Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«КАЗАНСКИЙ (ПРИВОЛЖСКИЙ) ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ МАТЕМАТИКИ И МЕХАНИКИ ИМ. Н.И. ЛОБАЧЕВСКОГО
КАФЕДРА МАТЕМАТИЧЕСКОГО АНАЛИЗА

Направление: 01.03.01 - Математика
Профиль: общий

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

«Вычислительная сложность элементов квантовых алгоритмов»

Студентка 4 курса

Группы 05-502

"__"_____2019 г. _____Теплякова А.В.

Научный руководитель

Кандидат физ. - мат. наук

"__"_____2019 г. _____Новиков А.А.

Заведующий кафедрой

Доктор физ. - мат. наук, профессор

"__"_____2019 г. _____Насыров С.Р.

Казань - 2019

Содержание

1 Введение.

В своей дипломной работе я рассматриваю разложение квантового алгоритма на "базовые"составляющие. При разбиении на "базовые"элементы достаточно воздействовать на каждый кубит по отдельности или использовать связку двух, что более просто осуществить, чем воздействовать на все кубиты одновременно.

Поэтому в своей работе я рассматриваю алгоритм Гровера, так как это один из квантовых алгоритмов, обладающий свойством квантового ускорения. Алгоритм Гровера-квантовый алгоритм решения задачи перебора,то есть нахождения решения уравнения $f(x) = 1$, где f есть булева функция n переменных. Предполагается, что функция f задана в виде чёрного ящика, или оракула, то есть в ходе решения мы можем только задавать оракулу вопрос типа:«чему равна f на данном x»,и после получения ответа использовать его в дальнейших вычислениях. То есть задача решения уравнения $f(x) = 1$ является общей формой задачи перебора; здесь требуется отыскать «пароль к устройству f», что классически требует прямого перебора всех $N = 2^n$ вариантов.

2 Теоретические сведения.

2.1 Связка кубитов. Операторы X,Y,Z и CNOT

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, 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 $|1\rangle$, полагая, что эти состояния соответствуют значениям 0 и 1 классического бита. Базис, образованный этими состояниями, называется вычислительным базисом. Тогда произвольное чистое состояние кубита можно записать в виде

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

где α и β - комплексные числа, удовлетворяющие условию нормировки

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2}$$

Мы можем измерить бит, чтобы определить, находится ли он в состоянии 0 или 1. Обычные компьютеры делают это постоянно при работе с памятью. Но мы не можем измерить кубит, чтобы определить его квантовое состояние, т.е значения α и β. Из квантовой механики следует,что можно получить лишь гораздо более ограниченную информацию о квантовом состоянии. При измерении кубита мы получаем либо результат 0 с вероятностью $|\alpha|^2$, либо результат 1 с вероятностью $|\beta|^2$. Разумеется $|\alpha|^2+|\beta|^2 = 1$, поскольку сумма вероятностей должна быть равна 1. Например кубит может находиться в состоянии

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{3}$$

Измерение которого в половине случаев дает 0, а в другой половине результат 1.

Несмотря на некоторую абстрактность существование и свойства кубитов подтверждены многочисленными экспериментами . Наиболее простая для понимания модель атома в которой электрон может существовать либо в основном ($|0\rangle$), либо в возбужденном ($|1\rangle$) состояниях.
Облучая атом светом в подходящей энергией в течении некоторого времени, можно перевести электрон из состояния $|0\rangle$ в состояние $|1\rangle$ и наоборот. Но более интересно то,что сокращая время облучения можно оставить электрон, первоначально находившийся в состоянии $|0\rangle$, на полпути между $|0\rangle$ и $|1\rangle$ в состоянии (3).

Унитарная матрица — квадратная матрица с комплексными элементами, результат умножения которой на эрмитовосопряжённую равен единичной матрице $U^\dagger U = UU^\dagger = I$. Другими словами, матрица унитарна тогда и только тогда, когда существует обратная к ней матрица, удовлетворяющая условию $U^{-1} = U^\dagger$. Для матрицы комплексного переменного сопряженная матрица имеет вид $U^\dagger = \overline{U^T} = U^*$.

Кубит - это вектор $|\psi\rangle = \alpha|0\rangle+\beta|1\rangle$, параметризованный двумя комплексными числами,удовлетворяющий условию $|\alpha|^2+|\beta|^2 = 1$. Операции над кубитами

должны сохранять эту нормализацию и тем самым описываются унитарными матрицами 2×2, из которых одними из наиболее полезных являются матрицы Паули:

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}; Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{4}$$

Путем взятия экспоненты из матриц Паули получают три важных класса унитарных матриц - операторы поворота относительно осей $\hat{x}, \hat{y}, \hat{z}$, задаваемые следующими формулами:

$$R_x(\theta) \equiv e^{-i\theta X/2} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}, \tag{5}$$

$$R_y(\theta) \equiv e^{-i\theta Y/2} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} Y = \begin{bmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}, \tag{6}$$

$$R_z(\theta) \equiv e^{-i\theta Z/2} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{-i\theta/2} \end{bmatrix}. \tag{7}$$

Эти соотношения можно легко проверить показав сначала что для $x \in \mathbb{R}$ и матрицы $A^2 = I$, выполняется:

$$exp(iAx) = \cos(x) I + i \sin(x) A \tag{8}$$

Разложив функции $e^{iAx}, \cos x, \sin x$ в ряд Тейлора и использовав, что $A^2 = I$, замечаем что равенство верно.

$$e^{iAx} = I + iAx + \frac{(iAx)^2}{2!} + \frac{(iAx)^3}{3!} + ... + ...,$$

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - ...,$$

$$\cos x = I - \frac{x^2}{2!} + \frac{x^4}{4!} - ....$$

Проверим с помощью этого равенства утверждение (5):

$$exp(-i\theta X/2) = \cos(-\frac{\theta}{2}) I + i \sin(-\frac{\theta}{2}) X = \cos(\frac{\theta}{2}) I - i \sin(\frac{\theta}{2}) X.$$

Утверждения (2.6),(2.7) проверяются аналогично. Покажем теперь,что $XYX = -Y$,ивыведемотсюдауравнение $XR_y(\theta)X = R_y(-\theta)$. Запишем в матричном виде:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} = -Y.$$

Используя это уравнение получаем:

$$X(\cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y)X = \cos\frac{\theta}{2}XIX - i\sin\frac{\theta}{2}XYX = \begin{bmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} = R_y(-\theta).$$

Аналогично выводятся уравнения:

$$YZY = -Z \Rightarrow YR_z(\theta)Y = R_z(-\theta)$$

$$ZXZ = -X \Rightarrow ZR_x(\theta)Z = R_x(-\theta)$$

Простейшая и типичная условная операция-"управляемое NOT". Этот элемент мы будем обозначать как CNOT,есть квантовый элемент с двумя входными кубитами, называемые соответственно управляющим и управляемым. В терминах вычислительного базиса действие элемента

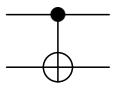


Рис.2:Условное обозначение элемента CNOT.Верхний отрезок изображает управляющий кубит, нижний управляемый.

CNOT задается формулой $|c\rangle|t\rangle \rightarrow |c\rangle|t \oplus c\rangle$; иными словами, если управляющий кубит установлен в единицу, то значение управляемого кубита меняется на противоположное,в противном случае управляемый кубит не изменяется.Таким образом,в вычислительном базисе $|$*управляющий,управляемый*$\rangle$ матричное представление элемента CNOT имеет вид

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{9}$$

Более общим образом, предположим, что U-произвольная унитарная операция на одном кубите. Тогда управляемое U-это операция на двух кубитах,попрежнему с управляющим и управляемым кубитами.Если управляющий кубит установлен в единицу, то к управляемому кубиту применяется операция U, в противном случае управляемый кубит не меняется; иными словами, $|c\rangle|t\rangle \to |c\rangle U^c|t\rangle$. Графическое изображение элемента "управляемое U"показано на рис.3

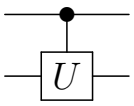


Рис. 3: Операция "управляемое U". Верхний отрезок изображает управляющий кубит, нижний управляемый.

2.2 Схема Гровера.

Будем считать, что имеется квантовый оракул - черный ящик, с внутренним устройством (которое сейчас нас не интересует), - он может распознавать решения задачи поиска. Сигнал распознавания подается с помощью кубита оракула.Точнее говоря,оракул представляет собой унитарный оператор O, определенный действием на вычислительный базис следующим образом:

$$|x\rangle|q\rangle \to |x\rangle|q \oplus f(x)\rangle \tag{10}$$

где $|x\rangle$ - индексный регистр, символ " $\oplus$ " обозначает сложение по модулю 2, а кубит оракула $|q\rangle$ меняет значение, если $f(x) = 1$, и сохраняет его в противном случае. Можно проверить, является ли x решением нашей задачи поиска, приготовив состояние $|x\rangle|0\rangle$, подействовав на него оракулом и проверив, перешел ли кубит оракула в состояние $|1\rangle$. Схема действия алгоритма поиска показана на рис.4. Алгоритм надлежащим образом использует одиночный n-кубитовый регистр. Детали внутреннего устройства оракула, включая потребность в дополнительных рабочих кубитах, не является важным для описания самого алгоритма. Цель алгоритма-найти решение задачи поиска с минимально

возможным числом обращений к оракулу.

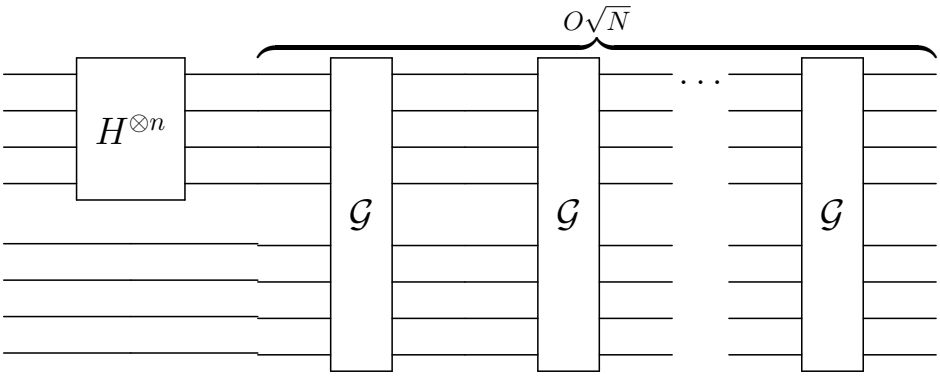


Рис. 4: Схема квантового алгоритма поиска. Оракул может использовать рабочие кубиты для своих целей, однако для анализа квантового поиска рассматривается только n-кубитовый регистр.

В начале алгоритма компьютер находится в состоянии $|0\rangle^{\otimes n}$. С помощью преобразования Адамара компьютер переводится в состояние

$$|\psi\rangle = \frac{1}{N^{1/2}} \sum_{x=0}^{N-1} |x\rangle \tag{11}$$

Дальше в квантовом алгоритме поиска последовательно применяется квантовая подпрограмма,называется итерацией(илиоператором) Гровера(будем обозначать ее буквой "G"). Итерация Гровера, квантовая схема которой изображена на рис.5, может быть разбита на четыре шага:

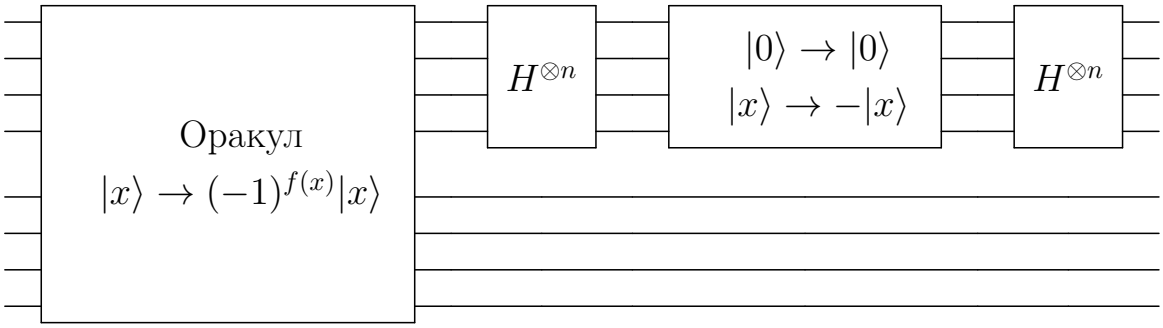
1. применение оракула O,

2. применение преобразования Адамара $H^{\otimes n}$,

3. применение к регистру условного сдвига фазы - каждое состояние вычислительного базиса, за исключением $|0\rangle$, приобретает фазовый сдвиг -1:

$$|x\rangle \to -(-1)^{\delta_x 0}|x\rangle \tag{12}$$

4. применение преобразования Адамара $H^{\otimes n}$.



Каждая операция в итерации Гровера может быть эффективно реализована на квантовом компьютере. Шаги 2 и 4 (Преобразования Адамара) требуют по $n = \log N$ операций каждый. Шаг 3 (условный фазовый сдвиг) можетбытьреализовансиспользованиемметодовдлякоторыхнеобходимо O(n) элементов. Затраты на обращение к оракулу зависят от конкретного приложения.

3 Построение разложения схемы Гровера.

3.1 Построение элемента CZ на n кубитах.

Обозначим CZ^n_{ij} оператор CZ действующий на n кубитах, где i это кубитнакоторомпроисходитуправление,а j кубитгдевыполняетсяоператор $Z, i, j \leq n$.

Для начала рассмотрим действие CZ на 2 кубитах. Покажем что этот оператор не зависит от расположения управления,то есть CZ^2_{12} равен CZ^2_{12}. 12 равен CZ2 21. И правда, запишем в матричном виде

$$CZ^2_{12} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} = CZ^2_{21}$$

Очевидно что это же свойство сохранится и при увеличении числа кубитов в связке.То есть $CZ^n_{ij} = CZ^n_{ji}$.Что существенно облегчит рассмотрение этих операторов при больших числах кубитов.Так как с учетом этого свойства всего различных операторов CZ на n кубитах будет $C^k_n = \frac{n!}{k!(n-k)!}$.Теперь рассмотрим

операторы CZ на 3 кубитах.

$$CZ_{12}^3 = \begin{bmatrix} E & 0 & 0 & 0 \\ 0 & E & 0 & 0 \\ 0 & 0 & E & 0 \\ 0 & 0 & 0 & -E \end{bmatrix} CZ_{13}^3 = \begin{bmatrix} E & 0 & 0 & 0 \\ 0 & E & 0 & 0 \\ 0 & 0 & Z & 0 \\ 0 & 0 & 0 & Z \end{bmatrix} CZ_{23}^3 = \begin{bmatrix} E & 0 & 0 & 0 \\ 0 & Z & 0 & 0 \\ 0 & 0 & E & 0 \\ 0 & 0 & 0 & Z \end{bmatrix}$$

Заметим то, что если представить Z_{12}^2 как $\begin{bmatrix} E & 0 \\ 0 & Z \end{bmatrix}$,

то Z_{12}^3 получается как бы "расщеплением"E на $\begin{bmatrix} E & 0 \\ 0 & E \end{bmatrix}$ и Z на $\begin{bmatrix} E & 0 \\ 0 & -E \end{bmatrix}$,

а Z_{12}^3 получается как бы "удвоением"E в $\begin{bmatrix} E & 0 \\ 0 & E \end{bmatrix}$ и Z в $\begin{bmatrix} Z & 0 \\ 0 & Z \end{bmatrix}$.

Лемма 1

$$D = \begin{bmatrix} D_1 & 0 \\ 0 & D_2 \end{bmatrix}, \textit{ где } D_1, D_2 \textit{ содержат 1, -1, 0.}$$

$|\psi\rangle$ *произвольный вектор, то при приписывании к нему одного кубита сверху получается*

$(E \otimes D)(|0\rangle|\psi\rangle) = |0\rangle D|\psi\rangle$

$(E \otimes D)(|1\rangle|\psi\rangle) = |1\rangle D|\psi\rangle$

А при приписывании одного кубита снизу, соответственно

$(D \otimes E)(|0\rangle|\psi\rangle) = D|\psi\rangle|0\rangle$

$(D \otimes E)(|1\rangle|\psi\rangle) = D|\psi\rangle|1\rangle$

Следствие 1 *Если приписываем канал сверху, то происходит "раздвоение" матрицы оператора. То есть* $E \otimes D$

$$D = \begin{bmatrix} D_1 & 0 \\ 0 & D_2 \end{bmatrix} \Rightarrow \begin{bmatrix} D_1 & 0 & 0 & 0 \\ 0 & D_2 & 0 & 0 \\ 0 & 0 & D_1 & 0 \\ 0 & 0 & 0 & D_2 \end{bmatrix}$$

Следствие 2 *Если приписываем канал снизу,то происходит замена всех 1 на*

E, всех -1 на E. То есть $D \otimes E$

$$D = \begin{bmatrix} D_1 & 0 \\ 0 & D_2 \end{bmatrix} \Rightarrow \begin{bmatrix} \pm E & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \pm E \end{bmatrix}$$

Любую матрицу оператора CZ можно представить как (рис.6). Где содержится $3 * 2^{n_1+n_2+m}$ единиц и $2^{n_1+n_2+m}$ минус единиц. Покажем, что количество 1 и -1 при $n_1 + n_2 + m = n_1^{'} + n_2^{'} + m^{'}$

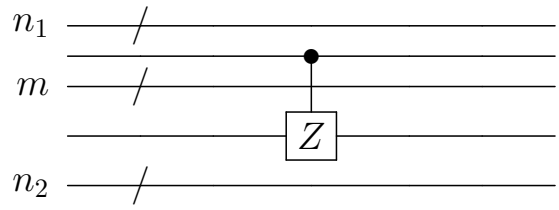


Рис. 6: Общий вид оператора CZ.

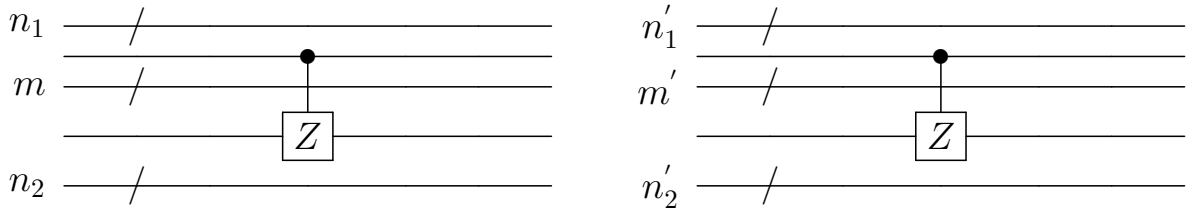


Рис. 7: Представление двух различных операторов CZ на одном наборе кубитов.

Первый оператор содержит $3 * 2^{n_1+n_2+m}$ единиц и $2^{n_1+n_2+m}$ минус единиц, а второй $3 * 2^{n_1^{'}+n_2^{'}+m^{'}}$ единиц и $2^{n_1^{'}+n_2^{'}+m^{'}}$ минус единиц. То есть для любой оператор CZ на n кубитах имеет одинаковое количество единиц и минус единиц. Заметим также, что элемент CZ_{1n}^n всегда будет выглядеть как

$$\begin{bmatrix} E & 0 & 0 & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 & 0 & 0 \\ 0 & 0 & E & 0 & 0 & 0 \\ 0 & 0 & 0 & Z & 0 & 0 \\ 0 & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 0 & Z \end{bmatrix}$$

Исходя из этого мы можем построить любой элемент CZ_{ik}^n, где $i, k \leq n, i \neq k$, путем построения $CZ_{1,(i-k)+1}^{(i-k)+1}$, а затем последовательного приписывания $n-((i-$

$k) + 1)$ каналов.

Составим таблицу умножения для оператора CZ на трех кубитах

	CZ^3_{12}	CZ^3_{13}	CZ^3_{23}
CZ^3_{12}	E	$\begin{bmatrix} E & 0 & 0 & 0 \\ 0 & E & 0 & 0 \\ 0 & 0 & Z & 0 \\ 0 & 0 & 0 & -Z \end{bmatrix}$	$\begin{bmatrix} E & 0 & 0 & 0 \\ 0 & Z & 0 & 0 \\ 0 & 0 & E & 0 \\ 0 & 0 & 0 & -Z \end{bmatrix}$
CZ^3_{13}	$\begin{bmatrix} E & 0 & 0 & 0 \\ 0 & E & 0 & 0 \\ 0 & 0 & Z & 0 \\ 0 & 0 & 0 & Z \end{bmatrix}$	E	$\begin{bmatrix} E & 0 & 0 & 0 \\ 0 & Z & 0 & 0 \\ 0 & 0 & Z & 0 \\ 0 & 0 & 0 & E \end{bmatrix}$
CZ^3_{23}	$\begin{bmatrix} E & 0 & 0 & 0 \\ 0 & Z & 0 & 0 \\ 0 & 0 & E & 0 \\ 0 & 0 & 0 & -Z \end{bmatrix}$	$\begin{bmatrix} E & 0 & 0 & 0 \\ 0 & Z & 0 & 0 \\ 0 & 0 & Z & 0 \\ 0 & 0 & 0 & E \end{bmatrix}$	E

Теорема 1 $[E, Z]$ *не содержит* CZ.

Для начала введем обозначение. Т.к рассматриваемые операторы имеют диагональный вид и состоят из 1,-1. То есть представимы в виде $diag(a_1, a_2, ..., a_n)$, где $a_i \in \{-1, 1\}$,будем отождествлять их с вектором вида $(\alpha_1, \alpha_2, ..., \alpha_n)$, размерности 2^k, где k-число кубитов, а $\alpha_i \in \{0, 1\}$,где 0 и 1 - степень i-го числа диагональной матрицы в представлении $a_i = (-1)^{\alpha_i}$. Умножение матриц операторов в нашем представлении будет выглядеть как сложение координат векторов по модулю два. То есть

$$(\alpha_1, \alpha_2, ..., \alpha_n)+(\gamma_1, \gamma_2, ..., \gamma_n) = ((\alpha_1+\gamma_1)\text{mod } 2, (\alpha_2+\gamma_2)\text{mod } 2, ..., (\alpha_n+\gamma_n)\text{mod } 2).$$

Вернемся к доказательству теоремы. Будем рассматривать только элементы Z, так как очевидно E ничего не поменяет. Случай для двух кубитов тривиальный,поэтому для начала рассмотрим случай для 3 кубитов. Запишем действия

операторов Z на три кубита в таблицу.

	1	2	3
$\|000\rangle$	0	0	0
$\|001\rangle$	0	0	1
$\|010\rangle$	0	1	0
$\|011\rangle$	0	1	1
$\|100\rangle$	1	0	0
$\|101\rangle$	1	0	1
$\|110\rangle$	1	1	0
$\|111\rangle$	1	1	1

Числа 1,2,3 обозначают кубит на который действует оператор Z.
Как известно оператор CZ на трех кубитах имеет 2 минус единицы. То есть в нашем представлении он должен иметь ровно две единицы. Но как следует из таблицы выше, при любом перемножении матриц операторов Z мы получим ровно четыре единицы.
Рассмотрим теперь действие операторов Z на четырех кубитах. Так же запишем их в таблицу.

	1	2	3	4
$\|0000\rangle$	0	0	0	0
$\|0001\rangle$	0	0	0	1
$\|0010\rangle$	0	0	1	0
$\|0011\rangle$	0	0	1	1
$\|0100\rangle$	0	1	0	0
$\|0101\rangle$	0	1	0	1
$\|0110\rangle$	0	1	1	0
$\|0111\rangle$	0	1	1	1

Как видно из таблицы выше, действие операторов Z на четыре кубита выражается через действие этого же оператора на 3 кубита. Очевидно так и должно было получиться, исходя из построения базисных векторов. Если мы разделим таблицу на два блока(здесь разделением служат две горизонтальные черты), увидим что в первом блоке мы получим ровно 4 единицы, исходя из предыдуще-

го примера, авовтором, несмотря на добавку столбца из 1, получим, очевидно, тоже 4 единицы. В итоге получим 8 единиц, как известно на 4 кубитах оператор CZ имеет ровно 4 единицы.
Докажем по индукции, пусть выполнено на $(n-1)$, запишем таблицу для n кубитов.

	1	2...n
$\|0\rangle\|\psi\rangle$	0	
$\vdots$	$\vdots$	Содержит ровно половину единиц.
$\|0\rangle\|\psi\rangle$	0	
$\|1\rangle\|\psi\rangle$	1	
$\vdots$	$\vdots$	Содержит ровно половину единиц.
$\|1\rangle\|\psi\rangle$	1	

В итоге получаем что при любом действии операторов Z мы получаем ровно половину единиц, тогда как оператор CZ содержит лишь четверть.

Теорема 2 $[E, Z, C^{n-1}Z]$ *не содержит* C^nZ.

Рассмотрим для начала рассмотрим оператор CCZ на трех кубитах, он имеет вид (0,0,0,0,0,0,0,1), то есть он содержит $\frac{1}{8}$ часть единиц. Оператор CZ содержит $\frac{1}{4}$ частьединиц,а Z $\frac{1}{2}$ в итоге получаем,что их перемножение не содержит CCZ. Доказательство того, что $[E, Z, C^{n-1}Z]$ не содержит C^nZ , получаем из того, что все операторы $C^{n-1}Z, C^{n-2}Z, ..., Z$ имеют четное число единиц в своем представлении, то есть при любом их перемножении мы получим четное число единиц, а оператор C^nZ нечетное.

3.2 Разложение оператора Гровера на $[E, Z, CZ, ..., C^nZ]$

Стоит отметить, что мы строим разложение без оракула и без рабочих кубитов. Существенным элементом в алгоритме квантового поиска Гровера является оператор $2|0^n\rangle\langle 0^n| - E_n$. Будем называть его оператор Гровера. Разложим его в композицию $(Z, CZ, ..., C^nZ)$, для этого рассмотрим квадратную диагональную матрицу оператора размером 2^n, где n число кубитов. В которой на первом

месте стоит 1, а на всех последующих -1.

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

Заметим, что операторы

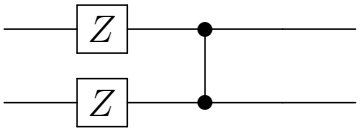


Рис. 8: Схема действия двух операторов Z и одного CZ.

имеют матрицу

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

То есть является искомым представлением оператора Гровера на двух кубитах. Этот оператор в представляется путем тензорного и обычного умножения, как $(Z \otimes Z) * CZ$. Обозначим его как H_2, то есть $H_2 \equiv (Z \otimes Z) * CZ$. Перейдем теперь к трем кубитам. Рассмотрим схему

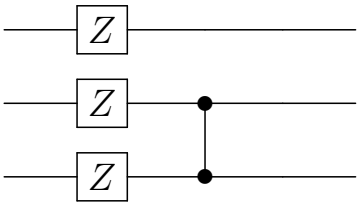


Рис. 9: Схема действия трех операторов Z и одного CZ.

Которая имеет матрицу

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{13}$$

Чтобы получить оператор Гровера, необходимо домножить матрицу на

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix} \tag{14}$$

Заметим что оператор CH_2 имеет матрицу (14), а схема операторов на Рис.9, описываемая матрицей (13) представляется в виде $Z \otimes H_2$.
Таким образом получаем, что $(Z \otimes H_2) * CH_2$ дает нам $2|000\rangle\langle 000| - E_3$, то есть оператор Гровера на 3 кубитах.

Пусть теперь $H_n = (Z \otimes H_{n-1}) * CH_{n-1}$ для $n > 2$.

$$\begin{bmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} & 0 \\ 0 & \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{bmatrix}$$

А CH_{n_1} имеет вид

$$\begin{bmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} & 0 \\ 0 & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \end{bmatrix}$$

Следовательно $H_n = (Z \otimes H_{n-1}) * CH_{n-1} = (Z \otimes ((Z \otimes H_{n-2}) * CH_{n-2}))$, то есть оператор Гровера на n кубитах.
Схематически его можно представить как.

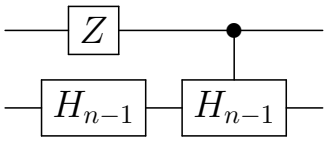


Рис. 10: Оператор Гровера в общем виде.

Схема оператора Гровера для n=3 (Рис.11).
Схема оператора Гровера для n=4 (Рис.12)
Количество элементов для n=4 исходя из (Рис.12) будет равно $C_4^1 + C_4^2 + C_4^3 +$

$C_4^4 = 2^4 - 1$

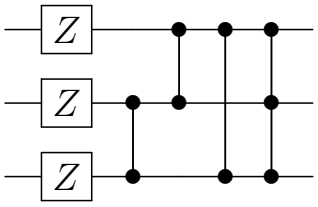


Рис. 11: Оператор Гровера на 3 кубитах.

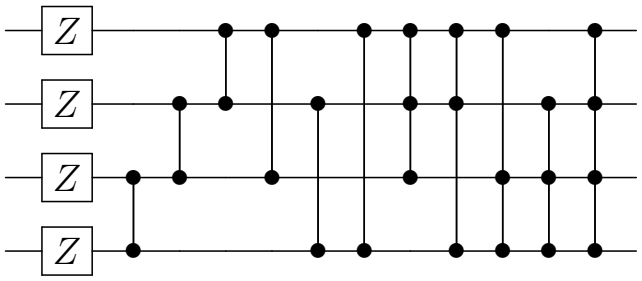


Рис. 12: Оператор Гровера на 4 кубитах.

Очевидно для общего случая количество элементов равно

$$C_n^1 + C_n^2 + ... + C_n^{n-1} + C_n^n = (1+1)^n - C_n^0 = 2^n - 1.$$

Для ускорения работы алгоритма по стоит заметить, что все операторы коммутируют, а некоторые из указанных операций можно выполнять одновременно, например, используя параллельно операторы $CZ \otimes E \otimes E$ и $E \otimes E \otimes CZ$ или $Z \otimes E \otimes E \otimes E \otimes CCZ$. Обратим при этом внимание, что $(n-k)$-кубитовых элементов ровно столько же, сколько k-кубитовых элементов и количество небоходимых этапов выполняния операций сокращается вдвое для всех операций,задействующих меньше n-кубитов,то есть количество времени оказывается не меньше 2^{n-1}.

4 Представление оператора C^nZ

Возникающие операторы C^nZ при разложении оператора Гровера, представим в виде операторов состоящих из однокубитовых элементов и CNOT.

Рассмотрим оператор C^nZ (Рис.13).

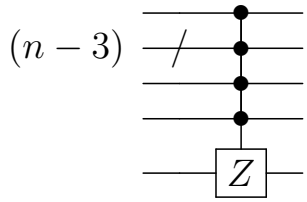


Рис. 13: Схематичное представление оператора C^nZ

Пусть $V_0 = Z, V_1 = S, V_2 = T, ..., V_n = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2^n}} \end{bmatrix}$

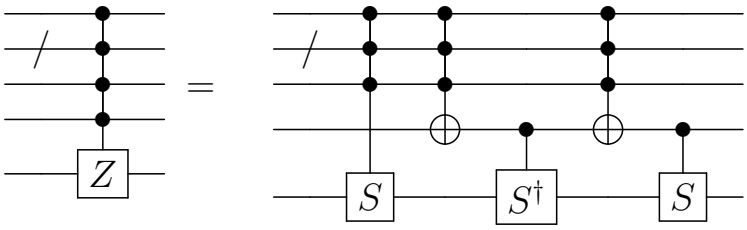


Рис. 14: Схема представления оператора C^nZ через операторы с меньшим количеством управляющих кубитов.

В общем виде формула имеет вид(Рис.15).

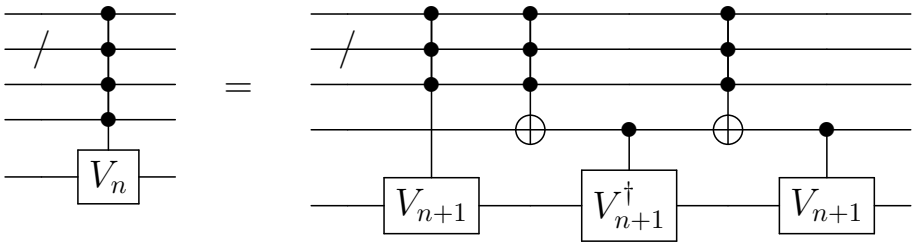


Рис. 15: Схема представления оператора C^nV_n через операторы с меньшим количеством управляющих кубитов.

Возникающие при этом элементы $C^{n-1}X$(Рис.16).

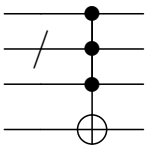


Рис. 16: Схематичное представление оператора $C^{n-1}X$.

Решаются путем представления X = HZH.

Чтобы наше представление было полным, то есть мы получили бы схему состоящую из однокубитовых элементов и CNOT, останется только разложить управляемые операторы.

Воспользуемся представлением вида(Рис.17).

Где $U = e^{i\alpha}AXBXC$ и $ABC = I$.

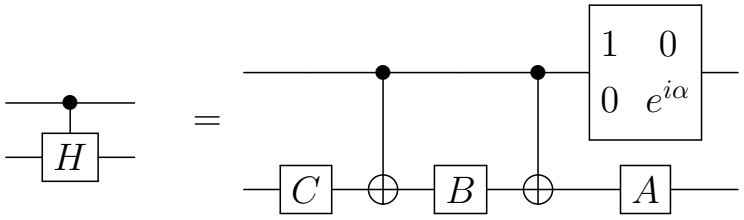
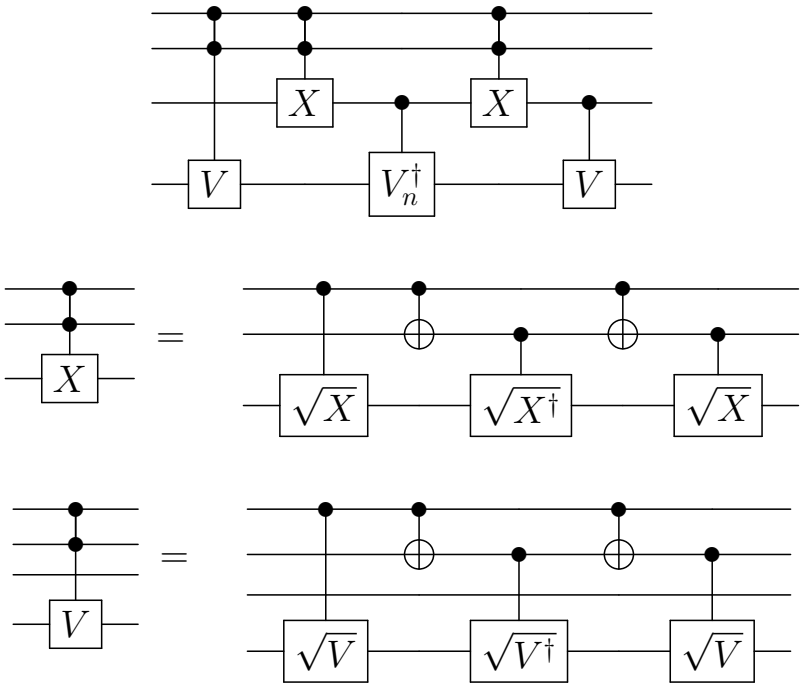
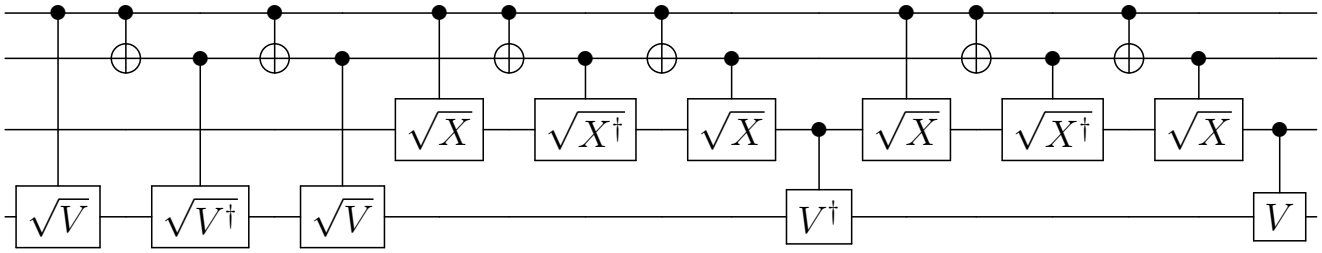


Рис. 17: Общий вид представления управляемого оператора U с помощью однокубитовых операторов и CNOT.

В нашем случае $V_n = exp\frac{i\pi}{2^{n+1}}R_z(\frac{\pi}{2^n})$, а значит
$A = R_z(\frac{\pi}{2^n}), B = R_y(-\frac{\pi}{2^{n+1}}), C = R_z(-\frac{\pi}{2^{n+1}}, \alpha = \frac{\pi}{2^{n+1}})$





5 Заключение.

В работе удалось разложить оператор $2|0\rangle\langle 0| - E$, использующийся в алгоритме Гровера, по системе операторов $\{Z, CZ, \ldots C^nZ\}$ и представить рекурсивную формулу получения через контролируемые операторы. Энергетическая затратность этого разложения, если считать, что все операции равноценны по энергетическим затратам, растет как 2^n, а оценка использованного времени составляет 2^{n-1}. Также удалось показать, что при дальнейшем разложении элементов типа C^nZ существенных упрощений системы не происходит. Таким образом, становится ясно, что даже учитывая существование разложений на стандартные элементы, для эффективной физической реализации алгоритма Гровера абсолютно необходимо использование операторов помимо операторов Паули и контролируемого отрицания.

Список литературы

[1] Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. М.: Мир, 2006.

[2] Холево А.С. Введение в квантовую теорию информации. М.: МЦ-НМО, 2002.

[3] Имре Ш., Баланж Ф. Квантовые вычисления и связь. М.: Физматлит, 2008.

[4] Калачёв А. Квантовая информатика в задачах. М.: Казанский(Приволжский) федеральный университет, 2012.