

Содержание

Введение	2
1 Квантовые биты	2
2 Квантовые логические элементы	5
2.1 Однокубитовые логические элементы	5
2.1.1 Элемент Паули X	7
2.1.2 Элемент Паули Y	7
2.1.3 Элемент Паули Z	8
2.1.4 Элемент Адамара H	9
2.1.5 Элемент P	10
2.1.6 Элемент T	11
2.1.7 Элемент S	11
2.2 Двухкубитовые состояния и операторы	11
2.2.1 Управляемые преобразования	13
2.2.2 Элемент CNOT	14
2.2.3 Элемент SWAP	16
3 Квантовые схемы	18
3.1 Однокубитовые схемы	18
3.1.1 Схемы из одинаковых элементов	18
3.1.2 Схемы из разных элементов	20
3.2 Двухкубитовые квантовые схемы	20
4 Квантовые вычисления	22
4.1 Квантовые алгоритмы	23
4.1.1 Алгоритм Гровера	24
4.1.2 Алгоритм Шора	24
4.1.3 Алгоритм Дойча–Йожи	25
Заключение	26
Список используемой литературы	27

Введение

Квантовая информатика – относительно новый раздел науки, посвященный использованию квантовых объектов для обработки и передачи информации. В настоящее время большие усилия прикладываются к разработке квантового компьютера. Создаются квантовые элементы, строятся квантовые алгоритмы и разрабатывается архитектура квантового компьютера.

Основными разделами квантовой информатики являются: квантовые вычисления, квантовая связь и квантовая теория информации. Первый посвящен разработке квантовых алгоритмов решения вычислительных задач и физических принципов функционирования квантовых компьютеров, второй – разработке безопасных протоколов передачи информации (квантовая криптография) и третий – изучению различных аспектов квантовой информации, таких как меры информации и перепутанности, квантовые каналы и квантовые методы исправления ошибок. [1, 2, 3]

1 Квантовые биты

Элементарными классическими носителями информации являются биты – системы, которые могут принимать два различных состояния, обозначаемых обычно через 0 и 1. В отличие от них квантовые биты, или сокращенно кубиты (qubits – quantum bits), могут принимать бесконечно много различных состояний и представляют собой системы, квантовые состояния которых описываются вектором двумерного гильбертова пространства. Выберем в этом пространстве пару нормированных ортогональных состояний и обозначим их через $|0\rangle$ и $|1\rangle$ ($\langle 0|0\rangle = 1$, $\langle 1|1\rangle = 1$, $\langle 0|1\rangle = 0$), полагая, что эти состояния соответствуют значениям 0 и 1 классического бита. Базис, образованный этими состояниями, называется вычислительным базисом. А состояние кубита в общем виде задается волновой функцией вида:

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

где α и β – комплексные коэффициенты. Примером такой системы может служить фотон с двумя возможными поляризациями или электрон с двумя возможными направлениями спина.

При измерении состояния системы с волновой функцией (1), вероятность обнаружить ее в состоянии $|0\rangle$ равна $|\alpha|^2$, а вероятность обнаружить ее в состоянии $|1\rangle$ равна $|\beta|^2$. Сумма этих вероятностей равна единице [1, 2, 3, 8]:

$$|\alpha|^2 + |\beta|^2 = 1. \quad (2)$$

Кубит допускает геометрическое изображение. Рассмотрим сначала случай вещественных коэффициентов α и β . В этом случае удобно использовать тригонометрическое представление:

$$\alpha = \cos \varphi, \quad \beta = \sin \varphi. \quad (3)$$

Тогда условие (2) выполняется автоматически. На плоскости (α, β) условие (2) задает единичную окружность с центром в начале координат (рис. 1).

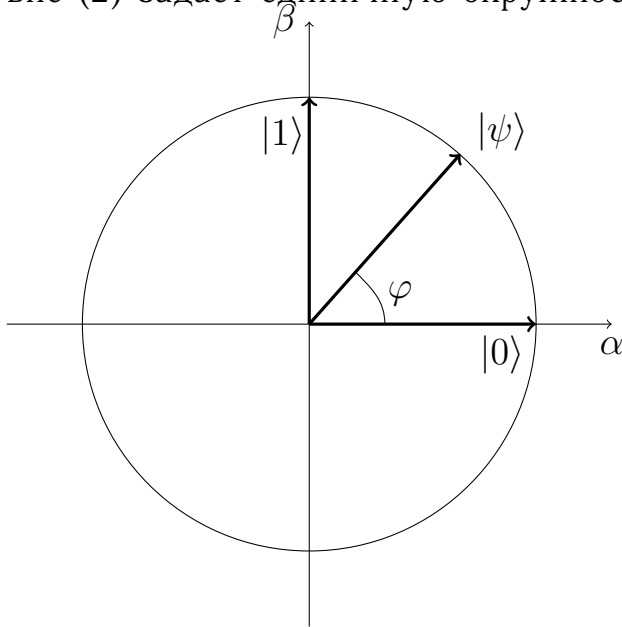


Рисунок 1 — Геометрическое изображение кубита для случая вещественных коэффициентов α и β

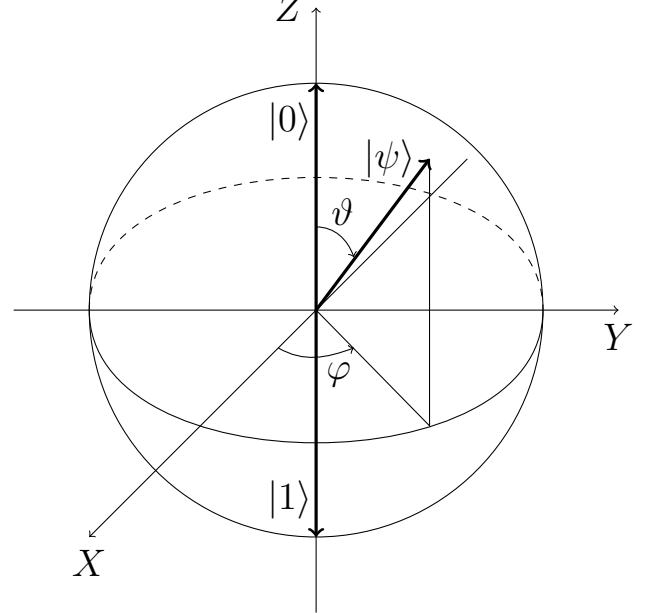


Рисунок 2 — Геометрическое изображение кубита для случая комплексных коэффициентов α и β

При $\varphi = 0$ по (3) получаем $|\psi\rangle = |0\rangle$, а при $\varphi = \pi/2$ получаем $|\psi\rangle = |1\rangle$.

В общем случае, комплексные коэффициенты α и β могут быть представлены в виде

$$\alpha = e^{i\gamma} \cos \frac{\vartheta}{2}, \quad \beta = e^{i\lambda} \sin \frac{\vartheta}{2}.$$

Тогда кубит (1) принимает следующий вид:

$$|\psi\rangle = e^{i\gamma} \cos \frac{\vartheta}{2} |0\rangle + e^{i\lambda} \sin \frac{\vartheta}{2} |1\rangle, \text{ или } |\psi\rangle = e^{i\gamma} \left(\cos \frac{\vartheta}{2} |0\rangle + e^{i(\lambda-\gamma)} \sin \frac{\vartheta}{2} |1\rangle \right).$$

Далее, поскольку векторы состояния определяются с точностью до общей фазы, можно положить $\gamma = 0$, тогда обозначая $\varphi = \lambda - \gamma$, получаем кубит в виде

$$|\psi\rangle = \cos \frac{\vartheta}{2} |0\rangle + e^{i\varphi} \sin \frac{\vartheta}{2} |1\rangle. \quad (4)$$

Таким образом, все многообразие состояний кубита описывается двумя действительными параметрами – ϑ и φ . Если использовать их в качестве углов сферической системы координат, то кубит изображается вектором единичной длины в трехмерном пространстве (рис. 2). Такое изображение кубита называется его представлением на сфере Блоха. В соответствии с (4), при $\vartheta = 0$ получаем $|0\rangle$, а при $\vartheta = \pi$ получаем $|1\rangle$ с точностью до фазового множителя $e^{i\varphi}$. [1, 2, 8]

На сфере Блоха бесконечно много точек. Соответственно, кубит может находиться в одном из бесконечного множества состояний. Однако, при измерении состояния кубита, он может быть найден в одном из двух возможных состояний – $|0\rangle$ или $|1\rangle$. Соответственно, из кубита можно извлечь один бит информации. [1, 2]

2 Квантовые логические элементы

Квантовый логический элемент (вентиль) – унитарное преобразование в пространстве состояний квантового регистра. Если регистр состоит из N кубитов, то размерность пространства состояний равна 2^N , так что матрица унитарного преобразования имеет размерность $2^N \times 2^N$.

2.1 Однокубитовые логические элементы

Любое воздействие на систему описывается линейным оператором \hat{U} , действующим на вектор состояния системы:

$$|\tilde{\psi}\rangle = \hat{U} |\psi\rangle.$$

Оператор \hat{U} является унитарным, что означает, что если исходное состояние системы нормировано, то и состояние, в которое система переходит после взаимодействия также является нормированным:

$$\langle\tilde{\psi}|\tilde{\psi}\rangle = \langle\psi|\hat{U}^\dagger\hat{U}|\psi\rangle = \langle\psi|\psi\rangle = 1.$$

Таким образом, можно рассматривать воздействие на кубит или их систему как процесс вычисления, в котором вектор $|\psi\rangle$ является входным сигналом, $|\tilde{\psi}\rangle$ – результатом вычисления, а оператор \hat{U} – вычислительным процессом (рис. 3).

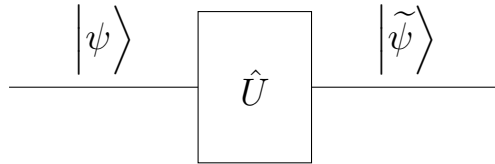


Рисунок 3 — Квантовый процесс вычисления

Унитарный оператор всегда обратим:

$$\hat{U}^\dagger\hat{U} = 1 \Rightarrow \hat{U}^\dagger\hat{U}\hat{U}^{-1} = \hat{U}^{-1} \Rightarrow \hat{U}^{-1} = \hat{U}^\dagger.$$

Согласно этому каждый квантовый вычислительный процесс обратим. То есть для каждого вычислительного процесса \hat{U} существует обратный процесс \hat{U}^{-1} ,

осуществляющий обратное преобразование. Классические вычислительные процессы не всегда обратимы.

Рассмотрим действие оператора на кубит. В силу линейности оператора:

$$\hat{U} |\psi\rangle = |\tilde{\psi}\rangle = \tilde{\alpha} |0\rangle + \tilde{\beta} |1\rangle = \hat{U} (\alpha |0\rangle + \beta |1\rangle) = \alpha \hat{U} |0\rangle + \beta \hat{U} |1\rangle. \quad (5)$$

Таким образом, действие оператора на кубит определяется его действием на базисные векторы $|0\rangle$ и $|1\rangle$. Разложим векторы $\hat{U} |0\rangle$ и $\hat{U} |1\rangle$ по базису:

$$\hat{U} |0\rangle = U_{00} |0\rangle + U_{10} |1\rangle, \quad \hat{U} |1\rangle = U_{01} |0\rangle + U_{11} |1\rangle. \quad (6)$$

Подставим (6) в (5):

$$|\tilde{\psi}\rangle = \tilde{\alpha} |0\rangle + \tilde{\beta} |1\rangle = \alpha (U_{00} |0\rangle + U_{10} |1\rangle) + \beta (U_{01} |0\rangle + U_{11} |1\rangle)$$

или

$$|\tilde{\psi}\rangle = (U_{00}\alpha + U_{01}\beta) |0\rangle + (U_{10}\alpha + U_{11}\beta) |1\rangle.$$

Таким образом,

$$\tilde{\alpha} = U_{00}\alpha + U_{01}\beta, \quad \tilde{\beta} = U_{10}\alpha + U_{11}\beta.$$

Переходя к матричному представлению оператора \hat{U} , вычислительный процесс $|\tilde{\psi}\rangle = \hat{U} |\psi\rangle$ можно записать в следующем виде:

$$\begin{pmatrix} \tilde{\alpha} \\ \tilde{\beta} \end{pmatrix} = \begin{pmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \quad \text{или } \tilde{\psi} = U\psi.$$

Существует несколько однокубитовых унитарных операторов, имеющих особое значение в квантовой информатике [1, 2]:

- элемент Паули X (элемент NOT),
- элемент Паули Y,
- элемент Паули Z,
- элемент Адамара H,
- элемент изменения фазы P,
- элемент $\pi/8$ (элемент T),
- элемент S.

2.1.1 Элемент Паули X

Элемент Паули X (обобщение элемента NOT) переводит $|0\rangle$ в $|1\rangle$, а $|1\rangle$ в $|0\rangle$:

$$\hat{X} |0\rangle = |1\rangle, \quad \hat{X} |1\rangle = |0\rangle. \quad (7)$$

Поскольку оператор линейный, то действие на произвольный кубит:

$$\hat{X} |\psi\rangle = \hat{X} (\alpha |0\rangle + \beta |1\rangle) = \alpha \hat{X} |0\rangle + \beta \hat{X} |1\rangle.$$

Используя (7):

$$\hat{X} |\psi\rangle = \alpha |1\rangle + \beta |0\rangle.$$

Таким образом, оператор \hat{X} меняет местами коэффициенты при базисных векторах.

Сравнивая последнее выражение с (6) запишем матрицу оператора \hat{X} :

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

Соответственно, в векторном виде процесс вычисления можно записать в виде

$$\begin{pmatrix} \tilde{\alpha} \\ \tilde{\beta} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}.$$

Интерпретируя геометрически, оператор \hat{X} поворачивает единичный вектор кубита на единичной окружности, отражая его от биссектрисы первого и третьего координатных углов $\tilde{\varphi} = \pi/2 - \varphi$ (рис. 4). [1]

2.1.2 Элемент Паули Y

Элемент Y является комплексным. Его матрица:

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

Поддействовав на вектор входного кубита, получим вектор выходного ку-

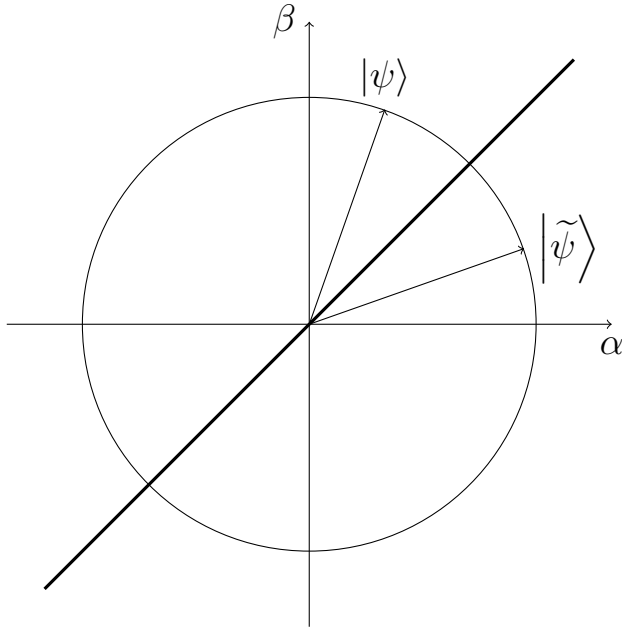


Рисунок 4 — Геометрическое изображение действия элемента X

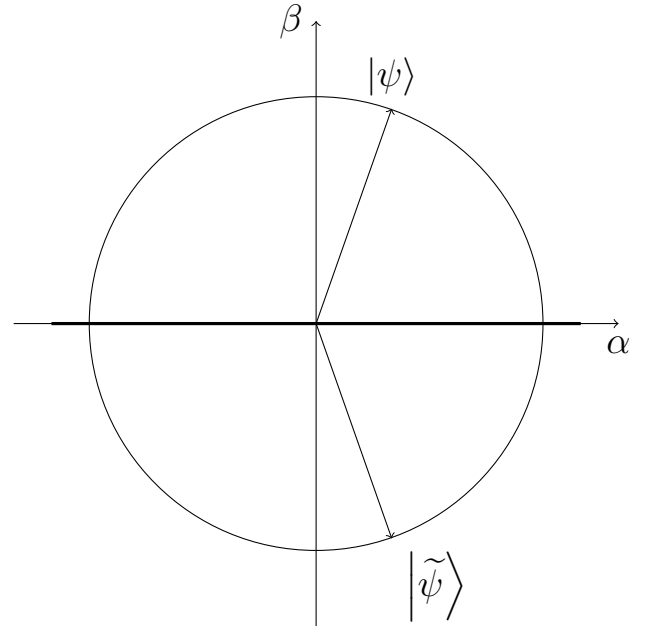


Рисунок 5 — Геометрическое изображение действия элемента Z

бита в виде:

$$\begin{pmatrix} \tilde{\alpha} \\ \tilde{\beta} \end{pmatrix} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} -i\beta \\ i\alpha \end{pmatrix}.$$

Таким образом, оператор \hat{Y} действует на кубит по правилу [1]:

$$\hat{Y} |\psi\rangle = -i\beta |0\rangle + i\alpha |1\rangle.$$

2.1.3 Элемент Паули Z

Оператор \hat{Z} должен не изменять $|0\rangle$, а вектор $|1\rangle$ переводить в $-|1\rangle$:

$$\hat{Z} |0\rangle = |0\rangle, \quad \hat{Z} |1\rangle = -|1\rangle. \quad (8)$$

Поскольку оператор линейный, то действие на произвольный кубит:

$$\hat{Z} |\psi\rangle = \hat{Z} (\alpha |0\rangle + \beta |1\rangle) = \alpha \hat{Z} |0\rangle + \beta \hat{Z} |1\rangle.$$

Используя (8):

$$\hat{Z} |\psi\rangle = \alpha |0\rangle - \beta |1\rangle.$$

Таким образом, мы получили нужный оператор \hat{Z} , меняющий знак у коэффициента при базисном векторе $|1\rangle$.

Сравнивая последнее выражение с (6) запишем матрицу оператора \hat{Z} :

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

Соответственно, в векторном виде процесс вычисления можно записать в виде

$$\begin{pmatrix} \tilde{\alpha} \\ \tilde{\beta} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ -\beta \end{pmatrix}.$$

Интерпретируя геометрически, оператор \hat{Z} поворачивает единичный вектор кубита на единичной окружности, отражая его от оси абсцисс $\tilde{\varphi} = -\varphi$ (рис. 5). В общем случае комплексных коэффициентов α и β , оператор \hat{Z} отражает вектор кубита на сфере Блоха от горизонтальной плоскости $\tilde{\vartheta} = -\vartheta$.

Является частным случаем элемента P с $\varphi = \pi$. [1, 2]

2.1.4 Элемент Адамара Н

Элемент Адамара Н задается матрицей:

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

Поддействовав на вектор входного кубита, получим вектор выходного кубита в виде:

$$\begin{pmatrix} \tilde{\alpha} \\ \tilde{\beta} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix}.$$

Таким образом, оператор \hat{H} действует на кубит по правилу:

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

Интерпретируя геометрически, оператор \hat{H} поворачивает единичный вектор кубита на единичной окружности, отражая его от луча под углом $\pi/8$ к оси абсцисс (рис. 6). [1, 2, 7]

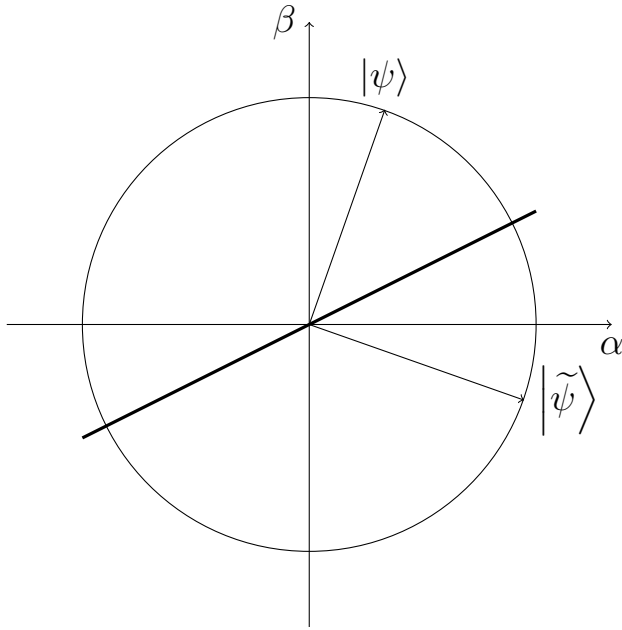


Рисунок 6 — Геометрическое изображение действия элемента Н

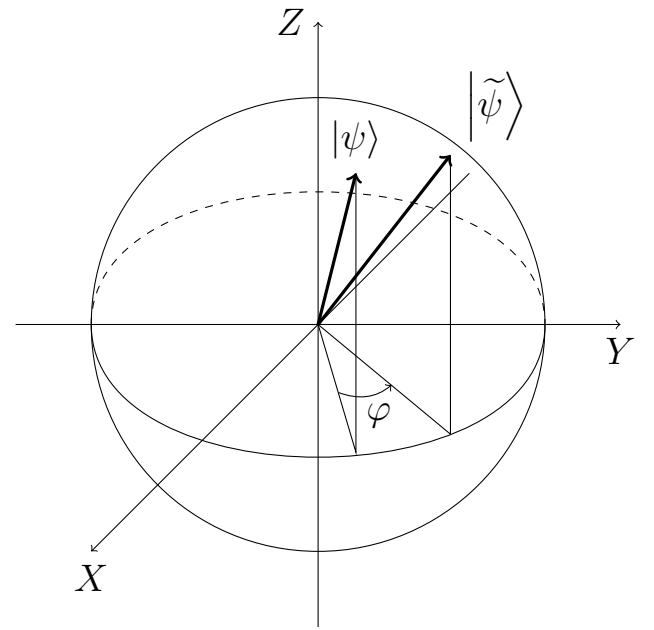


Рисунок 7 — Геометрическое изображение действия элемента Р

2.1.5 Элемент Р

Элемент изменения фазы Р задается матрицей:

$$P(\varphi) = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\varphi) \end{pmatrix}.$$

Подействовав на вектор входного кубита, получим вектор выходного кубита в виде:

$$\begin{pmatrix} \tilde{\alpha} \\ \tilde{\beta} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\varphi) \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \exp(i\varphi) \end{pmatrix}.$$

Таким образом, оператор \hat{P} действует на кубит по правилу:

$$\hat{P}|\psi\rangle = \alpha|0\rangle + \beta e^{i\varphi}|1\rangle.$$

Оператор \hat{P} изменяет фазу коэффициента при базисном векторе $|1\rangle$.

Интерпретируя геометрически, оператор \hat{P} поворачивает единичный вектор кубита на сфере Блоха на угол φ вокруг оси Z (рис. 7). [1, 2]

2.1.6 Элемент T

Элемент $\pi/8$ или T является частным случаем элемента P. Он задается матрицей

$$T = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\pi/8) \end{pmatrix},$$

а его оператор действует на кубит по правилу:

$$\hat{T}|\psi\rangle = \alpha|0\rangle + \beta e^{i\pi/8}|1\rangle.$$

Интерпретируя геометрически, оператор \hat{T} поворачивает единичный вектор кубита на сфере Блоха на угол $\pi/8$ вокруг оси Z. [1]

2.1.7 Элемент S

Элемент S также является частным случаем элемента P. Он задается матрицей

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

а его оператор действует на кубит по правилу:

$$\hat{S}|\psi\rangle = \alpha|0\rangle + i\beta|1\rangle.$$

Интерпретируя геометрически, оператор \hat{S} поворачивает единичный вектор кубита на сфере Блоха на угол $\pi/4$ вокруг оси Z. [1]

2.2 Двухкубитовые состояния и операторы

Рассмотрим квантовую систему, состоящую из двух кубитов:

$$|\psi_1\rangle = \alpha_1|0_1\rangle + \beta_1|1_1\rangle, \quad |\psi_2\rangle = \alpha_2|0_2\rangle + \beta_2|1_2\rangle, \quad (9)$$

где $|0_1\rangle$ и $|1_1\rangle$, $|0_2\rangle$ и $|1_2\rangle$ – базисные состояния первого и второго кубита соответственно, α_1 , β_1 , α_2 , β_2 – комплексные числа. Будем считать основные

состояния $|0_m\rangle$ и $|1_m\rangle$ ортонормированными:

$$\langle 0_m|0_m\rangle = 1, \langle 1_m|1_m\rangle = 1, \langle 0_m|1_m\rangle = 0.$$

Кубиты $|\psi_1\rangle$ и $|\psi_2\rangle$ относятся к разным векторным пространствам – H_1 и H_2 : $|\psi_1\rangle \in H_1$, $|\psi_2\rangle \in H_2$.

Пространство, элементами которого являются пары векторов, первый из которых принадлежит пространству H_1 , а второй – H_2 , называют тензорным произведением пространств H_1 и H_2 : $H_1 \otimes H_2$. Его элементы обозначим $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$. Базисные векторы этого пространства являются тензорными произведениями базисных векторов пространств H_1 и H_2 :

$$|00\rangle = |0_1\rangle \otimes |0_2\rangle, |01\rangle = |0_1\rangle \otimes |1_2\rangle, |10\rangle = |1_1\rangle \otimes |0_2\rangle, |11\rangle = |1_1\rangle \otimes |1_2\rangle.$$

Разложим двухкубитовое состояние по базисным векторам:

$$\begin{aligned} |\psi\rangle &= |\psi_1\rangle \otimes |\psi_2\rangle = (\alpha_1 |0_1\rangle + \beta_1 |1_1\rangle) \otimes (\alpha_2 |0_2\rangle + \beta_2 |1_2\rangle), \\ |\psi\rangle &= \alpha_1\alpha_2 |0_1\rangle \otimes |0_2\rangle + \alpha_1\beta_2 |0_1\rangle \otimes |1_2\rangle + \beta_1\alpha_2 |1_1\rangle \otimes |0_2\rangle + \beta_1\beta_2 |1_1\rangle \otimes |1_2\rangle. \end{aligned}$$

Обозначая $\gamma_{mn} = \langle mn|\psi\rangle$, получим

$$|\psi\rangle = \gamma_{00} |00\rangle + \gamma_{01} |01\rangle + \gamma_{10} |10\rangle + \gamma_{11} |11\rangle. \quad (10)$$

Вероятность найти двухкубитовую систему в состоянии $|mn\rangle$, как и в случае однокубитовой системы, составляет $|\gamma_{mn}|^2$, причем сумма таких вероятностей должна быть равна единице:

$$|\gamma_{00}|^2 + |\gamma_{01}|^2 + |\gamma_{10}|^2 + |\gamma_{11}|^2 = 1.$$

Отсюда следует, что система двух кубитов описывается вектором единичной длины. В четырехмерном комплексном пространстве коэффициентов α_m , β_m конец вектора $|\psi\rangle$ лежит на единичной сфере (10).

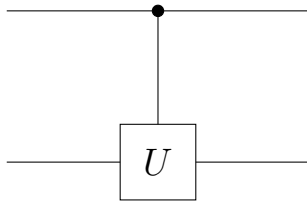
Операторы, определенные в пространствах H_1 и H_2 , действуют в их тензорном произведении $H_1 \otimes H_2$ покомпонентно [1, 2]:

$$(\hat{U}_1 \otimes \hat{U}_2) (|\psi_1\rangle \otimes |\psi_2\rangle) = (\hat{U}_1 |\psi_1\rangle) \otimes (\hat{U}_2 |\psi_2\rangle).$$

2.2.1 Управляемые преобразования

Унитарное преобразование, совершаемое в пространстве состояний квантового регистра над одним из кубитов, называется управляемым или условным, если его вид зависит от состояния остальных (одного или нескольких) кубитов. Кубит, над которым совершается преобразование называется управляемым, а кубиты, от состояния которых зависит вид преобразования, называются управляющими.

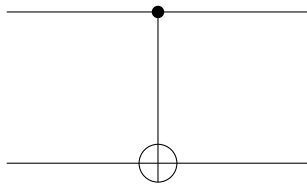
Наибольшее практическое значение имеют двухкубитовые вентили, когда один кубит является управляемым, а второй – управляющим. Графическое изображение элемента «Управляемое U », который обычно обозначается через CU , и структура его матрицы (в вычислительном базисе, упорядоченном по алфавиту) выглядят следующим образом:



$$CU = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{00} & U_{01} \\ 0 & 0 & U_{10} & U_{11} \end{pmatrix}$$

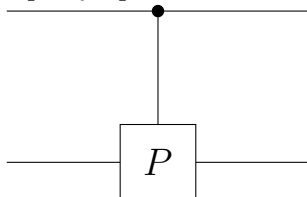
На схеме верхний провод соответствует управляющему кубиту, а нижний – управляемому, что отмечено черным кружком на верхнем проводе и вертикальной соединяющей линией. Черный кружок означает, что преобразование U совершается только тогда, когда управляющий кубит находится в состоянии $|1\rangle$.

Вместо оператора \hat{U} может стоять любой однокубитовый оператор. В частности, для оператора управляемого отрицания получаем:



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

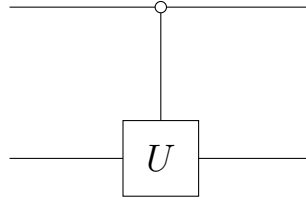
а для оператора управляемого изменения фазы:



$$CP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\varphi} \end{pmatrix}.$$

Часто рассматривают условные преобразования, в которых оператор U применяется к управляемому кубиту, если управляющий кубит находится в состоянии $|0\rangle$, а не $|1\rangle$. Такие логические элементы обозначаются через $\bar{C}U$ и

имеют следующее графическое изображение:



В общем случае условное преобразование может управляться состоянием нескольких кубитов и управлять состоянием нескольких кубитов.

Пусть регистр состоит из $n + k$ кубитов и U – унитарного k -кубитового оператора. Тогда $C^n U$ – условное преобразование U , совершаемое над последними k кубитами, если первые n кубитов находятся в состоянии $|1\rangle$. Его графическое представление и матрица:

$$C^n U = \begin{pmatrix} & & 0 & 0 & 0 \\ & E & 0 & 0 & 0 \\ & & 0 & 0 & 0 \\ 0 & 0 & 0 & & \\ 0 & 0 & 0 & U & \\ 0 & 0 & 0 & & \end{pmatrix},$$

где E – единичная матрица. [2]

2.2.2 Элемент CNOT

Одним из ключевых двухкубитовых операторов является CNOT. Он часто используется при построении схем и позволяет реализовывать другие элементы. [1, 2]

Действие на базисные векторы

Если первый (управляющий) кубит находится в состоянии $|0\rangle$, а второй – в одном из базисных состояний $|0\rangle$ или $|1\rangle$, то состояние такой двухкубитовой системы при воздействии на нее элементом CNOT не изменится.

Если же управляющий кубит находится в состоянии $|1\rangle$, то элемент CNOT переведет управляемый кубит в другое базисное состояние, состояние управляющего кубита при этом не изменится.

$$\begin{aligned} U_{CN} |0\rangle \otimes |0\rangle &= |0\rangle \otimes |0\rangle, & U_{CN} |0\rangle \otimes |1\rangle &= |0\rangle \otimes |1\rangle, \\ U_{CN} |1\rangle \otimes |0\rangle &= |1\rangle \otimes |1\rangle, & U_{CN} |1\rangle \otimes |1\rangle &= |1\rangle \otimes |0\rangle. \end{aligned}$$

Классическим аналогом данного элемента является элемент XOR [1]:

$$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1, \quad 1 \oplus 0 = 1, \quad 1 \oplus 1 = 0.$$

Действие на произвольный управляемый кубит

Рассмотрим систему, в которой управляющий кубит находится в состоянии $|0_1\rangle$, а управляемый – в произвольном состоянии $\alpha |0_2\rangle + \beta |1_2\rangle$. Вектор такого состояния:

$$|\psi\rangle = 1 |0_1\rangle \otimes (\alpha |0_2\rangle + \beta |1_2\rangle) = \alpha |0_1\rangle \otimes |0_2\rangle + \beta |0_1\rangle \otimes |1_2\rangle = \alpha |00\rangle + \beta |01\rangle.$$

Действуя элементом CNOT на такой вектор, получим его же – состояние системы не изменится:

$$|\tilde{\psi}\rangle = U_{CN} |\psi\rangle = |\psi\rangle.$$

Таким образом, каким бы ни был управляемый кубит, система не изменяет своего состояния при управляющем кубите, равном $|0_1\rangle$.

Рассмотрим систему, в которой управляющий кубит находится в состоянии $|1_1\rangle$, а управляемый – в произвольном состоянии $\alpha |0_2\rangle + \beta |1_2\rangle$. Вектор такого состояния:

$$|\psi\rangle = 1 |1_1\rangle \otimes (\alpha |0_2\rangle + \beta |1_2\rangle) = \alpha |1_1\rangle \otimes |0_2\rangle + \beta |1_1\rangle \otimes |1_2\rangle = \alpha |10\rangle + \beta |11\rangle.$$

Действуя элементом CNOT на такой вектор, получим:

$$|\tilde{\psi}\rangle = U_{CN} |\psi\rangle = \beta |10\rangle + \alpha |11\rangle.$$

Таким образом, если управляющий кубит равен $|1_1\rangle$, то действие CNOT на управляемый кубит эквивалентно действию элемента NOT. [2]

Действие на произвольный управляющий кубит

Если на управляющий вход элемента CNOT подать произвольный кубит

$$|\psi\rangle_1 = \alpha |0_1\rangle + \beta |1_1\rangle,$$

а на управляемый – нулевой базисный вектор $|0_2\rangle$, то состояние системы:

$$\psi = (\alpha |0_1\rangle + \beta |1_1\rangle) \otimes |0_2\rangle = \alpha |00\rangle + 0 |01\rangle + \beta |10\rangle + 0 |11\rangle.$$

Тогда выходной вектор $|\tilde{\psi}\rangle = U_{CN}|\psi\rangle$:

$$|\tilde{\psi}\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ 0 \\ \beta \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha \\ 0 \\ 0 \\ \beta \end{pmatrix} \quad (11)$$

Если на вход элемента CNOT подать две копии входного кубита, то двух-кубитовое состояние системы:

$$|\psi\rangle = (\alpha|0_1\rangle + \beta|1_1\rangle) \otimes (\alpha|0_2\rangle + \beta|1_2\rangle) = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle. \quad (12)$$

Приравнивая (11) и (12) получаем

$$\alpha^2 = \alpha, \quad \alpha\beta = 0, \quad \beta^2 = \beta.$$

У этой системы есть три возможных решения:

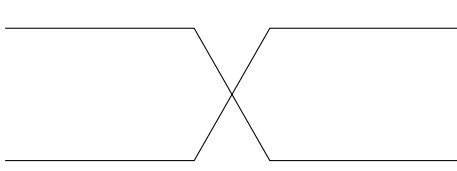
$$\alpha = 0, \beta = 0; \quad \alpha = 1, \beta = 0; \quad \alpha = 0, \beta = 1.$$

В полученных случаях, соответствующие классическим состояниям, являются единственно возможными случаями копирования (клонирования) кубита. В общем случае неизвестного кубита $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ клонирование невозможно.

Невозможность клонирования доказана для произвольного унитарного оператора. Многократное копирование кубита позволило бы извлечь сколь угодно много информации из одного кубита при помощи многократных измерений состояния копий исходного кубита. [2]

2.2.3 Элемент SWAP

Элемент SWAP обеспечивает обмен состояниями двух кубитов. Его матрица и графическое изображение:



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

Пусть первый кубит находится в состоянии $|\psi_1\rangle$, а второй – в состоянии $|\psi_2\rangle$:

$$\psi_1 = \alpha_1 |0_1\rangle + \beta_1 |1_1\rangle, \quad \psi_2 = \alpha_2 |0_2\rangle + \beta_2 |1_2\rangle.$$

Тогда система находится в состоянии

$$\begin{aligned} |\psi\rangle &= |\psi_1\rangle \otimes |\psi_2\rangle = (\alpha_1 |0_1\rangle + \beta_1 |1_1\rangle) \otimes (\alpha_2 |0_2\rangle + \beta_2 |1_2\rangle) = \\ &= \alpha_1 \alpha_2 |00\rangle + \alpha_1 \beta_2 |01\rangle + \beta_1 \alpha_2 |10\rangle + \beta_1 \beta_2 |11\rangle. \end{aligned}$$

Состояние системы после воздействия оператором SWAP:

$$|\tilde{\psi}\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha_1 \alpha_2 \\ \alpha_1 \beta_2 \\ \beta_1 \alpha_2 \\ \beta_1 \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 \alpha_2 \\ \beta_1 \alpha_2 \\ \alpha_1 \beta_2 \\ \beta_1 \beta_2 \end{pmatrix}.$$

Такой результат может быть получен умножением $|\psi_1\rangle \otimes |\psi_2\rangle$, если поменять местами коэффициенты α и β у этих векторов [2]:

$$\alpha_1 \leftrightarrow \alpha_2, \quad \beta_1 \leftrightarrow \beta_2$$

$$\begin{aligned} |\psi_1\rangle \otimes |\psi_2\rangle &= (\alpha_2 |0_1\rangle + \beta_2 |1_1\rangle) \otimes (\alpha_1 |0_2\rangle + \beta_1 |1_2\rangle) = \\ &= \alpha_2 \alpha_1 |00\rangle + \alpha_2 \beta_1 |01\rangle + \beta_2 \alpha_1 |10\rangle + \beta_2 \beta_1 |11\rangle. \end{aligned}$$

3 Квантовые схемы

3.1 Однокубитовые схемы

Рассмотрим два последовательно включенных однокубитовых квантовых логических элемента. На вход первого элемента поступает кубит, описываемый волновым вектором $|\psi\rangle$, действие первого элемента на кубит описывается оператором \hat{U}_1 , действие второго элемента – \hat{U}_2 (рис. 8).

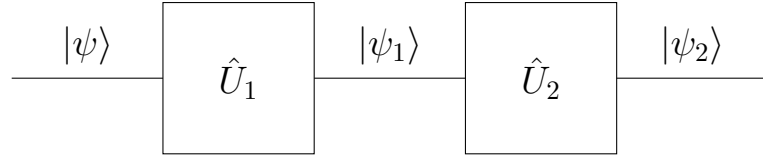


Рисунок 8 — Действие квантовой схемы на кубит

Действие последовательных преобразований элементами на кубит можно записать следующим образом:

$$|\psi_2\rangle = \hat{U}_2 |\psi_1\rangle = \hat{U}_2 \hat{U}_1 |\psi\rangle.$$

В матричном представлении последовательно действие операторами описывается матрицей U , равной произведению матриц U_1 и U_2 :

$$U = U_2 U_1.$$

Обобщив на n последовательных элементов, получаем процесс вычисления в виде [1]:

$$|\psi_n\rangle = \hat{U}_n \hat{U}_{n-1} \dots \hat{U}_1 |\psi\rangle; \quad U = U_n U_{n-1} \dots U_1.$$

3.1.1 Схемы из одинаковых элементов

1. **Элемент X:** поскольку элемент X имеет смысл квантового отрицания, то при воздействии на кубит двумя элементами X подряд должен получиться тот же кубит. Это означает, что квадрат матрицы элемента X должен быть равен единичной матрице:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad X^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0+1 & 0+0 \\ 0+0 & 1+0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E.$$

Это очевидно, если учесть что элементы X , Y и Z построены на матрицах Паули, квадрат которых равен единичной матрице.

2. Элемент Y :

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \quad Y^2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 - i^2 & 0 + 0 \\ 0 + 0 & -i^2 + 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E.$$

3. Элемент Z :

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}; \quad Z^2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 + 0 & 0 - 0 \\ 0 - 0 & 0 + 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E.$$

- 4. Элемент H :** поскольку элемент H имеет смысл отражения вектора кубита от луча под углом $\pi/8$ к оси абсцисс, то при воздействии на кубит двумя элементами H подряд должен получиться тот же кубит. Это означает, что квадрат матрицы элемента H должен быть равен единичной матрице:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}; \quad H^2 = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 + 1 & 1 - 1 \\ 1 - 1 & 1 + 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E.$$

5. Элемент P :

$$P = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}; \quad P^2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix} = \begin{pmatrix} 1 + 0 & 0 + 0 \\ 0 + 0 & 0 + e^{i2\varphi} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i2\varphi} \end{pmatrix} = 2P.$$

Таким образом, последовательное воздействие одинаковыми элементами P повернет вектор кубита на угол, вдвое больший угла поворота при одинарном воздействии элементом P .

- 6. Элемент S :** последовательно воздействующие на кубит элементы S , поворачивающие кубит на угол $\pi/2$, повернут его на угол π :

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}; \quad S^2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = \begin{pmatrix} 1 + 0 & 0 + 0 \\ 0 + 0 & 0 - 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z.$$

- 7. Элемент T :** Последовательно воздействующие на кубит элементы T , по-

ворачивающие кубит на угол $\pi/8$, повернут его на угол $\pi/4$:

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}; \quad T^2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/8} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/8} \end{pmatrix} = \begin{pmatrix} 1+0 & 0+0 \\ 0+0 & 0+e^{i\pi/4} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}.$$

Если последовательно соединить 4 элемента T , то они повернут кубит на угол $\pi/2$, а если соединить 8 – то на угол π [1, 2]:

$$T^4 = S, \quad T^8 = Z.$$

3.1.2 Схемы из разных элементов

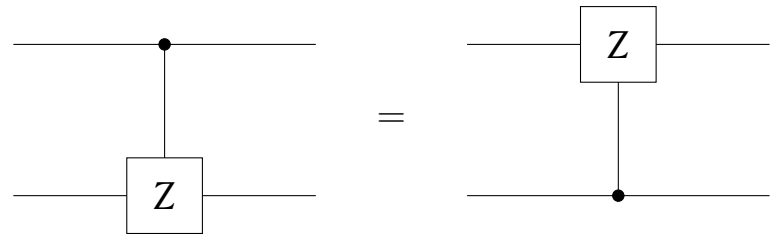
В основном при построении схем из нескольких элементов используют три тождества [1, 2]:

$$\begin{aligned} HXH &= \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z, \\ HYH &= \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = - \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = -Y, \\ HZH &= \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = X. \end{aligned}$$

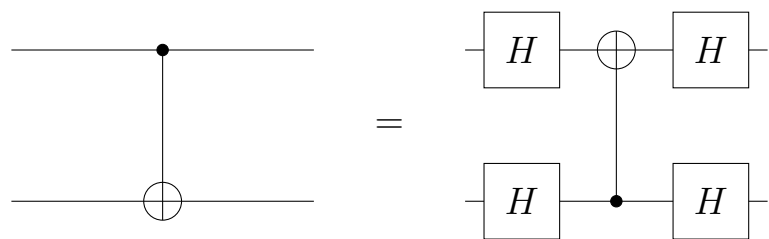
3.2 Двухкубитовые квантовые схемы

В отличие от классических элементов, в квантовых элементах выбор управляющего и управляемого кубитов зависит от того, в каком базисе действует оператор. [2]

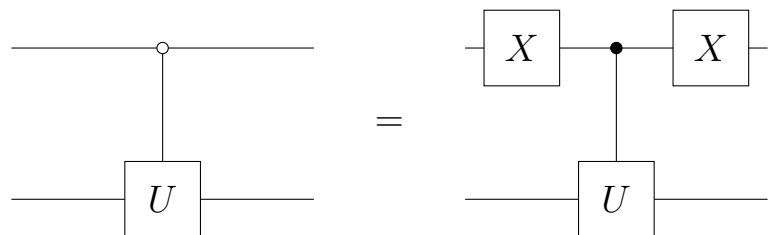
Например,



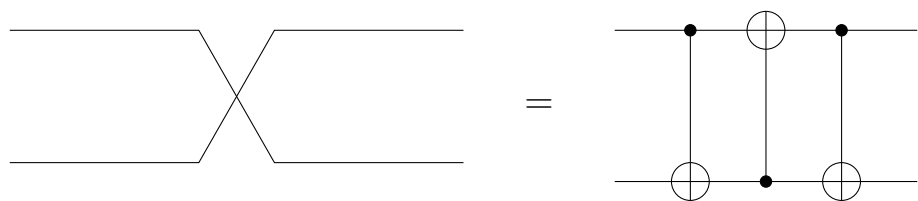
НО



Преобразование $\bar{C}U$ можно представить в виде



Элемент SWAP можно построить из трех элементов CNOT, поочередно действующих в разных базисах:



4 Квантовые вычисления

Квантовый компьютер – это устройство, способное производить параллельные вычисления, оперируя с квантовой суперпозицией состояний кубитов. [2, 3, 7]

Квантовый компьютер состоит из конечного множества кубитов, называемого квантовым регистром. Пространство состояний квантового регистра имеет размерность $N = 2n$, где n – число кубитов. Если нумеровать кубиты с 0 до $n - 1$, то вычислительный базис пространства состояний квантового регистра есть множество состояний вида

$$|x\rangle = |x_{n-1}, x_{n-2}, \dots, x_1, x_0\rangle, \quad \text{где } x_i = \{0, 1\}.$$

Каждому вектору вычислительного базиса можно сопоставить число $0 \leq x \leq N$ в двоичном представлении

$$x = x_{n-1}2^{n-1} + x_{n-2}2^{n-2} + \dots + x_12 + x_0.$$

Произвольное чистое состояние квантового регистра записывается в виде

$$|\psi\rangle = \sum_{x=0}^{N-1} a_x |x\rangle, \quad \text{где } \sum_x |a_x|^2 = 1.$$

Таким образом, квантовый регистр, в отличие от классического, может находиться в суперпозиционном состоянии. Поэтому если классический регистр, состоящий из n битов, может содержать лишь одно число x , то квантовый регистр из n кубитов может содержать 2^n чисел одновременно, благодаря принципу суперпозиции. Если выполнять вычисление на классическом компьютере, то для каждого числа потребуется отдельное вычисление (прогон). Наоборот, квантовый компьютер может выполнить вычисление сразу для всех чисел, записанных в квантовый регистр, за один прогон. Такая особенность его работы называется квантовым параллелизмом и является основой для резкого увеличения производительности квантового компьютера по сравнению с классическим.

Преимущество квантового компьютера по сравнению с классическим проявляется тогда, когда существует эффективное разложение унитарного преобразования U на элементарные логические элементы (эффективная квантовая

схема), число элементов в которой полиномиально (а не экспоненциально) зависит от числа кубитов.

Для выполнения квантового вычисления необходимо:

1. приготовить квантовый регистр в определенном состоянии $|\psi\rangle$;
2. осуществить унитарное преобразование $U: |\psi\rangle \rightarrow |\tilde{\psi}\rangle$;
3. выполнить измерение конечного состояния. В результате измерения происходит «коллапс» состояния квантового компьютера в некоторую бинарную последовательность значений физических величин, что и является результатом вычисления.

Данные в процессе вычислений представляют собой квантовую информацию, которая по окончании процесса преобразуется в классическую путем измерения конечного состояния квантового регистра. Выигрыш в квантовых алгоритмах достигается за счет того, что при применении одной квантовой операции большое число коэффициентов суперпозиции квантовых состояний, которые в виртуальной форме содержат классическую информацию, преобразуется одновременно. [2, 3, 7]

4.1 Квантовые алгоритмы

Квантовый алгоритм представляет собой классический алгоритм, который задает последовательность унитарных операций с указанием, над какими именно кубитами их надо совершать. Квантовый алгоритм задается либо в виде словесного описания таких команд, либо с помощью их графической записи в виде системы вентиляей.

Результат работы квантового алгоритма носит вероятностный характер. За счет небольшого увеличения количества операций в алгоритме можно сколь угодно приблизить вероятность получения правильного результата к единице.

Весь смысл применения квантового компьютера в том, что некоторые задачи он способен решить существенно быстрее, чем любой из классических. Для этого квантовый алгоритм должен по ходу вычисления генерировать и использовать запутанные квантовые состояния. Любая задача, решаемая квантовым алгоритмом, может быть решена и классическим компьютером путем прямого вычисления унитарных матриц экспоненциальной размерности, получения явного вида квантовых состояний. В частности, проблемы, неразрешимые на классических компьютерах, остаются неразрешимыми и на квантовых.

Главный тип задач, которые ускоряются квантовыми алгоритмами, являются задачи типа перебора. Их можно разделить на 2 основные группы [2, 3, 7]:

1. задачи моделирования динамики сложных систем (первоначальная идея Фейнмана),
2. математические задачи, сводящиеся к перебору вариантов:
 - 2.1. общий случай перебора: схема Гровера и ее варианты,
 - 2.2. задачи поиска скрытых периодов: схема Шора использования быстрого квантового преобразования Фурье, и ее аналоги.

Первый тип представлен алгоритмом Залки–Визнера моделирования унитарной динамики квантовых систем n частиц за почти реальное время и с линейной от n памятью. Этот алгоритм использует схему Шора квантового преобразования Фурье. Такой тип задач представляет наибольший интерес с точки зрения дальнейших приложений квантового компьютера.

Второй тип задач представлен:

- алгоритмом Гровера общей задачи перебора и его непрерывным и адиабатическим вариантами, а также алгоритмами, использующими схему Гровера: структурного поиска, алгоритмом поиска экстремума и поиска совпадающих строк в базе данных,
- алгоритмом Шора факторизации целых чисел, алгоритмом Абрамса–Ллойда выявления периода, алгоритмом Китаева определения скрытых подгрупп и др.

4.1.1 Алгоритм Гровера

Алгоритм Гровера решает задачу перебора, то есть решения уравнения $f(x) = 1$, где f – логическая функция от n переменных. Классически данная задача требует прямого перебора всех $N = 2^n$ переменных, данный алгоритм находит корень уравнения за $\pi\sqrt{N}/4$ обращений к функции f с использованием $O(n)$ кубитов. Схема алгоритма Гровера приведена на рисунке 9. [3, 5, 7]

4.1.2 Алгоритм Шора

Алгоритм Шора – квантовый алгоритм разложения числа на простые множители (факторизации), позволяющий разложить число M за время $O(\lg^3 M)$ с использованием $O(\lg M)$ кубитов. Схема алгоритма приведена на рисунке 10.

Значимость алгоритма заключается в том, что с его помощью становится возможным взлом криптографических систем с открытым ключом. [3, 6, 7, 8]

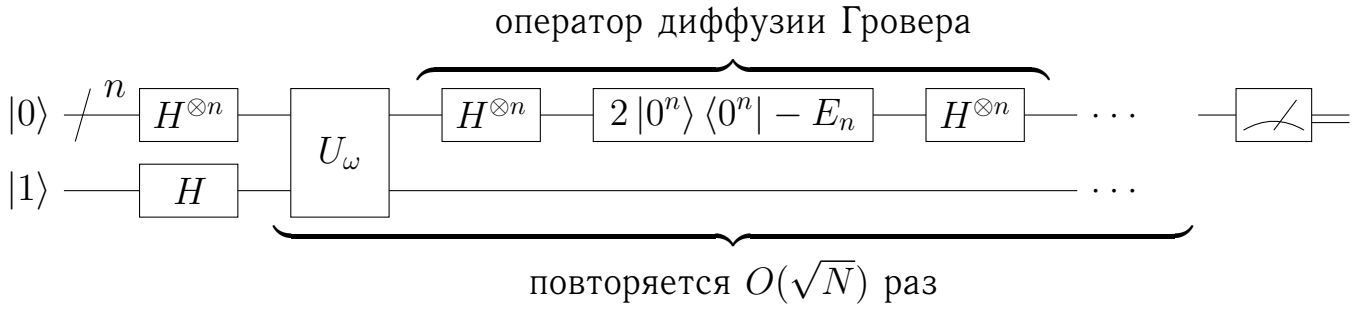


Рисунок 9 — Алгоритм Гровера

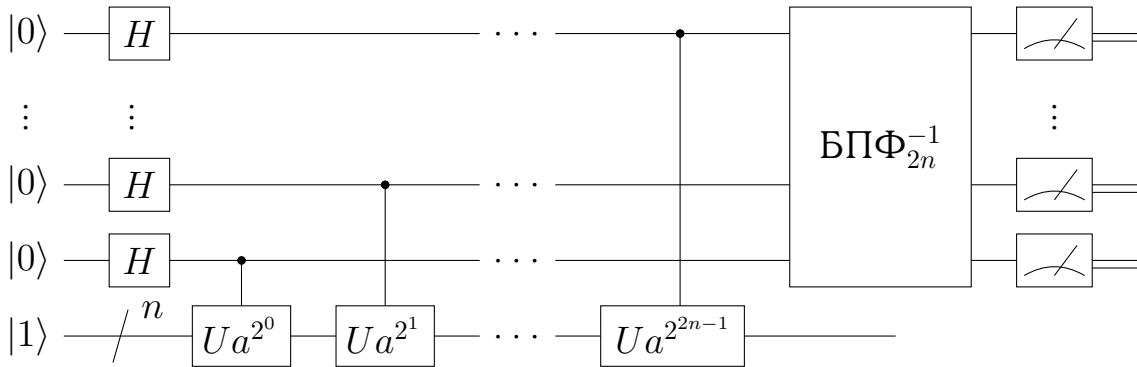


Рисунок 10 — Алгоритм Шора (БПФ – быстрое преобразование Фурье)

4.1.3 Алгоритм Дойча–Йожи

Задача Дойча–Йожи заключается в определении является ли функция двоичной переменной $f(n)$ постоянной (принимает либо значение 0, либо 1 при любых аргументах) или сбалансированной (для половины области определения принимает значение 0, для другой половины 1). При этом заранее считается известным, что функция либо является константой, либо сбалансирована.

Если на вход подать булеву функцию одной переменной, то она будет одной из четырех: $f(x) \equiv 0$, $f(x) \equiv 1$, $f(x) = x$, $f(x) = \bar{x}$. Первые две являются константными, последние две – сбалансированными. Алгоритм Дойча–Йожи выдает после работы 0 для константных и 1 для сбалансированных.

Схема алгоритма приведена на рисунке 11. [3, 4]

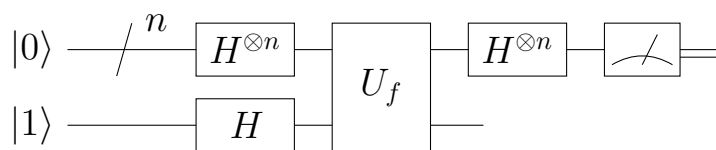


Рисунок 11 — Алгоритм Дойча–Йожи

Заключение

Построение квантового компьютера в виде реального физического прибора является фундаментальной задачей физики XXI века.

На сегодняшний день существуют ограниченные квантовые компьютеры – в пределах 512 кубит. Больших успехов добилась компания D-Wave, создавшая в 2007 году образец квантового компьютера на основе процессора из 16 кубит, в 2011 – из 128 кубит, а в 2012 – 512 кубит. Квантовый компьютер, построенный на базе последнего, назван D-Wave One. В 2013 году проводилось сравнение D-Wave One с 4-х процессорным компьютером на основе 2,4 ГГц чипов Intel с 16 Гб оперативной памяти. В задаче, подходящей под структуру процессора, D-Wave One показал выигрыш по скорости в 3600 раз, а из 33 заданных задач, требовавших «перевод» на язык, на котором работает D-Wave One, за 30 минут нашел решение для 28, тогда как компьютер на базе процессоров Intel нашел решение только для 9 задач.

Однако, такой прирост скорости зависит от алгоритма решения задачи, а прирост скорости в квантовых алгоритмах, существующих на текущий момент, появляется в некоторых, весьма специфичных задачах.

В заключение можно написать про то, что для построения полноценного квантового компьютера квантовая теория должна сделать большой скачок в области измерений и экспериментов, изменения состояний частиц и их запутывания, да и в области решения многочастичных задач в целом.

Список литературы

- [1] Чивилихин, С. А. Квантовая информатика. Учебное пособие / С. А. Чивилихин. — Санкт-Петербург: СПбГУИТМО, 2009. — 80 с.
- [2] Калачев, А. А. Квантовая информатика в задачах: учеб.-мет. пос. / А. А. Калачев. — Казань: Казан. ун-т, 2012. — 48 с.: ил.
- [3] Кронберг, Д. А. Квантовая информатика и квантовый компьютер. Учебное пособие / Д. А. Кронберг, Ю. И. Ожигов, А. Ю. Чернявский. — Режим доступа: http://sqi.cs.msu.su/store/storage/th25kzj_quantum_computer.pdf
- [4] Вялый, М. Квантовые алгоритмы: возможности и ограничения. Лекция 2: Квантовые запросы к «черному ящику» — Режим доступа: http://compsciclub.ru/sites/default/files/slides/20110204_quantum_algorithms_vyali_lecture02.pdf
- [5] Логинов О. В. Квантовый алгоритм Гровера / О. В. Логинов, А. В. Цыганов. — Режим доступа: <http://www.exponenta.ru/educat/systemat/grover/index.asp>
- [6] Shor's algorithm. — Available at: http://en.wikipedia.org/wiki/Shor's_algorithm
- [7] Ожигов, Ю. И. Квантовые вычисления. — Режим доступа: http://sqi.cs.msu.su/store/storage/g1xr51z_ozhigov.pdf
- [8] Лифшиц, Ю. Алгоритм Шора. — Режим доступа: <http://yury.name/modern/10modernnote.pdf>