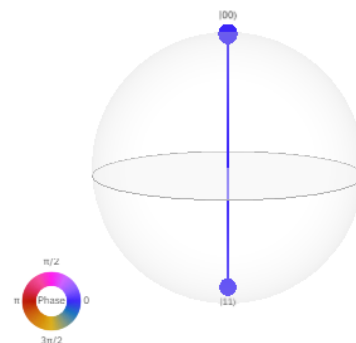
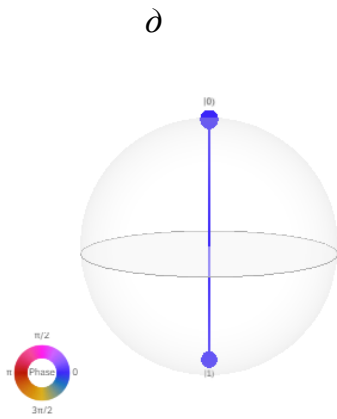
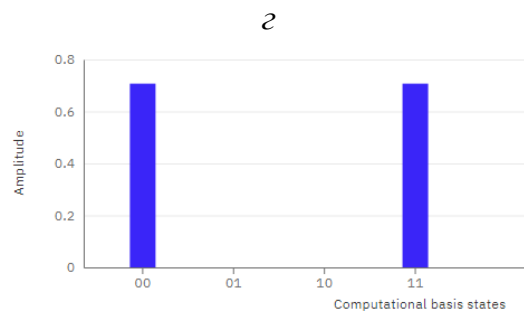
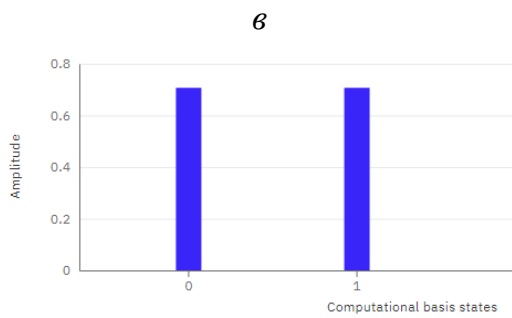
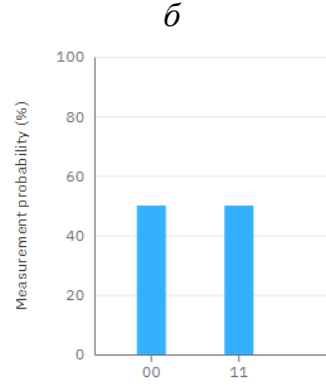
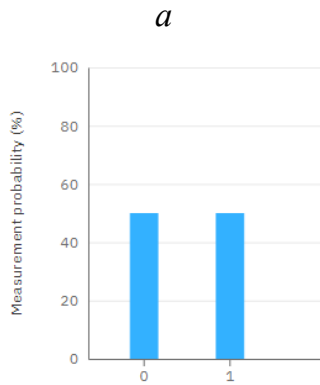
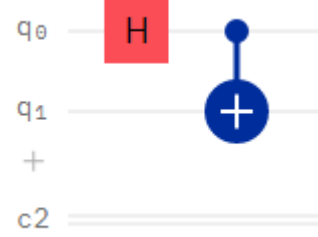


Рис. 4.9. Демонстрация процесса отображения амплитуд (д,е), вероятностей (в,г) и положений векторов на сфере Блоха (ж,з) в системе IBM Quantum Experience

Помимо теоретических расчетов состояний квантовой системы, в IBM Quantum Experience предусмотрена возможность реализации

квантового алгоритма с использованием реальных квантовых компьютеров и режима симуляции, в том числе, возможен выбор количества измерений. Настройка запуска симуляции осуществляется в панели «Run Settings» (рис. 4.10).

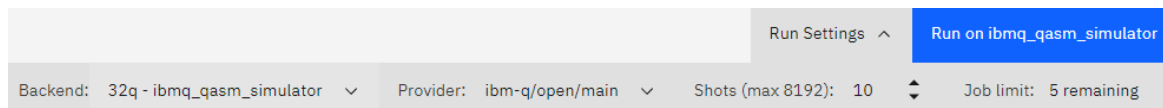
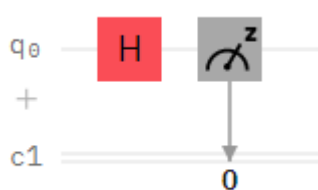
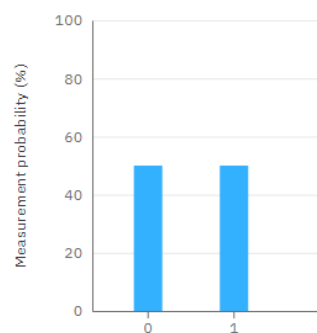


Рис. 4.10. Область настройки процесса симуляции в системе IBM Quantum Experience

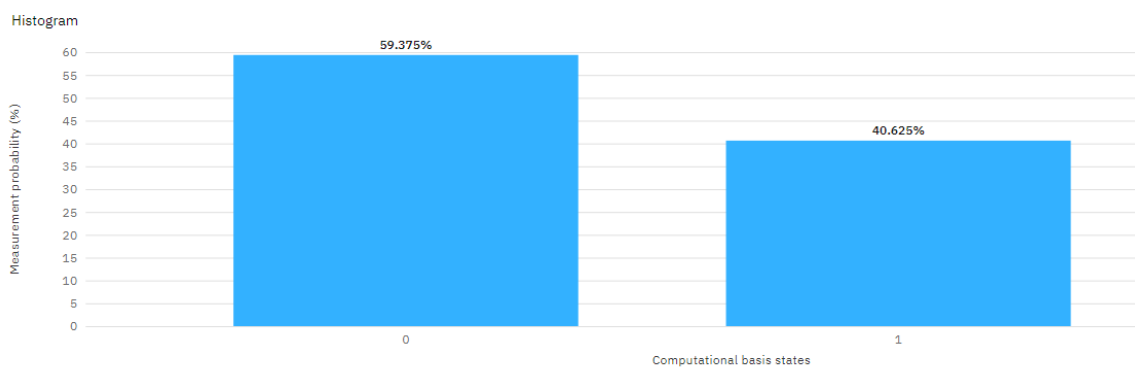
При запуске схемы в режиме симуляции или на каком-либо квантовом компьютере будут полученные вероятности нахождения системы в том или ином состоянии будут отличаться от теоретических. Следует отметить, что с увеличением числа измерений полученные вероятности будут стремиться к теоретическим значениям. Приведем пример запуска симуляции однокубитовой системы, представленной на рис. 4.11,а. В данном случае на кубит находящейся в состоянии $|0\rangle$ воздействуем гейтом Адамара, при этом мы получаем кубит в состоянии суперпозиции $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, т.е. теоретически данный кубит при измерении с вероятностью 50% принимает значение $|0\rangle$ или $|1\rangle$ (рис. 4.11,б). На рис. 4.11,в показаны вероятности нахождения квантовой системы при выполнении 64-х измерений, а на рис. 4.11,г – при выполнении 1024 измерений.



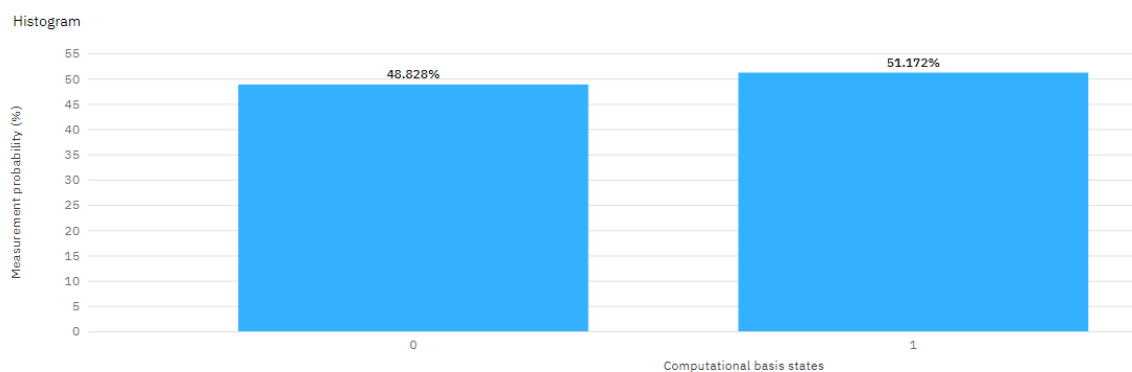
а



б



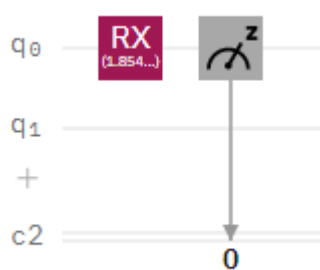
б



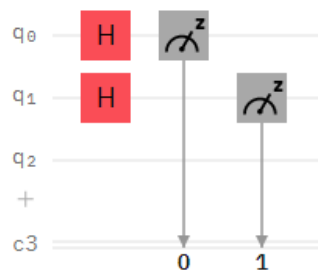
г

Рис. 4.11. Пример симуляции в системе IBM Quantum Experience: а) схема; б) теоретическое распределение вероятностей; в) распределение вероятностей для случая 64-х преобразований; г) распределение вероятностей для случая 1024-х преобразований

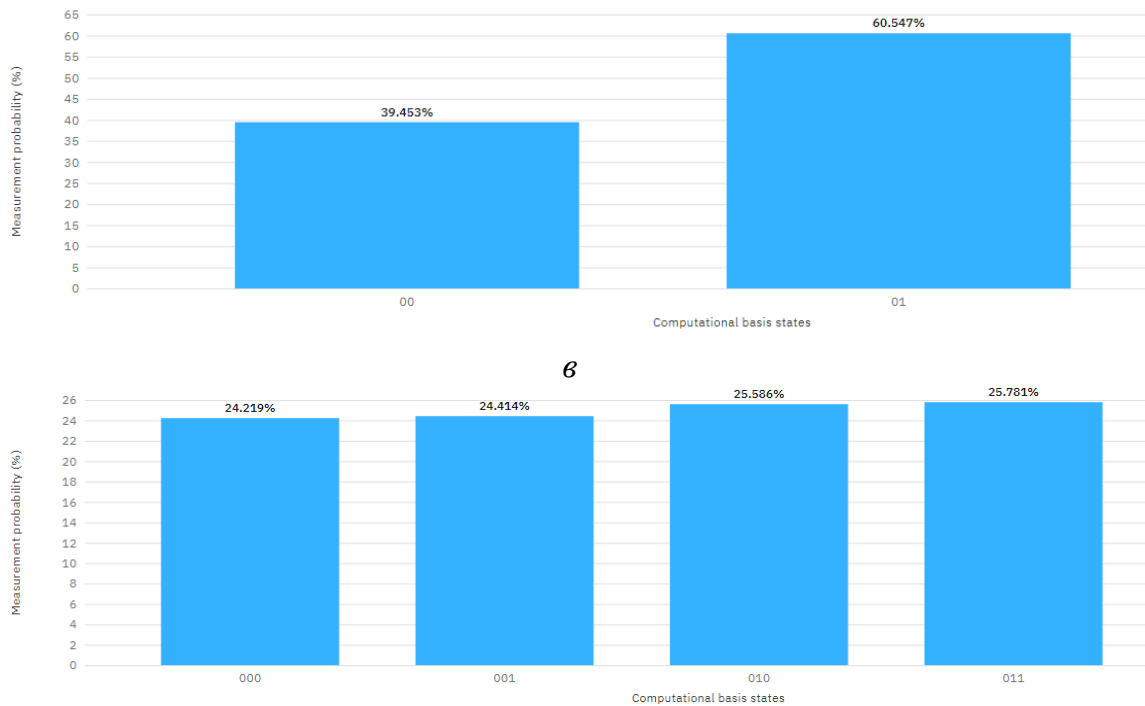
Выполнение измерений состояний **кубитов** в системе IBM Quantum Experience осуществляется с помощью инструмента «Measurement» графическое обозначение которого представлено на рис. 4.12,а. Система будет выполнять измерение состояния только тех **кубитов** к которым подключен данный инструмент (рис. 4.12,в,г).



а



б



б

г

Рис. 4.12. Пример измерения состояния системы

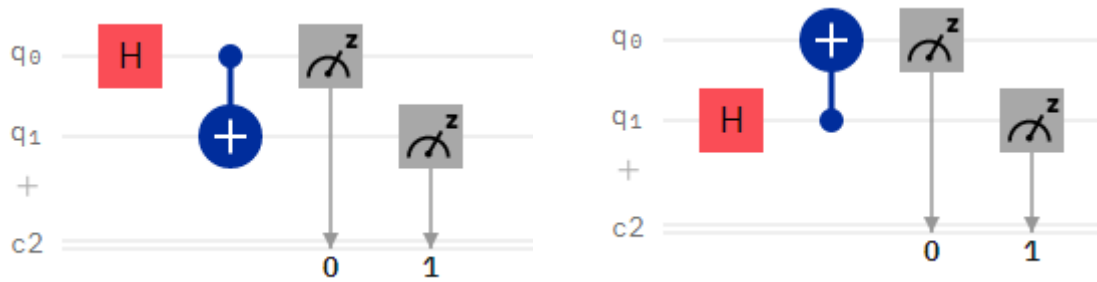
При измерении будут перечислены все возможные варианты состояния системы, а в случае если инструмент «*Measurement*» не подключен к какому-то из *кубитов*, то его состояние всегда будет иметь нулевое значение (рис. 4.12,г).

3. Программа работы

Выполните следующие пункты работы:

1. Выполните регистрацию в системе *IBM Quantum Experience*.
2. В «*Circuit Composer*» создайте схему из двух кубитов: один кубит должен иметь состояние $|0\rangle$, а второй кубит состояние $|1\rangle$. Состояние $|1\rangle$ можно получить с использованием гейта *X*. Примените операцию измерения для данных кубитов и выполните симулирование.
3. В «*Circuit Composer*» создайте схему из одного кубита находящегося в состоянии $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Примените операцию измерения к данному кубиту. Выполните симуляцию с различным количеством измерений: 1, 2, 8, 32, 64, 128, 512, 1024, 8192. Проанализируйте результаты измерений и сделайте выводы.

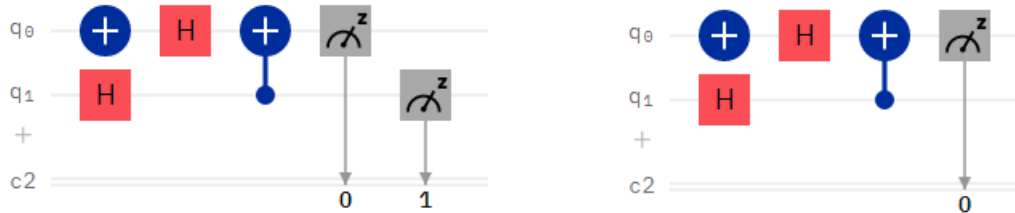
4. В «Circuit Composer» создайте схемы, представленные на рис. 4.13.



а б
Рис. 4.13. Квантовые схемы к заданию №4

Выполните симуляцию данных схем с числом измерений – 1024. Проанализируйте результаты симуляции и сделайте выводы.

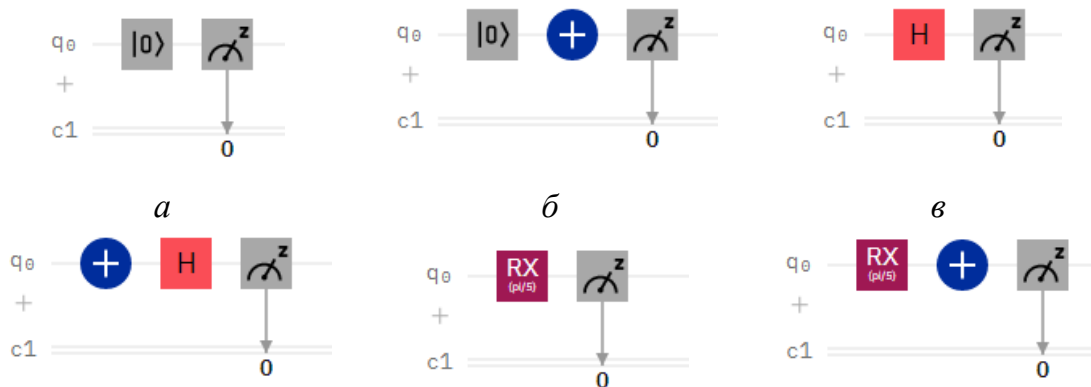
5. В «Circuit Composer» создайте схемы, представленные на рис. 4.14.



а б
Рис. 4.14. Квантовые схемы к заданию №5

Выполните симуляцию данных схем с числом измерений – 1024. Проанализируйте результаты симуляции и сделайте выводы.

6. В «Circuit Composer» создайте схемы, представленные на рис. 4.15.



g

$\delta \pi i/5$

$e \pi i/5$

Рис. 4.15. Квантовые схемы к заданию №6

Выполните симуляцию данных схем с числом измерений – 1024. Проанализируйте результаты симуляции и положение векторов на сфере Блоха. Сделайте выводы.

7. Оформите отчет по лабораторной работе. Отчет включает в себя скриншоты всех схем и результатов симуляции по программе работы, выводы.

Лабораторная работа №2

Однокубитные гейты











1. Цель работы

Целью работы является получение навыков применения однокубитных гейтов и реализация различных состояний суперпозиции кубита.

2. Однокубитные гейты в системе *IBM Quantum Experience*

В таблице 4.1 представлены варианты однокубитных гейтов, которые есть в системе *IBM Quantum Experience*.

Таблица 4.1. Однокубитные гейты в системе *IBM Quantum Experience*

Графическое обозначение	Название гейта	Вариант настройки
	Гейт Адамара	—
	гейт X	—
	гейт Y	—
	гейт Z	—
	гейт S	—
	гейт T	—
	гейт S^\dagger S -сопряженный гейт	—
	гейт T^\dagger T -сопряженный гейт	—
	гейт R_x	theta <input type="text" value="pi/2"/>
	гейт R_y	theta <input type="text" value="pi/2"/>

RZ	гейт Rz	phi <input type="text" value="pi/2"/>
U1	гейт U1	lambda <input type="text" value="pi/2"/>
U2	гейт U2	phi <input type="text" value="pi/2"/> lambda <input type="text" value="pi/2"/>
U3	гейт U3	theta <input type="text" value="pi/2"/> phi <input type="text" value="pi/2"/> lambda <input type="text" value="pi/2"/>

3. Программа работы

Выполните следующие пункты работы:

1. Получите кубит в состоянии суперпозиции $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

Выполните симуляцию.

2. Двумя способами получите кубит в состоянии суперпозиции $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Выполните симуляцию.

3. Получите кубит в состоянии суперпозиции $\frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle)$.

Выполните симуляцию.

4. Используя однокубитный гейт **Rx** получите кубит в состоянии суперпозиции $\alpha|0\rangle + \beta|1\rangle$ в соответствии с вариантом, представленном в таблице 4.2. Выполните симуляцию. Выполните их математическое обоснование результата.

Таблица 4.2. Варианты заданий

Вариант	Вероятность состояния $ 0\rangle$	Вероятность состояния $ 1\rangle$
1	5	95
2	10	90
3	20	80
4	30	70
5	40	60
6	55	45
7	60	40
8	70	30
9	80	20
10	90	10
11	95	5

5. Используя однокубитный гейт R_y получите кубит в состоянии суперпозиции $\alpha|0\rangle + \beta|1\rangle$ в соответствии с вариантом, представленном в таблице 4.2. Выполните симуляцию. Выполните их математическое обоснование результата.

6. Используя однокубитный гейт U_3 получите кубит в состоянии суперпозиции $\alpha|0\rangle + \beta|1\rangle$ в соответствии с вариантом, представленном в таблице 4.2. Выполните симуляцию. Выполните их математическое обоснование результата.

7. Используя однокубитный гейт R_x получите кубит в состоянии суперпозиции $\alpha|0\rangle - \beta|1\rangle$ в соответствии с вариантом, представленном в таблице 4.2. Выполните симуляцию. Выполните их математическое обоснование результата.

8. Используя однокубитный гейт R_y получите кубит в состоянии суперпозиции $\alpha|0\rangle - \beta|1\rangle$ в соответствии с вариантом, представленном в таблице 4.2. Выполните симуляцию. Выполните их математическое обоснование результата.

9. Используя однокубитный гейт U_3 получите кубит в состоянии суперпозиции $-\alpha|0\rangle + \beta|1\rangle$ в соответствии с вариантом, представленном в таблице 4.2. Выполните симуляцию. Выполните их математическое обоснование результата.

10. Используя однокубитные гейты Rx , Ry , $U3$ получите кубит в состоянии суперпозиции $\alpha|1\rangle + \beta|0\rangle$ в соответствии с вариантом, представленном в таблице 4.2. Выполните симуляцию. Выполните их математическое обоснование результата.

11. Экспериментально покажите унитарность гейта Адамара. Выполните их математическое обоснование результата.

12. Используя однокубитный гейт Rx получите кубит в состоянии суперпозиции $\alpha|0\rangle + \beta|1\rangle$ в соответствии с вариантом, представленном в таблице 4.2. Далее реализуйте схему, представленную на рис. 4.16. Выполните симуляцию. Пронаблюдав результаты симуляции выполните их математическое обоснование.

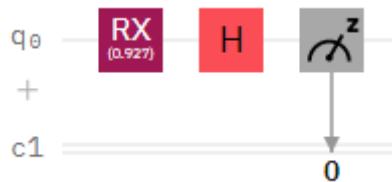


Рис. 4.16. Квантовая схема к заданию №12

13. Используя однокубитный гейт Rx получите кубит в состоянии суперпозиции $\alpha|0\rangle + \beta|1\rangle$ в соответствии с вариантом, представленном в таблице 4.2. Далее реализуйте схему, представленную на рис. 4.17. Выполните симуляцию. Пронаблюдав результаты симуляции выполните их математическое обоснование.



Рис. 4.17. Квантовая схема к заданию №13

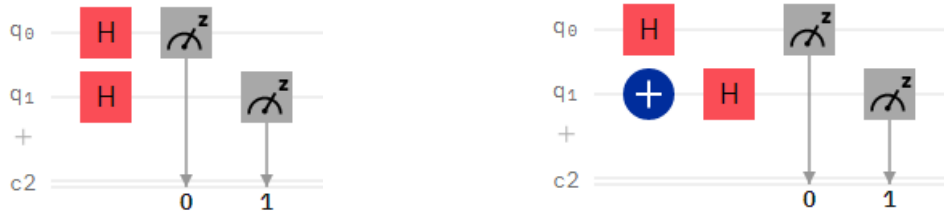
14. Реализуйте симуляцию схем, представленных на рис. 4.18. Проанализируйте результаты, выполните их математическое обоснование и поясните различие.



a б в

Рис. 4.18. Квантовые схемы к заданию №14

15. Реализуйте симуляцию схем, представленных на рис. 4.19. Проанализируйте результаты, выполните их математическое обоснование и поясните различие.



a б

Рис. 4.19. Квантовые схемы к заданию №15

16. Реализуйте трехкубитовую систему, к показано на рис. 4.20. В данной системы кубиты должны находиться в состояниях суперпозиции согласно варианту в таблице 4.3. Выполните симуляцию и проанализируйте результаты.

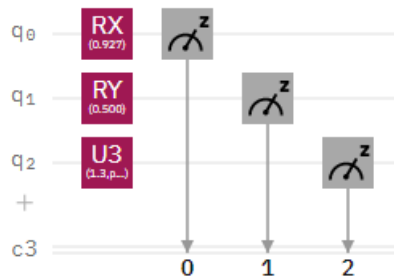


Рис. 4.20. Квантовая схема к заданию №16

Таблица 4.3. Варианты заданий

Вариант	Вероятность состояния $ 0\rangle$ первого кубита	Вероятность состояния $ 0\rangle$ второго кубита	Вероятность состояния $ 0\rangle$ третьего кубита
1	5	10	20
2	10	20	15
3	20	35	85
4	30	70	55
5	40	60	65
6	55	45	45
7	60	40	25
8	70	30	10

9	80	20	5
10	90	10	35
11	95	5	80

17. Оформите отчет по лабораторной работе. Отчет включает в себя скриншоты всех схем и результатов симуляции по программе работы, выводы.

Лабораторная работа №3

Контролируемые гейты


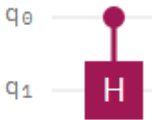



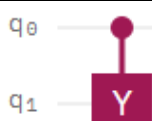

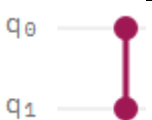



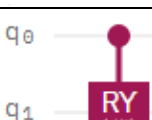
1. Цель работы


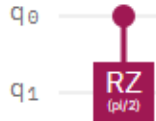

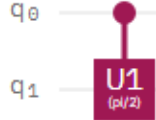

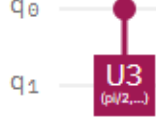

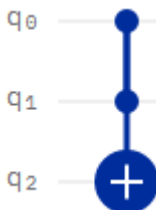
Целью работы является получение навыков применения однокубитных гейтов и реализации квантовых алгоритмов на их основе.

2. Контролируемые гейты в системе IBM Quantum Experience

В таблице 4.4 представлены варианты контролируемых гейтов, которые есть в системе *IBM Quantum Experience*, и описание их работы.

Таблица 4.4. Контролируемые квантовые гейты в системе *IBM Quantum Experience*

Графическое обозначение	Название гейта	Описание
	Контролируемый гейт Адамара	 Преобразование Адамара применяется к кубиту q_1 , если кубит q_0 находится в состоянии $ 1\rangle$.
	Контролируемый гейт X	 Инверсия (гейт X) применяется к кубиту q_1 , если кубит q_0 находится в состоянии $ 1\rangle$.
	Контролируемый гейт Y	 Гейт Y применяется к кубиту q_1 , если кубит q_0 находится в состоянии $ 1\rangle$.
	Контролируемый гейт Z	 Гейт Z применяется к кубиту q_1 , если кубит q_0 находится в состоянии $ 1\rangle$.
	Контролируемый гейт Rx	 Гейт Rx применяется к кубиту q_1 , если кубит q_0 находится в состоянии $ 1\rangle$.
	Контролируемый гейт Ry	 Гейт Ry применяется к кубиту q_1 , если кубит q_0 находится в состоянии $ 1\rangle$.

	Контролируемый гейт Rz	 <p>Гейт Rz применяется к кубиту q_1, если кубит q_0 находится в состоянии $1\rangle$.</p>
	Контролируемый гейт $U1$	 <p>Гейт $U1$ применяется к кубиту q_1, если кубит q_0 находится в состоянии $1\rangle$.</p>
	Контролируемый гейт $U2$	 <p>Гейт $U2$ применяется к кубиту q_1, если кубит q_0 находится в состоянии $1\rangle$.</p>
	Сдвоенный контролируемый гейт X	 <p>Гейт X применяется к кубиту q_2, если оба кубита q_0 и q_1 находятся в состоянии $1\rangle$.</p>

3. Программа работы

Выполните следующие пункты работы:

1. Реализуйте схему получения запутанного состояния двух кубитов $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Выполните симуляцию и обоснование результатов симуляции.
2. Реализуйте схему получения запутанного состояния двух кубитов $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. Выполните симуляцию и обоснование результатов симуляции.
3. Реализуйте схему получения запутанного состояния двух кубитов $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$. Выполните симуляцию и обоснование результатов симуляции.
4. Реализуйте схему получения запутанного состояния двух кубитов $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. Выполните симуляцию и обоснование результатов симуляции.
5. Реализуйте схему получения запутанного состояния двух кубитов согласно вашему варианту в таблице 4.5. Выполните симуляцию и обоснование результатов симуляции.

Таблица 4.5. Варианты заданий

Вариант	Состояние	Вероятность $ \alpha ^2$	Вероятность $ \beta ^2$
1	$\alpha 00\rangle + \beta 11\rangle$	5	95
2		10	90
3		20	80
4		30	70
5		80	20
6		90	10
7		95	5
8		5	95
9	$\alpha 01\rangle + \beta 10\rangle$	40	60
10		55	45
11		60	40
12		70	30
13		10	90
14		20	80
15		30	70
16		70	30

6. Реализуйте схему получения запутанного состояния двух кубитов $\alpha|00\rangle + \beta|01\rangle + \gamma|11\rangle$, согласно варианту в таблице 4.6. Выполните симуляцию и обоснование результатов симуляции.

Таблица 4.6. Варианты заданий

Вариант	Вероятность $ \alpha ^2$	Вероятность $ \beta ^2$	Вероятность $ \gamma ^2$
1	50	5	45
2	50	10	40
3	50	15	35
4	50	20	30
5	50	25	25
6	50	30	20
7	50	35	15

8	50	40	10
9	50	45	5

7. Реализуйте схему получения запутанного состояния двух кубитов $\alpha|01\rangle + \beta|10\rangle + \gamma|11\rangle$, согласно варианту в таблице 4.7. Выполните симуляцию и обоснование результатов симуляции.

Таблица 4.7. Варианты заданий

Вариант	Вероятность $ \alpha ^2$	Вероятность $ \beta ^2$	Вероятность $ \gamma ^2$
1	5	50	45
2	10	50	40
3	15	50	35
4	20	50	30
5	25	50	25
6	30	50	20
7	35	50	15
8	40	50	10
9	45	50	5

8. Реализуйте схему получения запутанного состояния двух кубитов $\alpha|00\rangle + \beta|01\rangle + \gamma|11\rangle$ с вероятностями $|\alpha|^2 = |\beta|^2 = |\gamma|^2 = 33.33\%.$ Выполните симуляцию и обоснование результатов симуляции.

9. Реализуйте схему получения запутанного состояния двух кубитов $\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$. Выполните симуляцию и обоснование результатов симуляции.

10. Реализуйте схему получения запутанного состояния двух кубитов $\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$. Выполните симуляцию и обоснование результатов симуляции.

11. Реализуйте схему получения запутанного состояния двух кубитов $\frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$. Выполните симуляцию и обоснование результатов симуляции.

12. Реализуйте схему получения запутанного состояния двух кубитов $\frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$. Выполните симуляцию и обоснование результатов симуляции.

13. Реализуйте схему получения запутанного состояния двух кубитов $-\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$. Выполните симуляцию и обоснование результатов симуляции.

14. Реализуйте схему получения запутанного состояния трех кубитов $\frac{1}{\sqrt{2}}(|010\rangle + |111\rangle)$. Выполните симуляцию и обоснование результатов симуляции.

15. Реализуйте схему получения запутанного состояния трех кубитов $\frac{1}{\sqrt{2}}(|001\rangle + |111\rangle)$. Выполните симуляцию и обоснование результатов симуляции.

16. Реализуйте схему получения запутанного состояния трех кубитов $\frac{1}{\sqrt{2}}(|001\rangle - |111\rangle)$. Выполните симуляцию и обоснование результатов симуляции.

17. Реализуйте схему получения запутанного состояния трех кубитов $\alpha|010\rangle + \beta|111\rangle$ с вероятностями согласно таблице 4.5. Выполните симуляцию и обоснование результатов симуляции.

18. Оформите отчет по лабораторной работе. Отчет включает в себя скриншоты всех схем и результатов симуляции по программе работы, выводы.

Лабораторная работа №4

Квантовые алгоритмы

1. Цель работы

Целью работы является получение навыков разработки квантовых алгоритмов в системе *IBM Quantum Experience*.

2. Программа работы

Выполните следующие пункты работы:

1. Реализуйте квантовый алгоритм передачи цифр $0 \div 3$ от Алисы к Бобу. Выполните симуляцию и обоснование результатов симуляции.
2. Реализуйте квантовый алгоритм передачи цифр $0 \div 3$ от Алисы к Бобу с использованием гетов «if». Выполните симуляцию и обоснование результатов симуляции.
3. Реализуйте алгоритм квантовой телепортации от Алисы к Бобу кубита в состоянии суперпозиции. Состояние кубита должно соответствовать варианту в таблице 4.8.

Таблица 4.8. Варианты заданий

Вариант	Вероятность состояния $ 0\rangle$	Вероятность состояния $ 1\rangle$
1	5	95
2	10	90
3	20	80
4	30	70
5	40	60
6	55	45
7	60	40
8	70	30
9	80	20
10	90	10
11	95	5

4. В системе *IBM Quantum Experience* реализуйте алгоритм Дойча для функций $f_1(x)=0$, $f_2(x)=1$, $f_3(x)=x$ и $f_3(x)=\bar{x}$. Выполните симуляцию для каждой функции и обоснование полученных результатов.

5. В системе *IBM Quantum Experience* реализуйте оракул функции $f(x_1, x_2) = x_1 \oplus x_2$. Выполните симуляцию и убедитесь в корректности работы.

6. В системе *IBM Quantum Experience* реализуйте алгоритм Дойча для функции $f(x_1, x_2) = x_1 \oplus x_2$. Выполните симуляцию и обоснование полученных результатов.

7. В системе *IBM Quantum Experience* реализуйте оракул функции $f(x_1, x_2) = \overline{x_1 \oplus x_2}$. Выполните симуляцию и убедитесь в корректности работы.

8. В системе *IBM Quantum Experience* реализуйте алгоритм Дойча для функции $f(x_1, x_2) = \overline{x_1 \oplus x_2}$. Выполните симуляцию и обоснование полученных результатов.

9. В системе *IBM Quantum Experience* реализуйте оракул функции $f(x_1, x_2) = x_1 \wedge x_2$ и реализуйте алгоритм Гровера. Выполните симуляцию и обоснование полученных результатов.

10. В системе *IBM Quantum Experience* реализуйте оракул функции $f(x_1, x_2) = \overline{x_1 \vee x_2}$ и реализуйте алгоритм Гровера. Выполните симуляцию и обоснование полученных результатов.

11. В системе *IBM Quantum Experience* реализуйте оракул функции $f(x_1, x_2) = x_1 \vee x_2$ и реализуйте алгоритм Гровера. Выполните симуляцию и обоснование полученных результатов.

12. В системе *IBM Quantum Experience* реализуйте функцию $f = 7 \bmod 15$. Выполните симуляцию и обоснование полученных результатов.

13. В системе *IBM Quantum Experience* реализуйте функцию $f = 7^2 \bmod 15$. Выполните симуляцию и обоснование полученных результатов.

14. В системе *IBM Quantum Experience* реализуйте функцию $f = 7^2 \bmod 15$. Выполните симуляцию и обоснование полученных результатов.

15. В системе *IBM Quantum Experience* реализуйте функцию алгоритм Шора для факторизации числа 15. Выполните симуляцию и обоснование полученных результатов.

16. В системе *IBM Quantum Experience* реализуйте алгоритм полного сумматора.

17. В системе *IBM Quantum Experience* реализуйте алгоритм умножения на 4.

18. В системе *IBM Quantum Experience* реализуйте алгоритм умножения на 5.

19. Оформите отчет по лабораторной работе. Отчет включает в себя скриншоты всех схем и результатов симуляции по программе работы, выводы.

Список литературы

1. Сысоев С.С. Введение в квантовые вычисления. Квантовые алгоритмы: учеб. пособие. – СПб.: Изд-во С.-Петерб. ун-та, 2019. – 144 с.
2. Квантовые вычисления: учеб. пособие. – Казань: Изд-во Казанского федерального университета, 2010. – 100 с.
3. Ожигов Ю.И. Квантовые вычисления: учебно-методическое пособие. – Москва: Изд-во Московского государственного университета, 2003. – 104 с.
4. Кайе Ф., Лафламм Р., Моска М. Введение в квантовые вычисления. – Москва-Ижевск: Изд-во НОЦ «Регулярная и хаотическая динамика» Институт компьютерных исследований, 2009. – 360 с.
5. Russian Quantum Center / RQC [Электронный ресурс] / YouTube канал – Режим доступа: <https://www.youtube.com/channel/UCpOG8wlozPr6qXnO3kGoIxQ>, свободный. – Загл. с экрана. – Яз. рус. (дата обращения 10/10/2020).
6. Get started with IBM Quantum Experience [Электронный ресурс] / Режим доступа: <https://quantum-computing.ibm.com/docs/>, свободный. – Загл. с экрана. – Яз. англ. (дата обращения 10/10/2020).
7. IBM Quantum Experience [Электронный ресурс] / Режим доступа: <https://quantum-computing.ibm.com/composer/new-experiment>, свободный. – Загл. с экрана. – Яз. англ. (дата обращения 10/10/2020).