# IBM2

## Алгоритм Гровера

*Выполнили: Фадеев Артём, Елизбарашвили Серго, М32021*

## Цель работы:

- Изучить применение алгоритма Гровера
- Изучить принцип работы алгоритма
- Проанализировать полученные результаты

## Суть алгоритма

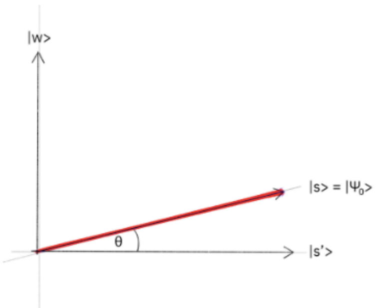
Представим классическую задачу поиска элемента в массиве. Классическими алгоритмами задача разрешима в среднем за $O(N/2)$ операций и за $O(N)$ в худшем.
Алгоритм Гровера позволяет сократить количество операций до $\sqrt{N}$.

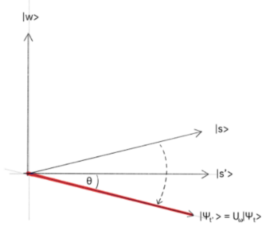
## Принцип работы

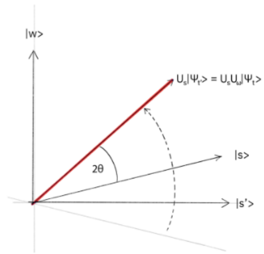
Алгоритм строится на методе *усиления амплитуды.* На каждой итерации алгоритма амплитуда искомого элемента увеличивается и, проделав определённое количество итераций, становится максимальной, что и позволяет найти искомый элемент.
Поскольку заранее ничего не известно о элементах массива данных, в котором производится поиск элемента, то единственное, что известно о нём — это суперпозиция всех его элементов $|s\rangle$. Поскольку изначально вероятность угадать искомый элемент ровно такая же, как угадать любой другой, то в худшем случае необходимо будет попробовать $N$ раз.

Метод усиления амплитуды имеет наглядную геометрическую интерпретацию:

в проекции на плоскость рассмотрим наш искомый элемент $w$ и изначальную суперпозицию всех элементов $|s\rangle$. Весь алгоритм основан на двух отражениях, переводящих через $T$ итераций вектор $|s\rangle$ в вектор $w$.




Первое отражение — отражение вектора суперпозиции относительно вектора $|s'\rangle$, перпендикулярного $w$. Пусть исходный угол между $|s\rangle$ = $\Psi_0$ и $|s'\rangle$ составляет $\theta$. Тогда после отражения угол между $\Psi_1$ и $|s\rangle$ будет $2\theta$, где $\Psi_1$ — образ вектора $\Psi_0$ после отражения.

Второе отражение — отражение $U_s|\Psi_1\rangle$ получившегося вектора $\Psi_1$ относительно вектора $|s>$. После двух отражений получаем, что исходный вектор $\Psi_0$ перешёл в вектор $U_s|\Psi_1\rangle,$ который составляет с вектором $|s'\rangle$ теперь уже угол, равный $3\theta$.

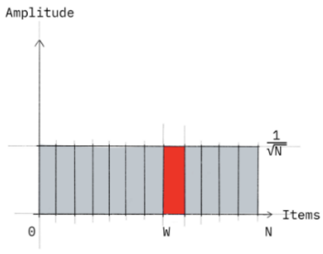
На следующей итерации угол между $U_s|\Psi_2\rangle$ и $|s\rangle$ будет $7\theta$, и с каждой итерацией будет увеличиваться на $2\theta^* + 1$, где $\theta^*$ - текущий угол между $\Psi_i$ и $|s'\rangle$

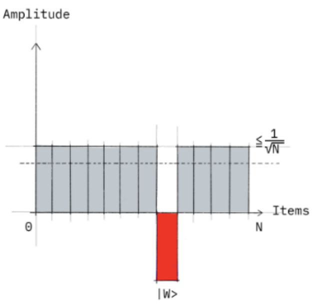
Итого получим уравнение на количество итераций, через которое исходный вектор $|s\rangle$ перейдёт в $w$:

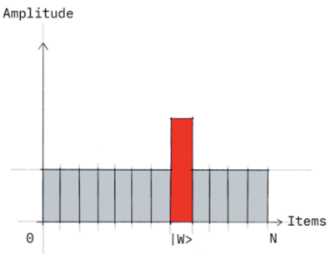
$\theta + 2\theta * T = \pi/2$, откуда $T = \frac{(\pi\sqrt{N})}{4} - \frac{1}{2\sqrt{N}}$, что доказывает факт о том, что элемент будет найден приблизительно за $\sqrt{N}$ операций

Наглядно описывает принцип работы и другая интерпретация в виде гистограммы:

Изначальная амплитуда всех состояний равна $\frac{1}{\sqrt{N}}$. Вышеприведенные отражения сначала изменяют амплитуду искомого элемента на противоположную, вследствие чего средняя амплитуда уменьшается, и модуль амплитуды отраженного элемента увеличивается. После чего искомый элемент вновь отражается и имеет более выраженную амплитуду, по сравнению с другими элементами.




## Пример с помощью квантового компьютера

Для простоты и наглядности возьмём всего 2 кубита. Для передачи их состояний будем использовать *оракулы:*

В общем виде оракул выглядит следующим образом:

$$U_w|x\rangle = \begin{cases} \ \ |x\rangle & \text{if } x \neq w \\ -|x\rangle & \text{if } x = w \end{cases}$$

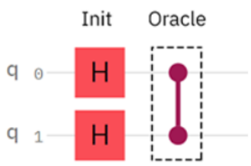
где $w$ — искомый элемент.

Не умаляя общности положим $|w\rangle = |11\rangle$

Тогда исходный оракул можно представить в виде матрицы:

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

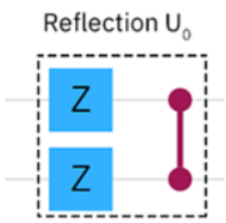
В схеме квантового компьютера оракул $U_w$ представляется в следующем виде:



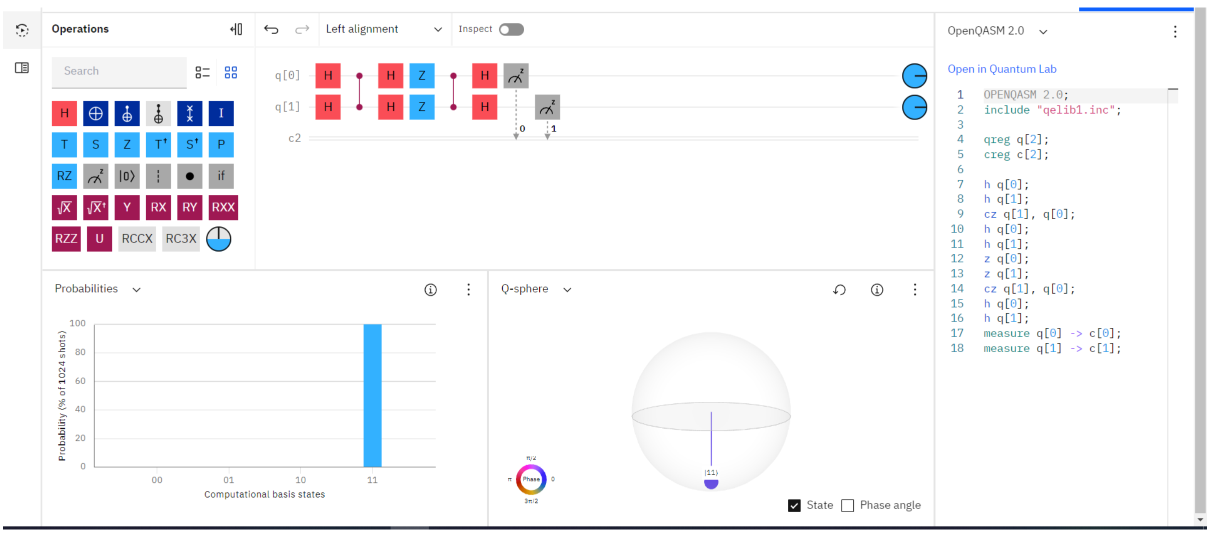

Оракул $U_s$ представляется следующим образом:

$$U_0 \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle - |11\rangle)$$

В схеме квантового компьютера оракул $U_s$ представляется в следующем виде:




И общая схема:




## Вывод

*Мы изучили принцип работы алгоритма Гровера и его применение, а также на практике реализовали его с помощью квантового компьютера и убедились в его преимуществе, по сравнению с обычными алгоритмами поиска.*