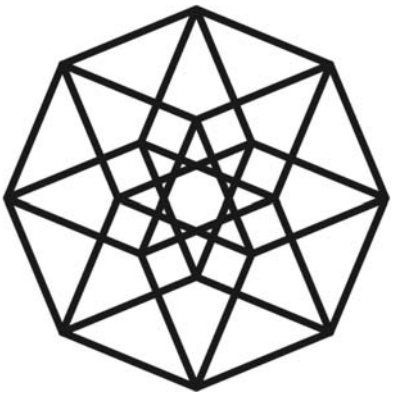
МЕЖГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛОРУССКО-РОССИЙСКИЙ УНИВЕРСИТЕТ»

Кафедра «Высшая математика»

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ

Методические рекомендации к лабораторным работам для студентов направления подготовки 01.03.04 «Прикладная математика» дневной формы обучения



Могилев 2022

УДК 510.6 + 519.7
ББК 22.12 + 32.815
К32

Рекомендовано к изданию
учебно-методическим отделом
Белорусско-Российского университета

Одобрено кафедрой «Высшая математика» «29» сентября 2022 г., протокол № 1

Составители: канд. физ.-мат. наук, доц. И. У. Примак;
канд. физ.-мат. наук, доц. Л. И. Сотская;
ст. преподаватель А. Н. Бондарев

Рецензент канд. физ.-мат. наук, доц. И. И. Маковецкий

Методические рекомендации содержат необходимые для проведения лабораторных занятий вопросы и задачи по курсу «Квантовые вычисления».

Учебно-методическое издание

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ

Ответственный за выпуск	В. Г. Замураев
Корректор	И. В. Голубцова
Компьютерная верстка	Н. П. Полевничая

Подписано в печать . Формат 60×84/16. Бумага офсетная. Гарнитура Таймс.
Печать трафаретная. Усл. печ. л. . Уч.-изд. л. . Тираж 56 экз. Заказ №

Издатель и полиграфическое исполнение:
Межгосударственное образовательное учреждение высшего образования
«Белорусско-Российский университет».
Свидетельство о государственной регистрации издателя,
изготовителя, распространителя печатных изданий
№ 1/156 от 07.03.2019.
Пр-т Мира, 43, 212022, г. Могилев.

Содержание

1 Лабораторная работа № 1. Введение

Вопросы к занятию

1 Что такое вычислительная задача?

2 Как построить алгоритмы, решающие данную вычислительную задачу?

3 Каковы минимальные ресурсы, необходимые для решения данной вычислительной задачи? Сформулировать тезис Чёрча – Тьюринга.

4 Понятие машины Тьюринга. Насколько общим является понятие машины Тьюринга?

5 Можно ли считать, что способ задания алгоритмов с помощью машины Тьюринга является универсальным?

6 Возможности машин Тьюринга.

Задачи к занятию **[1–6]**

1 *Невычислимые процессы в природе*. Как можно установить, что какой-то природный процесс вычисляет функцию, не вычисляемую машиной Тьюринга?

2 *Тьюринговы номера*. Покажите, что одноленточные машины Тьюринга можно пронумеровать числами 1, 2, 3, …, соответствующую машину.

Указание. Каждое натуральное число может быть разложено единственным образом на простые множители в $p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$, где p_i – различные простые числа и $a_1, a_2, ..., a_k$ – целые неотрицательные числа.

3 *Обращение битовой строки с помощью машин Тьюринга*. Опишите машину Тьюринга, которая получает на вход двоичное число x в обратном порядке.

Указание. Использовать многоленточную машину Тьюринга и / или символы, отличные от нуля, единицы, ⊳ и пробела.

4 Опишите машину Тьюринга, которая выполняет сложение двоичных чисел x и y по модулю 2. Числа подаются на вход в таком виде: x в двоичной системе, потом один пробел, затем y в двоичной системе. Если одно число короче другого, считается, что оно дополнено нулями слева в таком количестве, чтобы записи этих чисел имели одинаковую длину.

5 *Проблема остановки без входных данных*. Покажите, что не существует алгоритма, позволяющего выяснить, остановится ли машина Тьюринга, если на ее входе будут одни пробелы.

6 *Вероятностная проблема остановки*. Пусть мы пронумеровали вероятностные машины Тьюринга аналогично тому, как были пронумерованы стандартные машины Тьюринга в задаче 2, и определили вероятностную функцию остановки $h_p(x)$ как функцию, принимающую значение 1, если номер x останавливается при подаче x на вход с вероятностью, не меньшей $1/2$, и принимающую значение 0 с вероятностью, меньшей $1/2$. Покажите, что не существует вероятностной машины Тьюринга, которая для всех x выдает

значение $h_p(x)$ с вероятностью, строго большей $1/2$.

7 Докажите, что $f(n)$ принадлежит $O(g(n))$ тогда и только тогда, когда $g(n)$ принадлежит $\Omega\big(f(n)\big)$. Выведите отсюда, что $f(n)$ принадлежит $\Theta(g(n))$ тогда и только тогда, когда $g(n)$ принадлежит $\Theta\big(f(n)\big)$.

8 Пусть $g(n)-$ многочлен степени k. Покажите, что $g(n)$ принадлежит $O\big(n^l\big)$ при всех $l \geq k$.

9 Покажите, что $\log n$ принадлежит $O\big(n^k\big)$ при всех $k > 0$.

10 $n^{\log n}$ *суперполиномиальна*. Покажите, что n^k принадлежит $O\big(n^{\log n}\big)$ для любого k, но $n^{\log n}$ никогда не принадлежит $O\big(n^k\big)$.

11 $n^{\log n}$ *субэкспоненциальна*. Покажите, что c^n принадлежит $\Omega\big(n^{\log n}\big)$ для любого $c > 1$, но $n^{\log n}$ никогда не принадлежит $\Omega\big(c^n\big)$.

2 Лабораторная работа № 2. Основные понятия квантовых вычислений

Вопросы к занятию

1 Дать определения унитарного оператора и оператора проекции.

2 Дать определения тензорного произведения векторов и тензорного определения матриц.

3 Ввести понятие квантового бита (кубита) и описать его свойства.

4 Дать определение квантового регистра.

5 Пространство состояний регистра квантовых битов в сравнении с пространством состояний регистра классических битов.

6 Определить декартово и тензорное произведения двух пространств.

7 Описать сферу Блоха.

Задачи к занятию **[1–6]**

1 Найдите операторы плотности в вычислительном базисе для следующих состояний:

а) $\left\{\left(|0\rangle, \frac{1}{2}\right), \left(|1\rangle, \frac{1}{2}\right)\right\}$;

б) $\frac{1}{2}\big(|0\rangle + |1\rangle\big)$;

в) $\left\{\left(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),\frac{1}{2}\right),\left(\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle),\frac{1}{2}\right)\right\}$.

2 Предположим, что состояния $|\uparrow_z=|0\rangle\rangle$ и $|\uparrow_x\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ смешиваются в пропорции $\frac{1}{3}:\frac{2}{3}$. Запишите вектор Блоха результирующего состояния.

3 Неопределенность состояния квантовой системы можно описывать *степенью чистоты* (purity) $P(\rho)=tr(\rho^2)$. Покажите, что $P(\rho)\le 1$, причем равенство достигается тогда и только тогда, когда оператор ρ описывает чистое состояние. Чему равна величина $P(\rho)$ для максимально смешенного состояния? В случае одного кубита выразите степень чистоты через длину вектора Блоха.

4 Покажите, что координаты вектора Блоха $\overline{r}=(x,y,z)$ равны, соответственно, средним значениям $\sigma_x,\sigma_y,\sigma_z$ в состоянии $|\psi\rangle$.

5 Понятие степени совпадения двух состояний F обобщается на случай двух смешанных состояний следующим образом:

$$F\equiv\left(Tr\sqrt{\rho_1^{1/2}\rho_2\rho_1^{1/2}}\right)^2.$$

Используя представление Блоха, покажите, что степень совпадения двух состояний с векторами Блоха $\overline{r_1}$ и $\overline{r_2}$

$$F=\frac{1}{2}\left(1+\overline{r_1}\cdot\overline{r_2}+\sqrt{(1-\overline{r_1}^2)(1-\overline{r_2}^2)}\right).$$

6 *Следовая метрика* для квантовых состояний ρ_1 и ρ_2 определяется как $D\equiv\frac{1}{2}Tr|\rho_1-\rho_2|$, где $|A|=\sqrt{A^\dagger A}$. Эта величина является мерой различия квантовых состояний. Покажите, что в случае двумерного гильбертова пространства:

а) расстояние между состояниями в следовой метрике равно половине обычного евклидового расстояния между точками, на которые указывают соответствующие векторы Блоха;

б) $D=\sqrt{Tr\left[(\rho_1-\rho_2)^2\right]}$.

Покажите, что в случае двух чистых состояний следовая метрика выражается через степень совпадения по формуле $D=\sqrt{1-F}$.

7 Кубит находится в неизвестном состоянии $|\psi_1\rangle$. Мы выдвигаем гипотезу, что он находится в состоянии $|\psi_2\rangle$, выбирая последнее случайным образом. Какова степень совпадения нашей гипотезы с истинным состоянием?

8 Проверьте унитарность матриц

$$A=\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}, \qquad B=\begin{pmatrix} \frac{1}{\sqrt{15}} & \frac{2}{\sqrt{15}} & \sqrt{\frac{2}{15}} & \frac{2\sqrt{2}}{\sqrt{15}} \\ \frac{2}{\sqrt{15}} & -\frac{1}{\sqrt{15}} & \frac{2\sqrt{2}}{\sqrt{15}} & -\sqrt{\frac{2}{15}} \\ -\sqrt{\frac{2}{15}} & -\frac{2\sqrt{2}}{\sqrt{15}} & \frac{1}{\sqrt{15}} & \frac{2}{\sqrt{15}} \\ -\frac{2\sqrt{2}}{\sqrt{15}} & \sqrt{\frac{2}{15}} & \frac{2}{\sqrt{15}} & -\frac{1}{\sqrt{15}} \end{pmatrix}.$$

9 Докажите следующие свойства гильбертова пространства:

а) $\|\psi\| \geq 0 \ \forall \psi \in \mathrm{H}^d$;

б) $\|\psi\| = 0 \Leftrightarrow \psi = 0$;

в) $\|\psi\| = \|U\psi\|$, если U унитарно;

г) $\rho(\psi,\varphi) = \rho(U\psi, U\varphi)$, если U унитарно;

д) $\rho(\psi,\varphi) = 0 \Leftrightarrow \psi = \varphi$.

10 Покажите, что если U – унитарная матрица, то $\left\langle u_i \middle| u_j \right\rangle = \delta_{i,j}$. Здесь u_i – i-я строка матрицы U, $\delta_{i,j}$ – символ Кронекера ($\delta_{i,j}=1$, если $i=j$; $\delta_{i,j}=0$, если $i \neq j$).

3 Лабораторная работа № 3. Основные постулаты квантовой механики

Вопросы к занятию

1 Сформулировать основные постулаты квантовой механики.

2 Основные математические понятия, используемые в теории квантовых вычислений.

3 Определить суперпозицию квантовых состояний и эволюцию квантовой системы.

4 Как осуществляется измерение квантовой системы?

5 Сформулировать теорему о неклонировании.

Задачи к занятию **[1–6]**

1 Проверьте, что оператор Адамара H является унитарным.

2 Докажите, что $H^2 = I$.

3 Чему равны собственные числа и собственные векторы оператора H?

4 Пусть A и B – коммутирующие эрмитовы операторы. Докажите, что

$\exp(A)\exp(B) = \exp(A+B)$.

5 Используя спектральное разложение, покажите, что для любого унитарного оператора U оператор $K \equiv -i\log(U)$ является эрмитовым, а следовательно, $U = \exp(iK)$ для некоторого эрмитова оператора K.

6 Пусть $\left[A,B\right]=0, \left\{A,B\right\}=0$, A – обратимая матрица. Покажите, что $B=0$.

7 Покажите, что $\left[A,B\right]^{\dagger} = \left[B^{\dagger}, A^{\dagger}\right]$.

8 Покажите, что $\left[A,B\right] = -\left[B,A\right]$.

9 Пусть A и B – эрмитовы операторы. Покажите, что оператор $i\left[A,B\right]$ также является эрмитовым.

4 Лабораторная работа № 4. Определение запутанных квантовых состояний, примеры. EPR-парадокс

Вопросы к занятию

1 Определить разложимое состояние двухкубитной системы.
2 Дать определения запутанных квантовых состояний.
3 Сформулировать EPR-парадокс.
4 Описать использование эффекта *entaglement* в квантовых вычислениях.

Задачи к занятию **[1–6]**

1 Найдите разложение Шмидта для следующих состояний двухкубитовой квантовой системы:

а) $\dfrac{\left|00\right\rangle + \left|11\right\rangle}{\sqrt{2}}$;

б) $\dfrac{\left|00\right\rangle + \left|01\right\rangle + \left|10\right\rangle + \left|11\right\rangle}{2}$;

в) $\dfrac{\sqrt{3}-\sqrt{2}}{2\sqrt{6}}\left|00\right\rangle + \dfrac{\sqrt{6}+1}{2\sqrt{6}}\left|01\right\rangle + \dfrac{\sqrt{3}+\sqrt{2}}{2\sqrt{6}}\left|10\right\rangle$;

г) $\dfrac{\left|00\right\rangle + \left|01\right\rangle + \left|10\right\rangle}{\sqrt{3}}$.

2 Покажите, что перепутанные трехкубитовые состояния

$$\left|GHZ\right\rangle = \frac{\left|000\right\rangle + \left|111\right\rangle}{\sqrt{2}}, \qquad \left|W\right\rangle = \frac{\left|001\right\rangle + \left|010\right\rangle + \left|100\right\rangle}{\sqrt{3}}$$

невозможно преобразовать друг в друга посредством локальных преобразований.

3 Пусть $\left|\psi\right\rangle$ – чистое состояние составной системы, содержащей подсистемы *A* и *B*. Докажите, что:

а) число Шмидта вектора $|\psi\rangle$ равно рангу приведенной матрицы плотности $\rho_A = Tr_B\left(|\psi\rangle\langle\psi|\right)$;

б) приведенные операторы плотности в базисе разложения Шмидта являются диагональными и имеют одинаковые собственные значения, равные p_i.

4 Пусть квантовая система состоит из трех подсистем *A*, *B* и *C*. Приведите пример, что существуют такие квантовые состояния системы $|\psi\rangle$, которые нельзя представить в виде

$$|\psi\rangle = \sum_i \sqrt{p_i}\,|i_A\rangle|i_B\rangle|i_C\rangle,$$

где $|i_A\rangle$, $|i_B\rangle$ и $|i_C\rangle$ – ортонормированные базисы соответствующих подсистем.

5 Покажите, что состояние Вернера

$$\rho(p) = p|\text{Bell}\rangle\langle\text{Bell}| + \frac{1-p}{4}I,$$

где $0 \le p \le 1$ и $|\text{Bell}\rangle$ – любое из состояний Белла, является, с точки зрения критерия Переса – Городецких, сепарабельным при $p \le \frac{1}{3}$ и перепутанным при $p > \frac{1}{3}$.

6 Разработайте квантовую схему, которая:

а) из состояния $|00\rangle$ получает запутанное состояние $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$;

б) из состояния $\left|\underbrace{00...0}_{l}\right\rangle$ на *l* кубитах получает запутанное состояние $\frac{|00...0\rangle + |11...1\rangle}{\sqrt{2}}$.

7 Пусть $|q_0\rangle = a|0\rangle + b|1\rangle$, $|\psi_0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$, $|\psi\rangle = |q_0\rangle \otimes |\psi_0\rangle$. Выпишите, чему равно состояние $|\psi'\rangle$? и укажите, является оно запутанным или нет. Если состояние является запутанным, то какие кубиты запутаны с какими:

а) $|\psi'\rangle = (CNOT \otimes I)|\psi\rangle$;

б) $|\psi'\rangle = (I \otimes CNOT)|\psi\rangle$.

5 Лабораторная работа № 5. Квантовая криптография

Вопросы к занятию

1 Описать классический подход (квантовая криптография с открытым ключом).

2 Описать квантовое распределение ключей (КРК). Указать протоколы.

3 Чем задается нижняя оценка гарантированной секретности канала?

4 Требования для надежного протокола КРК.

Задачи к занятию **[1–6]**

1 Рассмотрите систему с n пользователями, любая пара которых хотела бы общаться лично. Сколько требуется ключей при использовании криптографии с открытым ключом? Сколько требуется ключей при использовании криптографии с закрытым ключом?

2 Пусть a'_k – результат измерения Бобом кубита $\left|\psi_{a_k b_k}\right\rangle$ в предположении, что канал без шума и нет подслушивания. Покажите, что при $b'_k \neq b_k$ результат a'_k является случайным и полностью не коррелирован с a_k, но $a'_k = a_k$ при $b'_k = b_k$.

3 *Распределение квантового ключа*. Алиса и Боб хотят выполнить протокол распределения квантового ключа. Алиса имеет все необходимое, чтобы приготовить любое из двух состояний: $\left|u\right\rangle$ или $\left|v\right\rangle$. В подходящем базисе эти два состояния могут быть представлены как

$$\left|u\right\rangle = \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix}, \qquad \left|v\right\rangle = \begin{pmatrix} \sin\alpha \\ \cos\alpha \end{pmatrix},$$

где $0 < \alpha < \dfrac{\pi}{4}$. Алиса выбирает наугад, что послать Бобу, $\left|u\right\rangle$ или $\left|v\right\rangle$, а Боб должен выполнить измерение, чтобы определить, что она послала. Так как эти два состояния не ортогональны, Боб не может различить их с абсолютной точностью. Рассмотрите следующие ситуации и ответьте на вопросы:

а) Боб понимает, что он не может рассчитывать на то, что всякий раз он сможет идентифицировать кубит Алисы, поэтому он довольствуется процедурой, которая лишь иногда обеспечивает успех. Он выполняет ПОЗМ с тремя возможными исходами: $\neg\left|u\right\rangle$, $\neg\left|v\right\rangle$ или НЕ ЗНАЮ. Если он получает результат $\neg\left|u\right\rangle$, он уверен, что было послано $\left|v\right\rangle$, а если он получает результат $\neg\left|v\right\rangle$ он уверен, что было послано $\left|u\right\rangle$. Если получен результат НЕ ЗНАЮ, тогда его измерение неубедительно (не позволяет сделать определенного вывода). Эта ПОЗМ определяется операторами

$$\mathbf{F}_{\neg u} = A\left(\mathbf{1} - |u\rangle\langle u|\right), \qquad \mathbf{F}_{\neg v} = A\left(\mathbf{1} - |v\rangle\langle v|\right),$$

$$\mathbf{F}_{DK} = (1-2A)\mathbf{1} + A\left(|u\rangle\langle u| + |v\rangle\langle v|\right)$$

(DK – Don't Know – НЕ ЗНАЮ), где A – положительное вещественное число. Какое значение A должен выбрать Боб, чтобы минимизировать вероятность результата НЕ ЗНАЮ, и чему равна эта минимальная вероятность НЕ ЗНАЮ (при условии, что Алиса выбирает $|u\rangle$ или $|v\rangle$ с равной вероятностью)?

Указание. Если A слишком велико, то $\mathbf{F}_{DK}$ будет иметь отрицательные собственные значения, а уравнения не будут представлять ПОЗМ;

б) сформулируйте протокол распределения квантового ключа, используя исходные данные Алисы и ПОЗМ Боба;

в) Ева тоже хочет знать, что Алиса посылает Бобу. Надеясь на то, что Алиса и Боб не заметят, она перехватывает каждый посылаемый Алисой кубит, выполняя ортогональное измерение, проецирующее его на базис $\left\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right\}$. Если она получает результат $\begin{pmatrix}1\\0\end{pmatrix}$, то она пересылает Бобу $|u\rangle$, а если – $\begin{pmatrix}0\\1\end{pmatrix}$, то пересылает ему $|v\rangle$. Следовательно, всякий раз, когда ПОЗМ Боба имеет убедительный результат, Ева знает; каков он. Но вмешательство вызывает обнаруживаемые ошибки: иногда Боб получает «убедительный» результат, который на самом деле отличается от того, что посылала Алиса. Какова вероятность такой ошибки?

6 Лабораторная работа № 6. Квантовые гейты

Вопросы к занятию

1 Определение квантового гейта.
2 Привести примеры классических гейтов.
3 Провести сравнение квантовых гейтов с классическими гейтами.
4 Определение основных одно- и двухкубитных гейтов.
5 Привести пример трехкубитного гейта.
6 Привести примеры универсальных квантовых гейтов.
7 Описать эффект квантового параллелизма.
8 Определение квантовой схемы.
9 Отличия квантовых и классических схем. Квантовый параллелизм.

Задачи к занятию **[1–6]**

1 Рассмотрите гейт CNOT со вторым, контролируемым кубитом в состоянии $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$. Опишите действие этого гейта на первый, контролирующий кубит.

2 Разработайте квантовую схему, состоящую из однокубитных гейтов и гейта CNOT, воздействующий на второй кубит, которая осуществляет преобразование:

$$|00\rangle \to \frac{|01\rangle-|10\rangle}{\sqrt{2}}, \qquad |11\rangle \to \frac{|00\rangle+|11\rangle}{\sqrt{2}}.$$

Каково воздействие этой схемы на состояния $|01\rangle$ и $|10\rangle$?

3 Дана квантовая схема (рисунок 6.1).

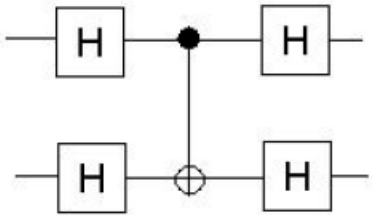


Рисунок 6.1

Найдите результат воздействия этой схемы на состояние $|01\rangle$.

4 Двухкубитная операция «*сумма*, *перенос*» $(a,b)\to(a\oplus b, a\wedge b)$ не является взаимно однозначной. Однако она может быть модифицирована во взаимно однозначную $(a,b,0)\to(a,a\oplus b,a\wedge b)$, которая может быть реализована при помощи квантовых гейтов CNOT, CCNOT изображённым на рисунке 6.2 образом.

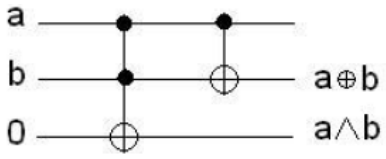


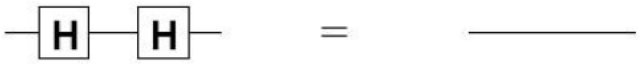
Рисунок 6.2

Нарисуйте схему для трехбитного сложения.

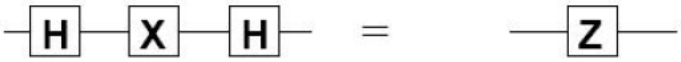
5 Покажите, что если гейт CNOT применяется к адамаровскому базису (т. е. с использованием преобразования Адамара до и после применения гейта CNOT), то контролируемый и контролирующий кубиты меняются местами. Можно привести такую аналогию – принтер вдруг становится сканером и наоборот.

6 Докажите эквивалентность следующих схем (рисунок 6.3).

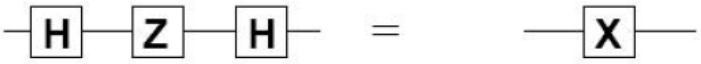
а)



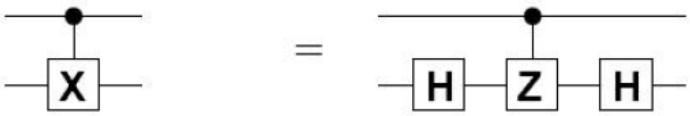
б)



в)



г)



д)

е)

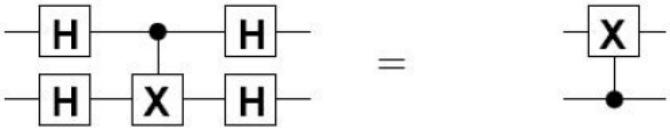


Рисунок 6.3

7 Лабораторная работа № 7. Плотное квантовое кодирование

Вопросы к занятию

1 Указать алгоритмы, использующие запутанные состояния.
2 Описать алгоритм плотного квантового кодирования.
3 Описать телепортацию.
4 Описать квантовую схему для телепортации кубита.
5 Применение элемента CHOT к двум телепортированным состояниям.

Задачи к занятию **[1–6]**

1 Докажите, что

$$|\psi\rangle|\beta_{00}\rangle = \frac{1}{2}|\beta_{00}\rangle|\psi\rangle + \frac{1}{2}|\beta_{01}\rangle\big(X|\psi\rangle\big) + \frac{1}{2}|\beta_{10}\rangle\big(Z|\psi\rangle\big) + \frac{1}{2}|\beta_{11}\rangle\big(XZ|\psi\rangle\big).$$

2 Покажите, что операция частичного транспонирования (см. критерий Переса – Городецких) не является вполне положительной.

3 Проверьте, что состояния

$$00:\ |\psi\rangle \to \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \qquad 01:\ |\psi\rangle \to \frac{|00\rangle - |11\rangle}{\sqrt{2}},$$
$$10:\ |\psi\rangle \to \frac{|10\rangle + |01\rangle}{\sqrt{2}}, \qquad 11:\ |\psi\rangle \to \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

образуют ортонормированный базис в пространстве состояний двух кубитов.

4 Пусть E – произвольный неотрицательно определенный оператор, действующий на кубит Алисы. Покажите, что $\langle\psi|E\otimes I|\psi\rangle$ принимает одинаковое значение для любого $|\psi\rangle$ из четырех состояний Белла. Предположим, что некий недоброжелатель («Ева») перехватывает кубит Алисы на пути к Бобу. Может ли Ева определить, какую из четырех возможных последовательностей битов (00, 01, 10 или 11) пыталась отправить Алиса? Если да, то как, а если нет, то почему?

5 *Телепортация с помощью непрерывных переменных*. Один полный ортонормированный базис в гильбертовом пространстве двух частиц на вещественной прямой представляет собой базис (сепарабельных) собственных состояний оператора положения $\{|q_1\rangle\otimes|q_2\rangle\}$. Другой – запутанный базис $\{|Q,P\rangle\}$, где

$$|Q,P\rangle = \frac{1}{\sqrt{2\pi}}\int dq e^{iPq}|q\rangle\otimes|q+Q\rangle;$$

они являются одновременными собственными состояниями оператора относительного положения $Q = q_2 - q_1$ и оператора полного импульса $P = p_1 + p_2$. Требуется:

а) проверьте, что

$$\langle Q',P'||Q,P\rangle = \delta(Q'-Q)\delta(P'-P);$$

б) поскольку состояния $\{|Q,P\rangle\}$ образуют базис, мы можем разложить собственные состояния положений как

$$|q_1\rangle\otimes|q_2\rangle = \int dQdP|Q,P\rangle\langle Q,P|\big(|q_1\rangle\otimes|q_2\rangle\big).$$

Вычислите коэффициенты разложения $\langle Q,P|\big(|q_1\rangle\otimes|q_2\rangle\big)$;

в) Алиса и Боб приготовили запутанное состояние $|Q,P\rangle_{AB}$ двух частиц A и B; Алиса оставила себе частицу A, а Боб – частицу B. Алиса получила неизвестный волновой пакет $|\psi\rangle_C = \int dq|q\rangle_C\langle q|_C|\psi\rangle_C$, который она намерена теле-

портировать Бобу. Составьте протокол, который они могут выполнить, чтобы осуществить телепортацию. Что должна измерить Алиса? Какую информацию она должна послать Бобу? Что должен сделать Боб, получив эту информацию, чтобы частица *B* была приготовлена в состоянии $|\psi\rangle_B$?

6 *Телепортация со смешанными состояниями*. Операциональный способ определения запутанного состояния заключается в том, что оно может быть использовано для телепортации неизвестного квантового состояния с лучшей точностью воспроизведения, чем этого можно было бы добиться с помощью одних только локальных операций и классической связи. В этом упражнении вы покажете, что существуют смешанные состояния, в этом смысле запутанные, но тем не менее не нарушающие никакого неравенства Белла. Следовательно, для смешанных состояний (в противоположность чистым состояниям) понятия «запутанный» и «нарушающий неравенство Белла» не эквивалентны. Рассмотрите «шумящую» запутанную пару с матрицей плотности

$$\rho(\lambda) = (\mathbf{1} - \lambda)|\psi^-\rangle\langle\psi^-| + \frac{\lambda}{4}\mathbf{1}.$$

Требуется:

а) найдите точность воспроизведения *F*, которой можно достичь, если состояние $\rho(\lambda)$ используется для телепортации одного кубита от Алисы к Бобу.

Указание. Необходимо вспомнить, что «случайное гадание» имеет точность воспроизведения $F = \frac{1}{2}$;

б) определите, при каких значениях λ найденная в а) точность воспроизведения лучше той, которой можно добиться, если Алиса измеряет свой кубит и посылает Бобу классическое сообщение?

Указание. Установлено, что можно достичь значения $F = \frac{2}{3}$, если Алиса измеряет свой кубит. Фактически это наилучшее возможное значение *F*, достижимое в классической связи.

8 Лабораторная работа № 8. Простейшие квантовые алгоритмы

Вопросы к занятию

1 Сравнить вероятностные и квантовые алгоритмы.

2 Описать случаи, когда моделирование на классическом компьютере более эффективно и наоборот.

3 Сформулировать задачу Дойча. Описать алгоритм Дойча и его схемную реализацию.

4 Сформулировать задачу Дойча – Джозса. Описать алгоритм Дойча – Джозса и его схемную реализацию.

5 Сформулировать задачу и алгоритм Бернштейна – Вазирани.

Задачи к занятию **[1–6]**

1 Пусть имеется некоторое квантовое устройство (черный ящик), вычисляющее функцию

$$f:\ \{0,1\}^n \to \{0,1\}.$$

Другими словами, черный ящик осуществляет следующее унитарное преобразование:

$$U_f \left|x_1,...,x_n\right\rangle \left|y\right\rangle = \left|x_1,...,x_n\right\rangle \left|y \oplus f\left(x_1,...,x_n\right)\right\rangle.$$

Такое устройство называется *квантовым оракулом*. Покажите, что преобразование, осуществляемое квантовым оракулом, является унитарным.

2 Пусть квантовый оракул вычисляет однобитовую функцию

$$f:\ \{0,1\} \to \{0,1\}.$$

Существуют четыре такие функции, которые можно разделить на два класса. Постоянные функции принимают всегда одно значение для всех значений аргумента $\left(f(0) = f(1)\right)$, а сбалансированные – равное количество значений 1 и 0 $\left(f(0) \neq f(1)\right)$. Алгоритм Дойча позволяет определить класс функции, которую вычисляет оракул, за одно обращение к последнему. Соответствующая схема выглядит следующим образом (рисунок 8.1). Требуется:

а) найдите матрицы двухкубитовых преобразований, которые совершает квантовый оракул при вычислении каждой из этих четырех функций;

б) нарисуйте квантовые схемы оракула для всех четырех случаев, используя однокубитовые элементы и элемент CNOT;

в) докажите, что $\left|0 \oplus f(x)\right\rangle - \left|1 \oplus f(x)\right\rangle = (-1)^{f(x)}\left(|0\rangle - |1\rangle\right)$;

г) убедитесь, что измерение первого кубита в вычислительном базисе на выходе схемы позволяет определить класс функции, вычисляемой оракулом.

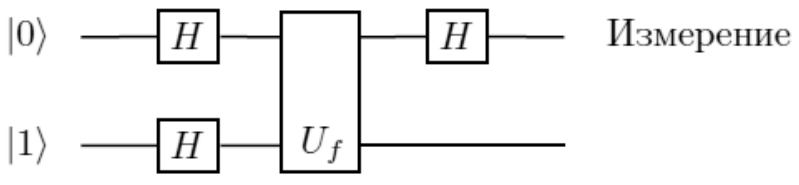


Рисунок 8.1

3 Пусть квантовый оракул вычисляет функцию

$$f:\{0,1\}^n \to \{0,1\},$$

определенную на множестве *n* битов и принимающую значения в однобитовой области. Все возможные функции можно разделить на два класса. Постоянные функции $f(x)$ принимают всегда одно значение для всех значений *x*, а сбалансированные – 1 для половины всех возможных *x* и 0 для другой половины. Алгоритм Дойча – Йожи является обобщением алгоритма, рассмотренного в предыдущей задаче, и позволяет определить класс функции за одно обращение к оракулу. Квантовая схема, позволяющая решить задачу Дойча – Йожи, имеет вид (рисунок 8.2).

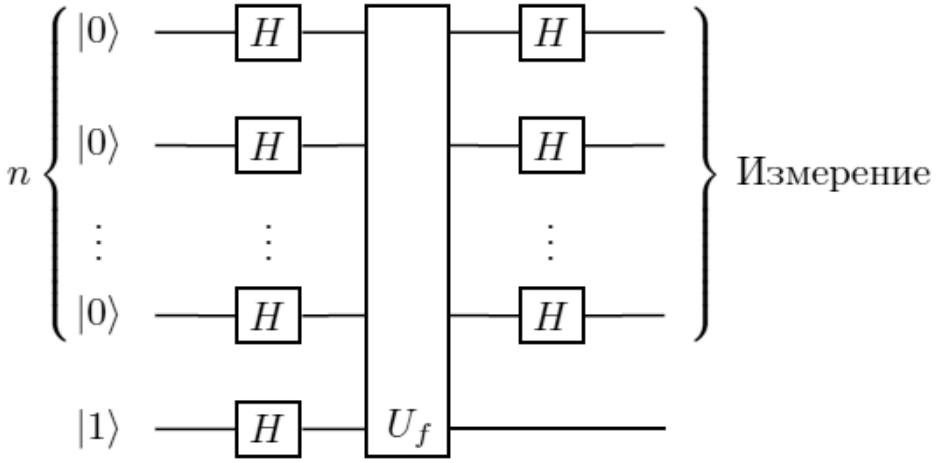


Рисунок 8.2

Требуется:
а) докажите, что

$$H^{(n)}|x\rangle = \left(\frac{|0\rangle + (-1)^{x_1}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + (-1)^{x_2}|1\rangle}{\sqrt{2}}\right)\ldots\left(\frac{|0\rangle + (-1)^{x_n}|1\rangle}{\sqrt{2}}\right) =$$

$$= \prod_{i=1}^{n}\left(\frac{1}{\sqrt{2}}\sum_{y_i=\{0,1\}}(-1)^{x_i y_i}|y_i\rangle\right) = \frac{1}{2^{\frac{n}{2}}}\sum_{y=0}^{2^n-1}(-1)^{xy}|y\rangle,$$

где $xy = (x_1y_1)\oplus(x_2y_2)\oplus\ldots\oplus(x_ny_n)$;

б) проанализируйте работу схемы н убедитесь, что измерение верхних *n* кубитов в вычислительном базисе на выходе схемы позволяет определить класс функции, вычисляемой оракулом;

в) предположим, что мы вычисляем $f(x)$ для *M* случайных значений аргумента *x* классическим образом. Если какие-то два значения $f(x)$ отличаются

друг от друга, то $f(x)$ – сбалансированная функция. Покажите, что если все значения одинаковы, то вероятность ошибки при утверждении, что $f(x)$ – постоянная, равна 2^{-M}.

9 Лабораторная работа № 9. Алгоритм Саймона

Вопросы к занятию

1 Сформулировать задачу Саймона.

2 Описать алгоритм Саймона и его схемную реализацию.

3 Таблица для проектирования оракула для алгоритма Саймона.

4 Время вычисления периода функции при классическом подходе и при использовании алгоритма Саймона.

5 Алгоритм с нулевой ошибкой. Сформулировать обобщенную задачу Саймона.

6 Приложения алгоритма Саймона.

Задачи к занятию **[1–6]**

1 Функция $f:\{0,1\}^2 \to \{0,1\}$, $f(x_1x_2)=x_0$ возвращает младший бит своего аргумента. Решите задачу Саймона для этой функции и запишите число α в десятичной системе счисления.

2 Пусть $x, y \in \{0,1\}^n$ и $s = x \oplus y$. Покажите, что

$$H^{\otimes n}\left(\frac{1}{\sqrt{2}}|x\rangle+\frac{1}{\sqrt{2}}|y\rangle\right)=\frac{1}{\sqrt{2^{n-1}}}\sum_{x\in\{s\}^{\perp}}(-1)^{x\cdot z}|z\rangle.$$

3 Мы определили $s^{\perp}$, но в более общем случае можно считать векторным подпространством в Z_2^n через S и принять определение

$$S^{\perp}=\left\{t\in Z_2^n \mid t\cdot s=0 \text{ для всех s}\in \mathrm{S}\right\}..$$

Тогда определённое выше $s^{\perp}$ будет соответствовать $S^{\perp}$, где $S\in\{0,s\}$ – двумерное векторное пространство, натянутое на s. Требуется:

а) определите $|S\rangle=\sum_{s\in S}\frac{1}{\sqrt{2^m}}|s\rangle$. Докажите, что $H^{\otimes n}|S\rangle=\sum_{w\in S^{\perp}}\frac{1}{2^{n-m}}|w\rangle$;

б) определите $y\in\{0,1\}^n$ при $|y+S\rangle=\sum_{s\in S}\frac{1}{\sqrt{2^m}}|s\rangle$. Что выражает формула $H^{\otimes n}|y+S\rangle$?

4 Предположим, что W – векторное подпространство в $\{0,1\}^n$, имеющее размерность m. Пусть $w_1, w_2, \ldots$ – последовательность элементов W, выбранных равновероятно и случайно, V_i – подпространство, натянутое на $w_1, w_2, \ldots, w_i$.

Пусть X_j есть случайная переменная, обозначающая наименьшее значение i, если V_i имеет размерность j. Тогда X_m – наименьшее значение i, если V_i имеет размерность m, следовательно, $V_i = W$.

Докажите, что ожидаемая величина X_m меньше $m+1$.

Подсказка. Определите $Y_1 = X_1$ и $Y_j = X_j - X_{j-1}$ при $j > 1$; обратите внимание, что $X_j = Y_1 + Y_2 + \ldots + Y_j$.

5 Как будет работать алгоритм Саймона, если период *y* не единственный? Можете ли вы модифицировать алгоритм на этот случай?

10 Лабораторная работа № 10. Алгоритм Гровера

Вопросы к занятию

1 Дать общую формулировку задачи, решаемой алгоритмом Гровера.

2 Сравнительная сложность решения задачи поиска квантовым и классическим алгоритмом.

3 Выполнить анализ алгоритма. Таблица для построения оракула для алгоритма Гровера. Итерация Гровера. Инверсия относительно среднего.

Задачи к занятию **[1–6]**

1 Задачу поиска в неупорядоченной базе данных можно сформулировать следующим образом. Имеется база данных, представляющая собой множество состояний вычислительного базиса квантового регистра

$$\left\{\left|x_0\right\rangle, \left|x_1\right\rangle, \ldots, \left|x_n\right\rangle\right\}, \qquad N = 2^n,$$

где n – число кубитов. Квантовый оракул вычисляет функцию

$$f_\omega(x) = \begin{cases} 0, & x \neq \omega, \\ 1, & x = \omega. \end{cases}$$

В этом случае говорят, что один из элементов базы данных, а именно $\left|\omega\right\rangle$, маркирован. Задача состоит в том, чтобы найти элемент (т. е. определить, какую из N возможных функций вида $f_\omega(x)$ вычисляет оракул), как можно меньше обращаясь к оракулу.

Алгоритм Гровера позволяет найти маркированный элемент за число ша-

гов порядка $\sqrt{N}$. В случае $N=4$ достаточно одного обращения к оракулу. Соответствующая квантовая схема имеет вид, представленный на рисунке 10.1.

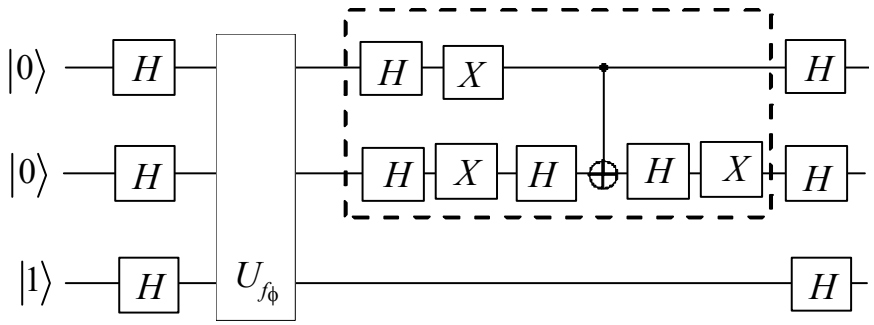


Рисунок 10.1

Здесь верхние два кубита образуют квантовый регистр, в пространстве состояний которого осуществляется поиск, а нижний кубит нужен для вычисления функции $f_\omega(x)$. Требуется:

а) нарисуйте квантовые схемы оракула для всех возможных случаев $\omega = 0, 1, 2, 3$;

б) убедитесь, что элементы, заключенные в пунктирную рамку, выполняют операцию условного фазового сдвига $2|00\rangle\langle 00| - I$ (с точностью до общего фазового множителя);

в) проверьте, что измерение над двумя верхними кубитами даёт результат ω;

г) покажите, что классический алгоритм поиска (перебор) в базе данных из четырёх элементов требует в среднем $2{,}25$ обращений к оракулу.

2 Покажите, что вероятность совершения ошибки при выполнении алгоритма Гровера порядка $1/N$, где N – число элементов в неупорядоченной базе данных.

3 Дано $|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$. Покажите, что оператор $HU_{0^\perp}H$ можно записать как $\left(2|\psi\rangle|\psi\rangle - I\right)$.

4 Докажите, что сумма амплитуд любого n-кубитового состояния ϕ, ортогонального $H|00...0\rangle$, равна 0.

5 Докажите, что $U_{\phi^\perp}$ «выполняет инверсию относительно среднего». Чтобы конкретизировать задание, возьмите суперпозицию вида

$$|\phi\rangle = \sum_x \alpha_x |x\rangle,$$

где $\mu = \frac{1}{\sqrt{N}}\sum_x \alpha_x$ – среднее значение амплитуды. Покажите, что

$$U_{\phi^\perp}|\phi\rangle = \sum_x (\mu - \alpha_x)|x\rangle.$$

6 Дана $f:\{0,1,...,N\}\to\{0,1\}$ при предположении, что $f(0)\equiv 0$. Покажите способ однократного применения оракула вида $|x\rangle\to(-1)^{f(x)}|x\rangle$ для реализации оракула вида $|x\rangle|b\rangle\to|x\rangle|b\oplus f(x)\rangle$.

7 Мы решаем задачу коммивояжера на графе с 10 узлами при помощи алгоритма Гровера. Сколько итераций Гровера нам потребуется сделать?

11 Лабораторная работа № 11. Квантовое преобразование Фурье

Вопросы к занятию

1 Определить квантовое преобразование Фурье. Сравнить квантовое и классическое преобразования Фурье.

2 Сложность квантового преобразования Фурье. Привести эффективную схему, вычисляющую квантовое преобразование Фурье.

3 Описать трехкубитовое преобразование Фурье.

4 Приложение преобразования Фурье (определение собственного числа).

Задачи к занятию **[1–6]**

1 Квантовое преобразование Фурье есть унитарное преобразование, действие которого в вычислительном базисе задается соотношением

$$U_{\text{КПФ}}:|x\rangle\to\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}e^{\left(\frac{2\pi i}{N}\right)xy}|y\rangle,$$

где $N=2^n$ – размерность гильбертова пространства состояний квантового регистра, состоящего из n кубитов, $|x\rangle$, $|y\rangle$ – векторы вычислительного базиса. Требуется:

а) запишите в явном виде матрицу оператора $U_{\text{КПФ}}$;

б) докажите, что матрица $U_{\text{КПФ}}$ является унитарной;

в) чему равны собственные значения оператора $U_{\text{КПФ}}$?

2 Квантовая схема, реализующая квантовое преобразование Фурье на трех кубитах, имеет вид, представленный на рисунке 11.1.

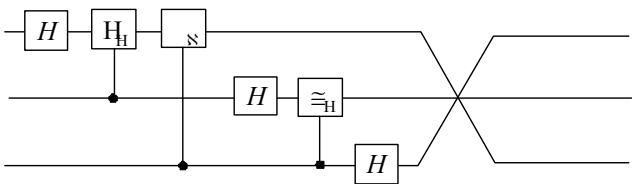


Рисунок 11.1

Здесь $\delta_k = \frac{2}{\pi^k}$. Требуется:

а) разложите элемент $CP(\delta_k)$ в композицию однокубитовых и CNOT-элементов;

б) постройте квантовую схему, реализующую обратное квантовое преобразование Фурье.

3 Постройте квантовую схему, вычисляющую квантовое преобразование Фурье

$$|j\rangle \to \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} e^{2\pi i jk/p} |k\rangle,$$

где p – простое число.

4 *Измеряемое квантовое преобразование Фурье*. Предположим, что квантовое преобразование Фурье производится на последнем шаге квантового вычисления, а затем выполняется измерение в вычислительном базисе. Покажите, что эту комбинацию квантового преобразования Фурье и измерения можно реализовать с помощью схемы, состоящей только из однокубитовых элементов и измерителей, с классическими условными операциями.

5 *Сложение с помощью преобразования Фурье*. Пусть требуется построить квантовую схему, выполняющую вычисление $|x\rangle \to |x + y \bmod 2^n\rangle$, где y – фиксированная константа и $0 \le x < 2^n$. Покажите, что при $y = 1$ это можно эффективно сделать следующим образом: провести квантовое преобразование Фурье, применить однокубитовые сдвиги фазы, а затем выполнить обратное преобразование Фурье. Для каких ещё значений y такой метод эффективен? Сколько при этом требуется операций?

6 Вычислите в явном виде преобразование Фурье n-кубитового состояния $|00...0\rangle$.

12 Лабораторная работа № 12. Задача факторизации числа

Вопросы к занятию

1 Определить квантовое преобразование Фурье. Сравнить квантовое и классическое преобразования Фурье.

2 Сложность квантового преобразования Фурье. Привести эффективную схему, вычисляющую квантовое преобразование Фурье.

3 Описать трехкубитовое преобразование Фурье.

4 Приложение преобразования Фурье (определение собственного числа).

Задачи к занятию **[1–6]**

1 Пусть $N = m^n$ для некоторых целых $m > 1$ и $n > 1$. Приведите способ нахождения нетривиального разложения N за время, полиномиальное по $\log(N)$.

2 Пусть число N записывается L битами. Цель этого упражнения – найти эффективный классический алгоритм, выясняющий, верно ли, что $N = a^b$ для некоторых целых чисел $a \geq 1$ и $b \geq 2$. Это можно следующим образом:

а) покажите, что $b \leq L$ (если b существует);

б) покажите, что не более чем за $O\left(L^2\right)$ операций можно вычислить $y = \log_2 N$, $x = y / b$ (где $b \leq L$) и найти два целых числа u_1 и u_2, ближайших к 2^x;

в) покажите, что не более чем за $O\left(L^2\right)$ операций можно вычислить u_1^b и u_2^b (пользуясь возведением в квадрат) и проверить, не равно ли одно из этих чисел числу N;

г) объединяя два предыдущих результата, покажите, что за $O\left(L^3\right)$ операций можно выяснить, верно ли, что $N = a^b$ для целых a и b.

3 Покажите, что $N = 15$ – наименьшее число, для которого при разложении на множители по описанному алгоритму требуется нахождение порядка (т. е. наименьшее составное число, не являющееся ни чётным, ни степенью меньшего числа).

4 *Разложение числа 91*. Пусть мы хотим разложить на множители число $N = 91$. Убедитесь, что на шагах 1 и 2 алгоритм не останавливается. На шаге 3 предположим, что мы выбрали $x = 4$ (это число взаимно просто с 91). Вычислите r – порядок x по модулю N и покажите, что $x^{r/2} (\mathrm{mod} 91) = 64 \neq -1 ((\mathrm{mod} 9) 1)$, так что алгоритм успешно завершается и выдаёт $\mathrm{НОД}(64 - 1, 19) = 7$.

5 Запустив алгоритм Шора при $n = 8$, $N = 2^8 = 256$, мы измерили значение $y = 165$. Если нам повезло, то на отрезке

$$\left[\frac{165}{256} - \frac{1}{512}, \frac{165}{256} + \frac{1}{512}\right]$$

находится рациональное число $\frac{k}{r}$ со знаменателем $r < \sqrt{N} = 16$. Найдите это число.

13 Лабораторная работа № 13. Устойчивость квантовых вычислений

Вопросы к занятию

1 Понятие устойчивости квантовых вычислений. Основная идея устойчивого к ошибкам квантового вычисления.

2 Модель ошибок. Сформулировать общую схему исправления квантовых ошибок.

3 Описать реализацию устойчивого элемента CNOT с последующим исправлением ошибок.

4 Каскадные коды. Пороговая теорема.

5 Примеры устойчивых к ошибкам квантовых логических элементов.

6 Устойчивое к ошибкам измерение.

Задачи к занятию **[1–6]**

1 Предположим, что кубиты передаются по квантовому каналу, который оставляет их неизменными с вероятностью $1-p$ и переворачивает с вероятностью p, т. е. с вероятностью p состояние $|\psi\rangle$ переходит в состояние $X|\psi\rangle$, где X – матрица Паули σ_x. Такой канал называется каналом с классической ошибкой. Квантовая схема, исправляющая классические ошибки, имеет вид, представленный на рисунке 13.1.

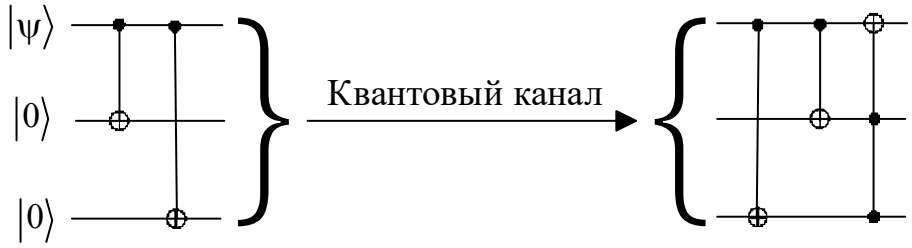


Рисунок 13.1

Требуется:

а) определите вид кодирования, выполняемого первыми двумя элементами $CNOT$, т. е. определите, в какое трёхкубитовое состояние преобразуется исходное состояние верхнего кубита;

б) покажите, что если в квантовом канале произошла ошибка с одним кубитом (в частности, с верхним), то элемент Тоффоли восстанавливает исходное состояние кубита.

2 Рассмотрим передачу кубита в состояние $|\psi\rangle$ через канал с классической ошибкой (см. условия предыдущей задачи). Без использования кода, исправляющего ошибки, состояние кубита после передачи его по каналу будет

$$\rho = (1-p)|\psi\rangle\langle\psi| + pX|\psi\rangle\langle\psi|X\,.$$

Степень совпадения исходного состояния с конечным

$$F = \langle\psi|\rho|\psi\rangle = (1-p) + p\langle\psi|X|\psi\rangle\langle\psi|X|\psi\rangle.$$

Поскольку второе слагаемое в правой части неотрицательно, минимальная степень совпадения равна $1-p$. Покажите, рассуждая аналогичным образом, что минимальная степень совпадения при использовании кода, исправляющего ошибки (см. предыдущую задачу), равна $1-3p^2+2p^3$. Проанализируйте зависимость F от вероятности ошибки p.

3 Предположим, что кубиты передаются по квантовому каналу, который оставляет их неизменными с вероятностью $1-p$ и меняет относительную фазу состояний $|0\rangle$ и $|1\rangle$ с вероятностью p, т. е. с вероятностью p состояние $|\psi\rangle$ переходит в состояние $Z|\psi\rangle$, где Z – матрица Паули σ_z. Такой канал называется каналом с фазовой ошибкой (или переворотом фазы). Трёхкубитовый квантовый код, позволяющий обнаруживать и исправлять фазовую ошибку, создаётся с помощью схемы, представленной на рисунке 13.2.

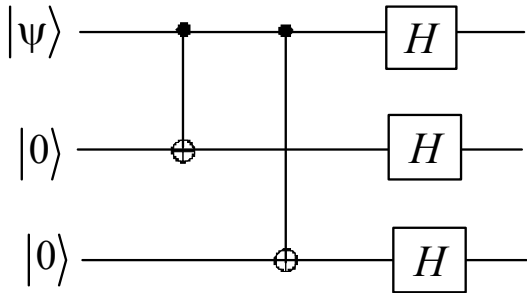


Рисунок 13.2

Требуется:

а) убедитесь, что данная схема кодирования позволяет обнаруживать и исправлять фазовые ошибки, произошедшие с одним из трёх кубитов;

б) нарисуйте квантовую схему, восстанавливающую исходное состояние верхнего кубита $|\psi\rangle$.

4 Квантовый код, исправляющий произвольную ошибку в одном кубите, получается каскадным объединением трёхкубитовых кодов, исправляющих классические и фазовые ошибки. В результате получается девятикубитовый код, называемый кодом Шора. Соответствующая кодирующая схема приведена на рисунке 13.3.

Требуется:

а) проанализируйте работу данной схемы. Выясните, каким образом с помощью данного кода можно обнаружить и исправить классическую ошибку, фазовую ошибку и их комбинацию, если ошибка произошла с одним из девяти

кубитов. Докажите, на примере возникновения ошибки в первом кубите, что код Шора позволяет исправить произвольную ошибку, произошедшую с одним кубитом;

б) нарисуйте квантовую схему, восстанавливающую исходное состояние кубита $|\psi\rangle$ после прохождения кода через квантовый канал.

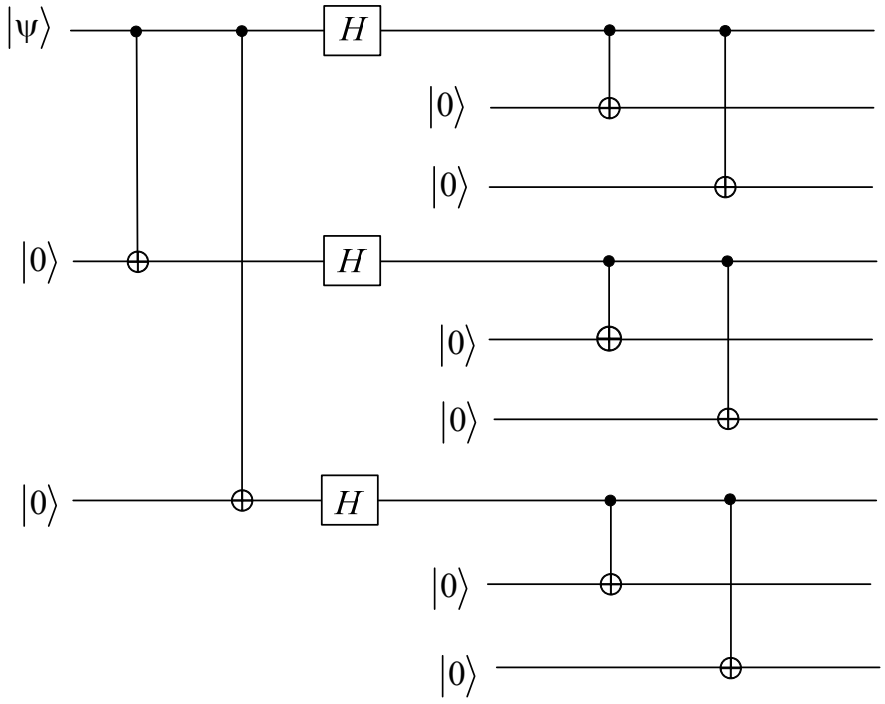


Рисунок 13.3

5 Проверьте, что схемы, представленные на рисунке 13.4, работают нормально.

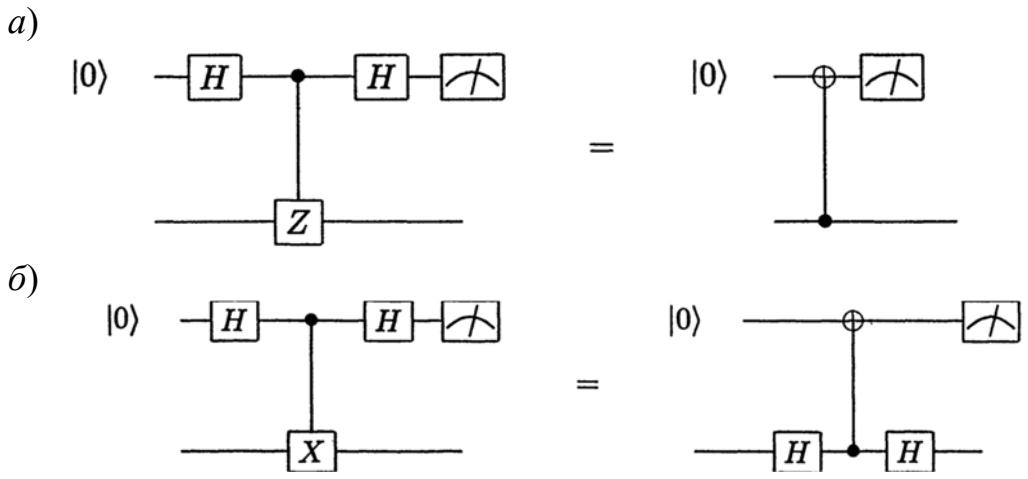


Рисунок 13.4

Докажите эквивалентность соответствующих схем.

6 *Обратное распространение ошибок*. Очевидно, что ошибка X в управ-

ляющем кубите элемента CNOT распространяется на управляемый кубит. Оказывается, что ошибка Z в управляемом кубите распространяется обратно на управляющий кубит! Покажите это, используя формализм стабилизаторов, а также тождественность квантовых схем.

7 Можно произвести обмен кубита в неизвестном состоянии $|\psi\rangle$ с кубитом, приготовленным в состоянии $|0\rangle$ с помощью двух элементов CNOT, используя схему на рисунке 13.5.

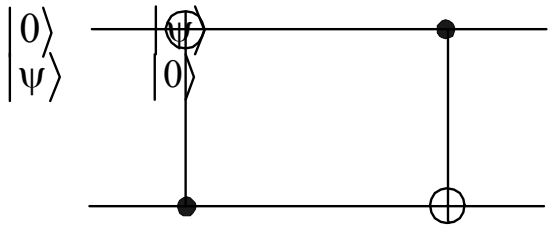


Рисунок 13.5

Покажите, что приведенные далее две схемы (рисунок 13.6) с одним элементом CNOT, измерением и классически управляемым однокубитовым элементом выполняют ту же задачу.

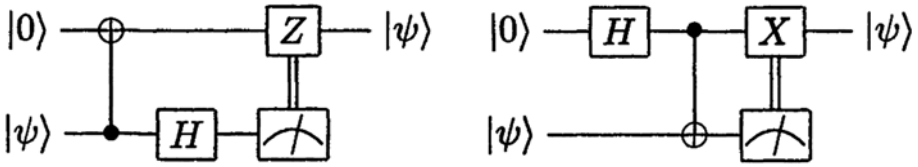


Рисунок 13.6

8 Постройте устойчивый к ошибкам элемент Тоффоли.

9 Покажите, что приведенные далее схемы (рисунок 13.7) эквивалентны.

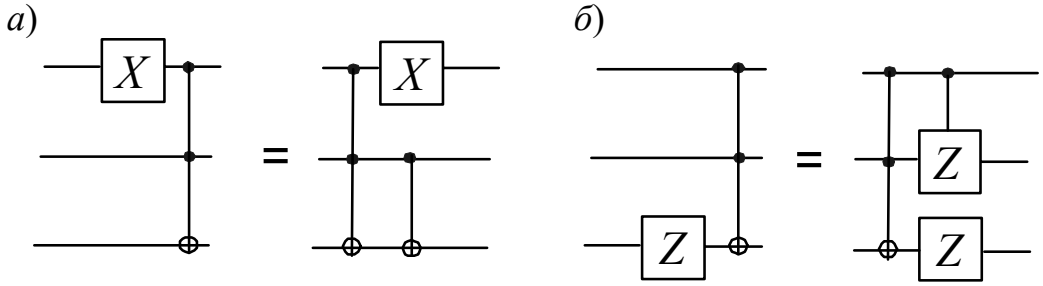


Рисунок 13.7

10 Постройте устойчивую к ошибкам квантовую схему для приготовления состояния $|0\rangle$, закодированного пятикубитовым кодом.

Список литературы

1 **Калачев, А. А.** Квантовая информатика в задачах: учебно-методическое пособие / А. А. Калачев. – Казань: Казан. ун-т, 2012. – 48 с.

2 **Гайнутдинова, А. Ф.** Сборник задач и упражнений по курсу «Основы квантовых вычислений» / А. Ф. Гайнутдинова. – Казань: Казан. ун-т, 2014. – 28 с.

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

4 **Кайе, Ф.** Введение в квантовые вычисления / Ф. Кайе, Р. Лафламм, М. Моска. – Москва: Ин-т компьютерных исследований, 2009. – 360 с.

5 **Прескилл, Дж.** Квантовая информация и квантовые вычисления: в 2 томах / Дж. Прескилл. – Москва; Ижевск : Регулярная и хаотическая динамика; Ин-т компьютерных исследований, 2008. – Т. 1. – 464 с.

6 **Сысоев, С. С.** Введение в квантовые вычисления. Квантовые алгоритмы: учебное пособие / С. С. Сысоев. – Санкт-Петербур: С.-Петерб. ун-т, 2019. – 144 с.