НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
ВЫСШАЯ ШКОЛА ЭКОНОМИКИ

Факультет физики

Вопрос по выбору

Обзор квантовых алгоритмов Гровера, Дойча и Дойча-Йожи

Работу выполнил студент 4 курса
Захаров Сергей Дмитриевич

Москва
2021

Содержание

Для обеспечения эффективной работы с квантовыми компьютерами необходимо использовать не обычные, а квантовые алгоритмы. Для ряда задач такие алгоритмы уже были придуманы. В этом обзоре я рассмотрю некоторые из них.

1. Алгоритм Гровера

Задача, которую решают с помощью алгоритма Гровера, формулируется следующим образом. Пусть задана некоторая функция $F(x)$, которая для некоторого конкретного x возвращает 1, для остальных — 0. Нужно найти этот x.

Рассмотрим ситуацию, когда x может принимать вид одной из четырех двоичных последовательностей из 0 и 1. Задача теперь стоит в определении нужной последовательности. Если решать задачу классическим способом, то правильный ответ мы будем получать в среднем за 2.25 вычисления функции F от разных последовательностей (при условии равных вероятностей). Для детерминированности положим $F(10) = 1$.

Сконструируем т.н. *оракул* — вентиль, который будет инкапсулировать нашу функцию F. В примере с четырьмя двоичным последовательностями оракул выглядит так, как указано на рисунке 1. Сам же алгоритм Гровера представлен на рисунке 2. Рассмотрим подробнее, что он делает.

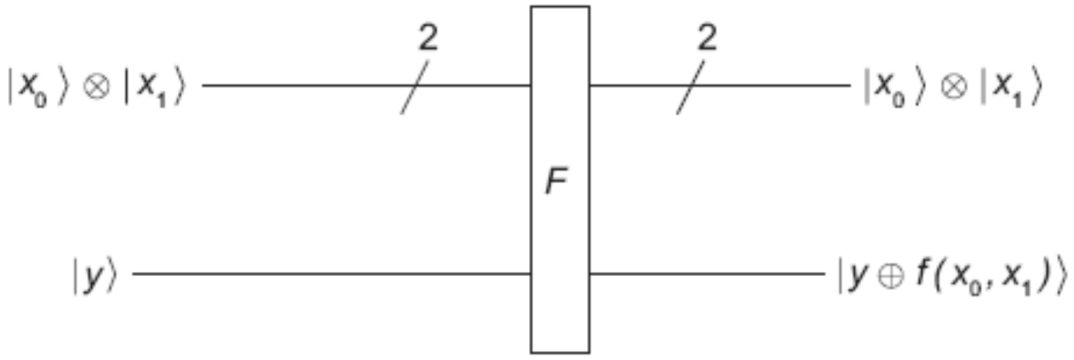

Рис. 1. Оракул для функции F. Косые наклонные линии с числом 2 означают обозначают параллельные входы и выходы.

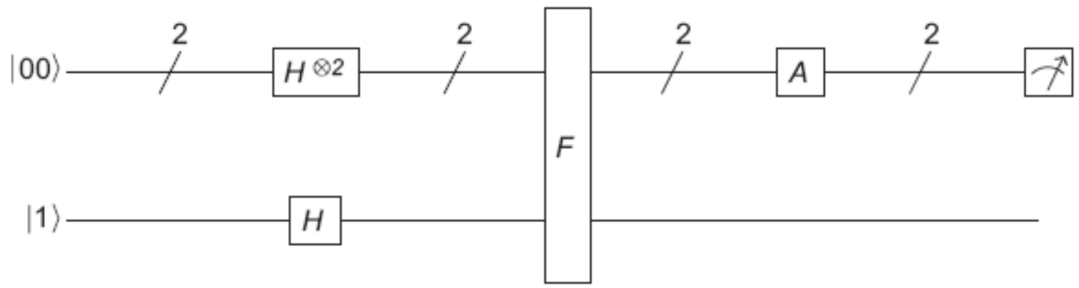

Рис. 2. Цепь алгоритма Гровера. Косые наклонные линии с числом 2 означают обозначают параллельные входы и выходы.

После передачи данных через вентили Адамара два верхних кубита получают состояние:

$$\frac{1}{2}\big(\,|00\rangle + |01\rangle + |10\rangle + |11\rangle\,\big) \tag{1}$$

Для нижнего же кубита:

$$\frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big) \tag{2}$$

После прохождения оракула происходит инвертирование 0 и 1 в третьем кубите в местоположение, которое нам нужно найти. Для нашего примера $F(10) = 1$:

$$\frac{1}{2}\left[|00\rangle \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big) + |01\rangle \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big) + |10\rangle \otimes \frac{1}{\sqrt{2}}\big(\,|1\rangle - |0\rangle\,\big) + \right.$$
$$\left. + |11\rangle \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big)\right]$$

В компактной форме можно это переписать:

$$\frac{1}{2}\big(\,|00\rangle + |01\rangle - |10\rangle + |11\rangle\,\big) \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big) \tag{3}$$

В результате мы получили два верхних кубита, ну спутанных с нижним, но амплитуда вероятности $|10\rangle$ поменяла знак, что и указывает на нужное местоположение.

Проделанного, однако, недостаточно: если на этом шаге измерить два верхних кубита, то мы равновероятно получим одну из четырех последовательностей, что нас не устраивает. Нам нужно теперь усилить амплитуда вероятности. Делается это путем переворачивания последовательности числе относительно их среднего: если число выше среднего, то оно перевернется и окажется ниже среднего и наоборот. В каждом случае расстояние до среднего очевидно сохраняется.

Для примера рассмотрим четыре числа: 1, 1, 1 и -1. Их среднее есть $1/2$. Посмотрим, что будет происходить при перевороте чисел. Первое, второе и третье числа выше среднего на $1/2$. Таким образом в результате переворота они превратятся в 0. Четвертое же число — -1 — меньше среднего и после переворота окажется равным 2.

В контексте нашей задачи мы имеем два верхних кубита в состоянии:

$$\frac{1}{2}\,|00\rangle + \frac{1}{2}\,|01\rangle - \frac{1}{2}\,|10\rangle + \frac{1}{2}\,|11\rangle \tag{4}$$

После переворота относительно среднего мы получим иные коэффициенты:

$$0\,|00\rangle + 0\,|01\rangle + 1\,|10\rangle + 0\,|11\rangle = |10\rangle \tag{5}$$

Теперь после измерения мы гарантированно получим последовательность 10. Нужно только убедиться в существовании вентиля (или ортогональной матрицы), которая описывала бы переворот относительно среднего. Такая матрица существует и записывается как:

$$A = \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix} \tag{6}$$

Если подставить ее действие на состояние 4, то мы получим как раз нужное нам состояние. Таким образом в случае $n = 2$ алгоритм Гровера позволяет гарантированно получить точный

ответ после единственного обращения к функции F, что в 2.25 раза быстрее, чем в классическом случае.

Идея распространяется и на случай произвольного числа кубитов n. Алгоритм действия такой же: мы переворачиваем знак амплитуды вероятности, соответствующей искомой последовательности, после чего совершаем переворот относительно среднего и усиливаем амплитуду. Однако в этом случае вероятность будет меньше. Рассмотрим для примера восемь чисел (3 кубита), первые из которых равны 1, а последнее — -1. Их среднее $6/8$, после переворота первые семь перейдут в $1/2$, а последнее — в $10/4$. Видно, что вероятность нужного нам числа больше, чем других, но уже не равно 100%. Нам нужно еще сильнее усилить амплитуду перед измерением.

Решением этой задачи может служить повторная передача кубитов через сеть. Таким образом нужная амплитуда усилится больше.

В общем случае задачу можно сформулировать так: из m возможных последовательностей нужно найти нужную. В классическом случае нужно будет в худшем случае $m-1$ измерение, число вопросов растет как $O(m)$. В квантовом же случае, как было показано Гровером, ассимптотика меняется и сложность алгоритма составляет $O(\sqrt{m})$ для получения максимальной вероятности правильного ответа (нужно $\sqrt{m}$ раз «прогнать» задачу через цепь).

2. Алгоритм Дойча

Зададимся похожей задачей. Пусть теперь у нас есть одна переменная, которая может принимать значение либо 1, либо 0, а также 4 функции, которые устроены следующим образом:

$$f_0(0) = 0, \quad f_0(1) = 0 \tag{7}$$
$$f_1(0) = 0, \quad f_0(1) = 1 \tag{8}$$
$$f_2(0) = 1, \quad f_0(1) = 0 \tag{9}$$
$$f_3(0) = 1, \quad f_0(1) = 1 \tag{10}$$

Функции, которые возвращают всегда одно и то же число (f_0, f_3), будем называть **константными**, функции, которые для половины значений возвращают 0, для половины — 1 (f_1, f_2), будем называть **сбалансированными.**

Задача — определить, какие функции являются сбалансированными, а какие — константными за минимальное число вычислений.

С точки зрения классики для каждой функции, очевидно, нужно произвести два измерения. Рассмотрим задачу с квантовой точки зрения.

Сконструируем модель вентиля, представленную на рисунке 2.

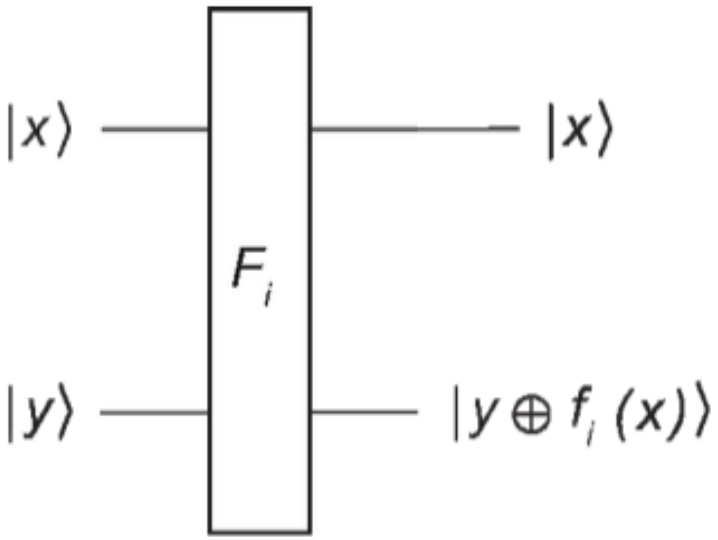

Рис. 3. Оракул для функции f_i в алгоритме Дойча

Согласно этой модели:

- Если на вход подать $|0\rangle \otimes |0\rangle$, то она выведет $|0\rangle \otimes |f_i(0)\rangle$;
- Если на вход подать $|0\rangle \otimes |1\rangle$, то она выведет $|0\rangle \otimes |f_i(0) \oplus 1\rangle$;
- Если на вход подать $|1\rangle \otimes |0\rangle$, то она выведет $|1\rangle \otimes |f_i(1)\rangle$;
- Если на вход подать $|1\rangle \otimes |1\rangle$, то она выведет $|0\rangle \otimes |f_i(1)\rangle \oplus 1$.

Таким образом для каждого i одна из $f_i(0)$, $f_i(0) \oplus 1$ равна 0, в то время как вторая равна 1 и аналогично для значения в 1. Таким образом четыре выхода всегда дают нам элементы стандартного базиса, т.е. матрица ортогональна, а значит модель действительно является вентилем.

Даже при том что мы вводим два бита информации и получаем два бита на выходе, информация, которую эти вентили дают для битов $|0\rangle$ и $|1\rangle$ такая же, как для функций, получающих 0 и 1. Верхний кубит — то, что мы вводим, поэтому вывод не дает нам ничего нового. Выбирая же $|0\rangle$ или $|1\rangle$ для второго, то мы получаем второй выход, дающий нам тот же результат, что вернула функция для верхнего входного кета или противоположный, т.е. зная один мы знаем второй.

Если ограничиться только вводом $|0\rangle$ и $|1\rangle$, то мы придем к тому же ответу, что и прежде. Вентиль нужно использовать дважды, но Дойч показал, что если использовать суперпозиции этих векторов, то можно обойтись одним использованием вентиля.

Для доказательства этого факта рассмотрим цепь, представленную на рисунке 2. Кубиты $|0\rangle \otimes |1\rangle$ — вход. Проходя через вентили Адамара, они перейдут в состояние:

$$\frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big) \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big) = \frac{1}{2}\big(\,|00\rangle - |01\rangle + |10\rangle - |11\rangle\,\big) \tag{11}$$

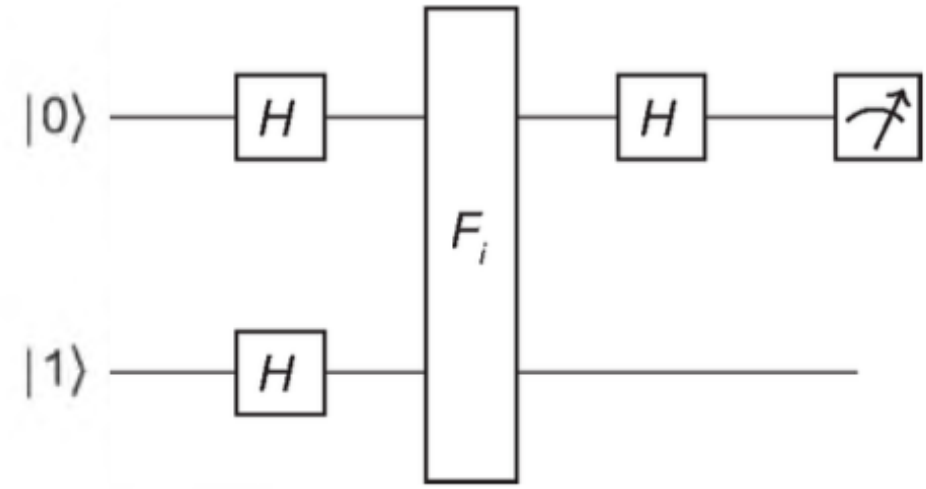

Рис. 4. Цепь алгоритма Дойча

Затем после прохождения вентиля F_i:

$$\frac{1}{2}\big(\,|0\rangle \otimes |f_i(0)\rangle - |0\rangle \otimes |f_i(0)\oplus 1\rangle + |1\rangle \otimes |f_i(1)\rangle - |1\rangle \otimes |f_i(1)\oplus 1\rangle\,\big) \tag{12}$$

Упрощая:

$$\frac{1}{2}\Big(\,|0\rangle \otimes \big(\,|f_i(0)\rangle - |f_i(0)\oplus 1\rangle\,\big) + |1\rangle\,\big(\,|f_i(1)\rangle - |f_i(1)\rangle \oplus 1\big)\Big) \tag{13}$$

Заметим, что верно выражение:

$$|f_i(0)\rangle - |f_i(0)\oplus 1\rangle = (-1)^{f_i(0)}\big(\,|0\rangle - |1\rangle\,\big) \tag{14}$$

А также:

$$|f_i(1)\rangle - |f_i(1)\oplus 1\rangle = (-1)^{f_i(1)}\big(\,|0\rangle - |1\rangle\,\big) \tag{15}$$

Тогда полученное выражение переписывается:

$$\frac{1}{2}\Big(\,|0\rangle \otimes \big((-1)^{f_i(0)}(|0\rangle - |1\rangle)\big) + |1\rangle \otimes \big((-1)^{f_i(1)}(|0\rangle - |1\rangle)\big)\Big) \tag{16}$$

Упрощая, получим итоговое выражение:

$$\frac{1}{\sqrt{2}}\big((-1)^{f_i(0)}\,|0\rangle + (-1)^{f_i(1)}\,|1\rangle\,\big) \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big) \tag{17}$$

Таким образом два кубита не спутаны и верхний кубит имеет состояние:

$$\frac{1}{\sqrt{2}}\big((-1)^{f_i(0)}\,|0\rangle + (-1)^{f_i(1)}\,|1\rangle\,\big) \tag{18}$$

Исследуем это состояние для каждой из возможных f_i:

- Для f_0 мы имеем $f_0(0) = f_0(1) = 0$, то есть кубит имеет состояние $(1/\sqrt{2})(|0\rangle + |1\rangle)$.

- Для f_1 мы имеем $f_1(0) = 0$ и $f_1(1) = 1$, то есть кубит имеет состояние $(1/\sqrt{2})(|0\rangle - |1\rangle)$.
- Для f_2 мы имеем $f_2(0) = 1$ и $f_2(1) = 0$, то есть кубит имеет состояние $-(1/\sqrt{2})(|0\rangle - |1\rangle)$.
- Для f_3 мы имеем $f_3(0) = f_3(1) = 1$, то есть кубит имеет состояние $-(1/\sqrt{2})(|0\rangle + |1\rangle)$.

Следующий шаг это еще одна передача в вентиль Адамара. В результате мы получим:

- если $i = 0$, то кубит имеет состояние $|0\rangle$;
- если $i = 1$, то кубит имеет состояние $|1\rangle$;
- если $i = 2$, то кубит имеет состояние $-|1\rangle$;
- если $i = 3$, то кубит имеет состояние $-|0\rangle$.

Теперь если мы измерим кубит в стандартном базисе, то мы получим 0, если $i = 0, 3$ и 1, если $i = 1, 2$, т.е. мы гарантированы отделяем константные функции от сбалансированных. Таким образом, мы можем обойтись одним обращением к оракулу.

3. Алгоритм Дойча-Йожи

Рассмотрим алгоритм Дойча, но теперь с функциями не одной, а n переменных. Каждая из них как и прежде приобретает значение 0 или 1. Концепция константной функции не меняется, а сбалансированная функция должна давать 0 для половины комбинаций выходов, а для второй половины должна возвращать 1. Задача остается той же, нужно понять, является ли случайная функция сбалансированной или константной.

Для примера рассмотрим случай $n = 3$. Тогда у нас есть $2^3 = 8$ различных входных комбинаций.

Рассматривая задачу с классической точки зрения можно показать, что в общем случае нужно в худшем случа задать $2^{n-1} + 1$ вопрос, т.е. сложность экспоненциальная.

Перейдем к квантовому описанию Для каждой функции f_i n булевых переменных сконструируем вентиль F, представленный на рисунке 3. Здесь косые наклонные линии с числом n означают обозначают параллельные входы и выходы.

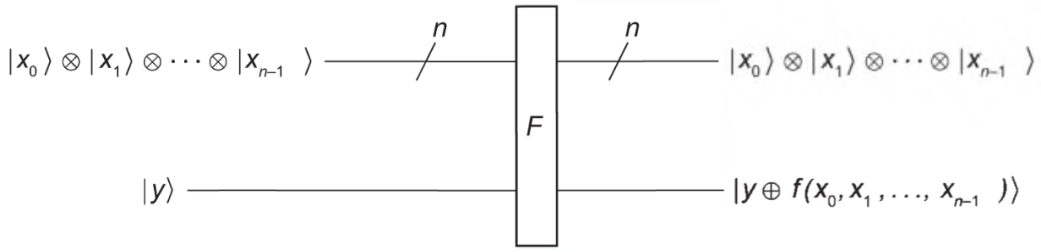

Рис. 5. Оракул для функции f_i в алгоритме Дойча-Йожи

Эта цепь сообщает нам, что происходит, когда каждый из $|x_i\rangle$ представлен как $|0\rangle$ или $|1\rangle$. На входе имеем $n + 1$ кетов, представимых в виде:

$$|x_0\rangle \otimes |x_1\rangle \otimes ... \otimes |x_{n-1}\rangle \tag{19}$$

а также $|y\rangle$, где первые n кетов соответствуют входным переменным. На выходе же мы видим $n+1$ кетов, первые n из которых в точности совпадают со входными кетами, в то время как последний выходной будет равне $|f(x_0, x_1, ..., x_{n-1})\rangle$, если $y = 0$ и кет с другим **булевым** значением, если $y = 1$.

Квантовая цепь для алгоритма выглядит так, как представлено на рисунке 3. Для упрощения задачи придется рассматривать $n = 2$ с оговоркой, что большие n работают так же.

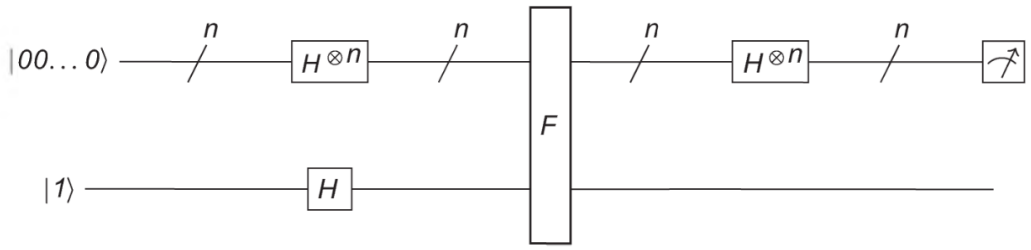

Рис. 6. Цепь алгоритма Дойча-Йожи

Первым этапом происходит передача кубитов через вентили Адамара. Все верхние n входов равны $|0\rangle$, т.е. в нашем случае это $|00\rangle$. После применения вентиля состояние:

$$\frac{1}{2}\big(\,|00\rangle + |01\rangle + |10\rangle + |11\rangle\,\big) \tag{20}$$

Нижний же выход это просто $|1\rangle$. После прохождения кубита через вентиль будет состояние:

$$\frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big) \tag{21}$$

Таким образом общее состояние:

$$\frac{1}{2}\big(\,|00\rangle + |01\rangle + |10\rangle + |11\rangle\,\big) \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big) \tag{22}$$

Мы можем переписать это выражение как:

$$\frac{1}{2\sqrt{2}}\Big(\,|00\rangle \otimes \big(\,|0\rangle - |1\rangle\,\big) + |01\rangle \otimes \big(\,|0\rangle - |1\rangle\,\big) + |10\rangle \otimes \big(\,|0\rangle - |1\rangle\,\big) + |11\rangle \otimes \big(\,|0\rangle - |1\rangle\,\big)\Big) \tag{23}$$

После перехода через вентиль F получится состояние:

$$\frac{1}{2\sqrt{2}}\,|00\rangle \otimes \big(\,|f(0,0)\rangle - |f(0,0)\oplus 1\rangle\,\big) + \frac{1}{2\sqrt{2}}\,|01\rangle \otimes \big(\,|f(0,1)\rangle - |f(0,1)\oplus 1\rangle\,\big) +$$
$$+\frac{1}{2\sqrt{2}}\,|10\rangle \otimes \big(\,|f(1,0)\rangle - |f(1,0)\oplus 1\rangle\,\big) + \frac{1}{2\sqrt{2}}\,|11\rangle \otimes \big(\,|f(1,1)\rangle - |f(1,1)\oplus 1\rangle\,\big)$$

Далее, если какое-то a может принимать только значения 0 или 1, тогда выполняется равенство:

$$|a\rangle - |a\oplus 1\rangle = (-1)^a(|0\rangle - |1\rangle) \tag{24}$$

С учетом этого факта:

$$(-1)^{f(0,0)}\frac{1}{2}\left|00\right\rangle \otimes \frac{1}{\sqrt{2}}\big(\left|0\right\rangle - \left|1\right\rangle\big) + (-1)^{f(0,1)}\frac{1}{2}\left|01\right\rangle \otimes \frac{1}{\sqrt{2}}\big(\left|0\right\rangle - \left|1\right\rangle\big) + \tag{25}$$

$$+(-1)^{f(1,0)}\frac{1}{2}\left|10\right\rangle \otimes \frac{1}{\sqrt{2}}\big(\left|0\right\rangle - \left|1\right\rangle\big) + (-1)^{f(1,1)}\frac{1}{2}\left|11\right\rangle \otimes \frac{1}{\sqrt{2}}\big(\left|0\right\rangle - \left|1\right\rangle\big) \tag{26}$$

Отсюда видно, что нижний кубит с верхними не запутан. Рассмотрим теперь просто два верхних кубита. Они находятся в состоянии:

$$\frac{1}{2}\Big((-1)^{f(0,0)}\left|00\right\rangle + (-1)^{f(0,1)}\left|01\right\rangle + (-1)^{f(1,0)}\left|10\right\rangle + (-1)^{f(1,1)}\left|11\right\rangle\Big) \tag{27}$$

Такое доказательство (идейно) будет верным для любого n.

Теперь нужно преобразовать состояние в вектор столбец с последующем умножением на соответствующее кронекеровское произведение матрицы Адамара. Нам, однако, не требуется вычислять все элементы, нам хватит только верхнего элемента, который будет получаться умножением бра, соответствующим верхней строке матрицы, на кет, заданный вектором-столбцом. Опуская вычисления:

$$\frac{1}{4}\Big((-1)^{f(0,0)} + (-1)^{f(0,1)} + (-1)^{f(1,0)} + (-1)^{f(1,1)}\Big) \tag{28}$$

Это амплитуда вероятности кета $\left|00\right\rangle$. Вычислим эту амплитуду для разных функций:

- Если f константная и всегда возвращает 0, то амплитуда вероятности равна 1;
- Если f константная и всегда возвращает 1, то амплитуда вероятности равна -1;
- Для сбалансированных функций амплитуда вероятности равна 0.

Измерив верхние кубиты, мы получим одно из значений: 00, 01, 10 или 11. Подумаем, когда мы получим 00. Если функция константная, то мы получим 1. Если сбалансированная, то 0. То есть если мы получаем 00, то можно утверждать, что функция константная. В случае любого другого отличного от 00 результата мы можем утверждать, что функция была сбалансированной.

Аналогичные размышления верны и для любого n. Непосредственно перед измерением кубитов амплитуда вероятности для $\left|0...0\right\rangle$ равна:

$$\frac{1}{2^n}\Big((-1)^{f(0,0,\ldots,0)} + (-1)^{f(0,0,\ldots,1)} + ... + (-1)^{f(1,1,\ldots,1)}\Big) \tag{29}$$

Как и для $n = 2$ в результате будет ± 1, если f — константная и 0, если f сбалансированная. Если все измерения дают 0, то функция константная, в противном случае — сбалансированная.

Таким образом нам нужно задавать оракулу **всего один вопрос**, в то время как в классическом алгоритме сложность была экспоненциальна. Очевидно значительное ускорение выполнения задачи.