Алгоритм Гровера

М. В. Волков

Уральский федеральный университет
Институт естественных наук и математики
кафедра алгебры и фундаментальной информатики

2020/2021 учебный год

Рассматривается функция $f : \mathbb{F}^n \to \mathbb{F}$, где, как обычно, $\mathbb{F} := \{0, 1\}$ — двухэлементное поле.

Рассматривается функция $f : \mathbb{F}^n \to \mathbb{F}$, где, как обычно, $\mathbb{F} := \{0, 1\}$ — двухэлементное поле. Об этой функции заранее известно, что есть ровно один «пароль» $x_0 \in \mathbb{F}^n$ такой, что $f(x_0) = 1$; $f(x) = 0$ для всех $x \neq x_0$.

Рассматривается функция $f\colon \mathbb{F}^n \to \mathbb{F}$, где, как обычно, $\mathbb{F} := \{0, 1\}$ — двухэлементное поле. Об этой функции заранее известно, что есть ровно один «пароль» $x_0 \in \mathbb{F}^n$ такой, что $f(x_0) = 1$; $f(x) = 0$ для всех $x \neq x_0$.

Как обычно, функция f неизвестна, но к ней можно обращаться как к черному ящику: задать аргумент $x \in \mathbb{F}^n$ и получить значение $f(x)$.

Рассматривается функция $f\colon \mathbb{F}^n \to \mathbb{F}$, где, как обычно, $\mathbb{F} := \{0, 1\}$ — двухэлементное поле. Об этой функции заранее известно, что есть ровно один «пароль» $x_0 \in \mathbb{F}^n$ такой, что $f(x_0) = 1$; $f(x) = 0$ для всех $x \neq x_0$.

Как обычно, функция f неизвестна, но к ней можно обращаться как к черному ящику: задать аргумент $x \in \mathbb{F}^n$ и получить значение $f(x)$.

Требуется найти x_0.

Алгоритм Гровера: постановка задачи

Рассматривается функция $f\colon \mathbb{F}^n \to \mathbb{F}$, где, как обычно, $\mathbb{F} := \{0, 1\}$ — двухэлементное поле. Об этой функции заранее известно, что есть ровно один «пароль» $x_0 \in \mathbb{F}^n$ такой, что $f(x_0) = 1$; $f(x) = 0$ для всех $x \neq x_0$.

Как обычно, функция f неизвестна, но к ней можно обращаться как к черному ящику: задать аргумент $x \in \mathbb{F}^n$ и получить значение $f(x)$.

Требуется найти x_0.

В отличие от задач, рассмотренных выше, задача Гровера имеет ясный практический смысл.

Алгоритм Гровера: постановка задачи

Рассматривается функция $f\colon \mathbb{F}^n \to \mathbb{F}$, где, как обычно, $\mathbb{F} := \{0, 1\}$ — двухэлементное поле. Об этой функции заранее известно, что есть ровно один «пароль» $x_0 \in \mathbb{F}^n$ такой, что $f(x_0) = 1$; $f(x) = 0$ для всех $x \neq x_0$.

Как обычно, функция f неизвестна, но к ней можно обращаться как к черному ящику: задать аргумент $x \in \mathbb{F}^n$ и получить значение $f(x)$.

Требуется найти x_0.

В отличие от задач, рассмотренных выше, задача Гровера имеет ясный практический смысл.

Легко понять, что любой классический вероятностный алгоритм для задачи Гровера требует по крайней мере $2^{n-1} + 1$ вызовов функции f, чтобы гарантировать успех с вероятностью $\frac{1}{2}$.

Рассматривается функция $f\colon \mathbb{F}^n \to \mathbb{F}$, где, как обычно, $\mathbb{F} := \{0, 1\}$ — двухэлементное поле. Об этой функции заранее известно, что есть ровно один «пароль» $x_0 \in \mathbb{F}^n$ такой, что $f(x_0) = 1$; $f(x) = 0$ для всех $x \neq x_0$.

Как обычно, функция f неизвестна, но к ней можно обращаться как к черному ящику: задать аргумент $x \in \mathbb{F}^n$ и получить значение $f(x)$.

Требуется найти x_0.

В отличие от задач, рассмотренных выше, задача Гровера имеет ясный практический смысл.

Легко понять, что любой классический вероятностный алгоритм для задачи Гровера требует по крайней мере $2^{n-1} + 1$ вызовов функции f, чтобы гарантировать успех с вероятностью $\frac{1}{2}$.

Лов Гровер в 1996 г. предложил для нее квантовый вероятностный алгоритм, который вызывает оператор U_f значительно реже.

Алгоритм Гровера работает с квантовой системой $H := H_{2^n} \otimes H_2$.

Алгоритм Гровера работает с квантовой системой $H := H_{2^n} \otimes H_2$.
Вместо $|a\rangle \otimes |b\rangle$ пишем $|a\rangle|b\rangle$ и ссылаемся на $|a\rangle$ и соответственно $|b\rangle$ как на *содержимое* первого и соответственно второго регистра.

Алгоритм Гровера работает с квантовой системой $H := H_{2^n} \otimes H_2$. Вместо $|a\rangle \otimes |b\rangle$ пишем $|a\rangle|b\rangle$ и ссылаемся на $|a\rangle$ и соответственно $|b\rangle$ как на *содержимое* первого и соответственно второго регистра.

Алгоритм Гровера

1. Инициализируем H в состояние $|0\rangle|1\rangle$.
2. Применяем преобразование Адамара $R_{2^n} \otimes R_2$
3. m раз применяем пару операторов: оператор $U_f : |a\rangle|b\rangle \mapsto |a\rangle|f(a) \oplus b\rangle$ и *оператор диффузии* $D := \dfrac{J}{2^{n-1}} - E$, где J — $2^n \times 2^n$-матрица из всех единиц, а E — единичная $2^n \times 2^n$-матрица.
4. Измеряя первый регистр, находим вектор x_0.

Алгоритм Гровера работает с квантовой системой $H := H_{2^n} \otimes H_2$. Вместо $|a\rangle \otimes |b\rangle$ пишем $|a\rangle|b\rangle$ и ссылаемся на $|a\rangle$ и соответственно $|b\rangle$ как на *содержимое* первого и соответственно второго регистра.

Алгоритм Гровера

1. Инициализируем H в состояние $|0\rangle|1\rangle$.
2. Применяем преобразование Адамара $R_{2^n} \otimes R_2$
3. m раз применяем пару операторов: оператор $U_f : |a\rangle|b\rangle \mapsto |a\rangle|f(a) \oplus b\rangle$ и *оператор диффузии* $D := \dfrac{J}{2^{n-1}} - E$, где J — $2^n \times 2^n$-матрица из всех единиц, а E — единичная $2^n \times 2^n$-матрица.
4. Измеряя первый регистр, находим вектор x_0.

Почему оператор диффузии можно применять, т.е. почему он унитарен?

Алгоритм Гровера работает с квантовой системой $H := H_{2^n} \otimes H_2$. Вместо $|a\rangle \otimes |b\rangle$ пишем $|a\rangle|b\rangle$ и ссылаемся на $|a\rangle$ и соответственно $|b\rangle$ как на *содержимое* первого и соответственно второго регистра.

Алгоритм Гровера

1. Инициализируем H в состояние $|0\rangle|1\rangle$.
2. Применяем преобразование Адамара $R_{2^n} \otimes R_2$
3. m раз применяем пару операторов: оператор $U_f : |a\rangle|b\rangle \mapsto |a\rangle|f(a) \oplus b\rangle$ и *оператор диффузии* $D := \dfrac{J}{2^{n-1}} - E$, где J — $2^n \times 2^n$-матрица из всех единиц, а E — единичная $2^n \times 2^n$-матрица.
4. Измеряя первый регистр, находим вектор x_0.

Почему оператор диффузии можно применять, т.е. почему он унитарен?

Как выбрать число итераций m, чтобы измерение первого регистра дало вектор x_0 с максимальной вероятностью?

То, что оператор диффузии $D = \frac{J}{2^{n-1}} - E$, где J — $2^n \times 2^n$-матрица из всех единиц, а E — единичная $2^n \times 2^n$-матрица, унитарен, проверяется прямым подсчётом.

То, что оператор диффузии $D = \frac{J}{2^{n-1}} - E$, где J — $2^n \times 2^n$-матрица из всех единиц, а E — единичная $2^n \times 2^n$-матрица, унитарен, проверяется прямым подсчётом.

Поскольку D — действительная симметрическая матрица, имеем $D^* = D$.

То, что оператор диффузии $D = \dfrac{J}{2^{n-1}} - E$, где J — $2^n \times 2^n$-матрица из всех единиц, а E — единичная $2^n \times 2^n$-матрица, унитарен, проверяется прямым подсчётом.

Поскольку D — действительная симметрическая матрица, имеем $D^* = D$. Теперь вычислим $DD^* = D^2$:

Оператор диффузии

То, что оператор диффузии $D = \dfrac{J}{2^{n-1}} - E$, где J — $2^n \times 2^n$-матрица из всех единиц, а E — единичная $2^n \times 2^n$-матрица, унитарен, проверяется прямым подсчётом.

Поскольку D — действительная симметрическая матрица, имеем $D^* = D$. Теперь вычислим $DD^* = D^2$:

$$D^2 = \frac{J^2}{2^{2(n-1)}} - 2\frac{J}{2^{n-1}} + E = \frac{J}{2^{n-2}} - \frac{J}{2^{n-2}} + E = E,$$

поскольку $J^2 = 2^n J$.

То, что оператор диффузии $D = \dfrac{J}{2^{n-1}} - E$, где J — $2^n \times 2^n$-матрица из всех единиц, а E — единичная $2^n \times 2^n$-матрица, унитарен, проверяется прямым подсчётом.

Поскольку D — действительная симметрическая матрица, имеем $D^* = D$. Теперь вычислим $DD^* = D^2$:

$$D^2 = \frac{J^2}{2^{2(n-1)}} - 2\frac{J}{2^{n-1}} + E = \frac{J}{2^{n-2}} - \frac{J}{2^{n-2}} + E = E,$$

поскольку $J^2 = 2^n J$.

Отметим еще, что если обозначить через $|1^n\rangle$ вектор $R_{2^n}|0\rangle = \dfrac{1}{\sqrt{2^n}}\begin{bmatrix}1\\1\\\vdots\\1\end{bmatrix}$,

то $\dfrac{J}{2^{n-1}}$ можно записать как $2|1^n\rangle\langle 1^n|$.

То, что оператор диффузии $D = \frac{J}{2^{n-1}} - E$, где J — $2^n \times 2^n$-матрица из всех единиц, а E — единичная $2^n \times 2^n$-матрица, унитарен, проверяется прямым подсчётом.

Поскольку D — действительная симметрическая матрица, имеем $D^* = D$. Теперь вычислим $DD^* = D^2$:

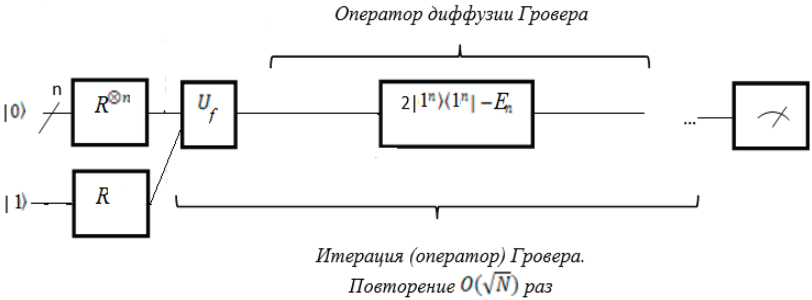
$$D^2 = \frac{J^2}{2^{2(n-1)}} - 2\frac{J}{2^{n-1}} + E = \frac{J}{2^{n-2}} - \frac{J}{2^{n-2}} + E = E,$$

поскольку $J^2 = 2^n J$.

Отметим еще, что если обозначить через $|1^n\rangle$ вектор $R_{2^n}|0\rangle = \frac{1}{\sqrt{2^n}}\begin{bmatrix}1\\1\\\vdots\\1\end{bmatrix}$,

то $\frac{J}{2^{n-1}}$ можно записать как $2|1^n\rangle\langle 1^n|$. Для краткости положим $N := 2^n$.

Алгоритм Гровера: схема



Разберем алгоритм Гровера сначала на примере, когда $n = 2$, а $x_0 = 10_2 = 2_{10}$.

Разберем алгоритм Гровера сначала на примере, когда $n = 2$, а $x_0 = 10_2 = 2_{10}$. После шага 1 состояние $|0\rangle|1\rangle$.

Разберем алгоритм Гровера сначала на примере, когда $n = 2$,
а $x_0 = 10_2 = 2_{10}$. После шага 1 состояние $|0\rangle|1\rangle$.

На шаге 2 применяется преобразование Адамара. Первый регистр станет равным $R_4|0\rangle = \frac{1}{2}\begin{bmatrix}1\\1\\1\\1\end{bmatrix}$, а второй – $R_2|1\rangle = |\chi\rangle$, где $|\chi\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Разберем алгоритм Гровера сначала на примере, когда $n = 2$, а $x_0 = 10_2 = 2_{10}$. После шага 1 состояние $|0\rangle|1\rangle$.

На шаге 2 применяется преобразование Адамара. Первый регистр станет равным $R_4|0\rangle = \frac{1}{2}\begin{bmatrix}1\\1\\1\\1\end{bmatrix}$, а второй – $R_2|1\rangle = |\chi\rangle$, где $|\chi\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

На шаге 3 сначала применяется оператор $U_f : |a\rangle|b\rangle \mapsto |a\rangle|f(a) \oplus b\rangle$.

Разберем алгоритм Гровера сначала на примере, когда $n = 2$, а $x_0 = 10_2 = 2_{10}$. После шага 1 состояние $|0\rangle|1\rangle$.

На шаге 2 применяется преобразование Адамара. Первый регистр станет равным $R_4|0\rangle = \frac{1}{2}\begin{bmatrix}1\\1\\1\\1\end{bmatrix}$, а второй – $R_2|1\rangle = |\chi\rangle$, где $|\chi\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

На шаге 3 сначала применяется оператор $U_f : |a\rangle|b\rangle \mapsto |a\rangle|f(a) \oplus b\rangle$. Поскольку $0 \oplus \chi = \chi$, а $1 \oplus \chi = \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) = -\chi$, имеем $f(a) \oplus \chi = (-1)^{f(a)}\chi$.

Разберем алгоритм Гровера сначала на примере, когда $n = 2$, а $x_0 = 10_2 = 2_{10}$. После шага 1 состояние $|0\rangle|1\rangle$.

На шаге 2 применяется преобразование Адамара. Первый регистр станет равным $R_4|0\rangle = \frac{1}{2}\begin{bmatrix}1\\1\\1\\1\end{bmatrix}$, а второй – $R_2|1\rangle = |\chi\rangle$, где $|\chi\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

На шаге 3 сначала применяется оператор $U_f : |a\rangle|b\rangle \mapsto |a\rangle|f(a) \oplus b\rangle$.

Поскольку $0 \oplus \chi = \chi$, а $1 \oplus \chi = \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) = -\chi$, имеем

$f(a) \oplus \chi = (-1)^{f(a)}\chi$. Наша функция f такова, что $f(0) = f(1) = f(3) = 0$, а $f(2) = 1$.

Разберем алгоритм Гровера сначала на примере, когда $n = 2$, а $x_0 = 10_2 = 2_{10}$. После шага 1 состояние $|0\rangle|1\rangle$.

На шаге 2 применяется преобразование Адамара. Первый регистр станет равным $R_4|0\rangle = \frac{1}{2}\begin{bmatrix}1\\1\\1\\1\end{bmatrix}$, а второй – $R_2|1\rangle = |\chi\rangle$, где $|\chi\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

На шаге 3 сначала применяется оператор $U_f : |a\rangle|b\rangle \mapsto |a\rangle|f(a) \oplus b\rangle$.

Поскольку $0 \oplus \chi = \chi$, а $1 \oplus \chi = \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) = -\chi$, имеем $f(a) \oplus \chi = (-1)^{f(a)}\chi$. Наша функция f такова, что $f(0) = f(1) = f(3) = 0$, а $f(2) = 1$. Поэтому действие оператора U_f сводится к смене знака коэффициента у третьего базисного вектора $|2\rangle$, т.е. к умножению на матрицу $T := \begin{bmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & -1 & 0\\0 & 0 & 0 & 1\end{bmatrix}$.

Алгоритм Гровера: пример при $n = 2$

Разберем алгоритм Гровера сначала на примере, когда $n = 2$, а $x_0 = 10_2 = 2_{10}$. После шага 1 состояние $|0\rangle|1\rangle$.

На шаге 2 применяется преобразование Адамара. Первый регистр станет равным $R_4|0\rangle = \frac{1}{2}\begin{bmatrix}1\\1\\1\\1\end{bmatrix}$, а второй – $R_2|1\rangle = |\chi\rangle$, где $|\chi\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

На шаге 3 сначала применяется оператор $U_f : |a\rangle|b\rangle \mapsto |a\rangle|f(a) \oplus b\rangle$.

Поскольку $0 \oplus \chi = \chi$, а $1 \oplus \chi = \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) = -\chi$, имеем $f(a) \oplus \chi = (-1)^{f(a)}\chi$. Наша функция f такова, что $f(0) = f(1) = f(3) = 0$, а $f(2) = 1$. Поэтому действие оператора U_f сводится к смене знака коэффициента у третьего базисного вектора $|2\rangle$, т.е. к умножению

на матрицу $T := \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&-1&0\\0&0&0&1\end{bmatrix}$. Затем применяется оператор

$$D = \frac{J}{2} - E = \begin{bmatrix}-0.5&0.5&0.5&0.5\\0.5&-0.5&0.5&0.5\\0.5&0.5&-0.5&0.5\\0.5&0.5&0.5&-0.5\end{bmatrix}.$$

Перемножая матрицы, получим

$$DT = \begin{bmatrix} -0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & -0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & -0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 & -0.5 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} -0.5 & 0.5 & -0.5 & 0.5 \\ 0.5 & -0.5 & -0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & -0.5 & -0.5 \end{bmatrix}.$$

Перемножая матрицы, получим

$$DT = \begin{bmatrix} -0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & -0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & -0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 & -0.5 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} -0.5 & 0.5 & -0.5 & 0.5 \\ 0.5 & -0.5 & -0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & -0.5 & -0.5 \end{bmatrix}.$$

Отсюда $DT \cdot \dfrac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |2\rangle.$

Перемножая матрицы, получим

$$DT = \begin{bmatrix} -0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & -0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & -0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 & -0.5 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} -0.5 & 0.5 & -0.5 & 0.5 \\ 0.5 & -0.5 & -0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & -0.5 & -0.5 \end{bmatrix}.$$

Отсюда $DT \cdot \frac{1}{2}\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |2\rangle$. Измеряя, находим верное значение $x_0 = 2$ с вероятностью 1.

Перемножая матрицы, получим

$$DT = \begin{bmatrix} -0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & -0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & -0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 & -0.5 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} -0.5 & 0.5 & -0.5 & 0.5 \\ 0.5 & -0.5 & -0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & -0.5 & -0.5 \end{bmatrix}.$$

Отсюда $DT \cdot \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |2\rangle$. Измеряя, находим верное значение $x_0 = 2$ с вероятностью 1. Итак, для $n = 2$ правильное число итераций m равно 1.

Перемножая матрицы, получим

$$DT = \begin{bmatrix} -0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & -0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & -0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 & -0.5 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} -0.5 & 0.5 & -0.5 & 0.5 \\ 0.5 & -0.5 & -0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & -0.5 & -0.5 \end{bmatrix}.$$

Отсюда $DT \cdot \dfrac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |2\rangle$. Измеряя, находим верное значение $x_0 = 2$ с вероятностью 1. Итак, для $n = 2$ правильное число итераций m равно 1.

Заметим, что еще одно выполнение шага 2 только испортило бы результат:

$$DT \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} -0.5 \\ -0.5 \\ 0.5 \\ -0.5 \end{bmatrix}.$$

Выполним оператор DT над произвольным вектором вида $\begin{bmatrix} r_0 \\ r_0 \\ s_0 \\ r_0 \end{bmatrix}$.

Выполним оператор DT над произвольным вектором вида $\begin{bmatrix} r_0 \\ r_0 \\ s_0 \\ r_0 \end{bmatrix}$.

$$DT \begin{bmatrix} r_0 \\ r_0 \\ s_0 \\ r_0 \end{bmatrix} = \begin{bmatrix} -0.5 & 0.5 & -0.5 & 0.5 \\ 0.5 & -0.5 & -0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & -0.5 & -0.5 \end{bmatrix} \begin{bmatrix} r_0 \\ r_0 \\ s_0 \\ r_0 \end{bmatrix} = \begin{bmatrix} 0.5r_0 - 0.5s_0 \\ 0.5r_0 - 0.5s_0 \\ 1.5r_0 + 0.5s_0 \\ 0.5r_0 - 0.5s_0 \end{bmatrix}.$$

Выполним оператор DT над произвольным вектором вида $\begin{bmatrix} r_0 \\ r_0 \\ s_0 \\ r_0 \end{bmatrix}$.

$$DT \begin{bmatrix} r_0 \\ r_0 \\ s_0 \\ r_0 \end{bmatrix} = \begin{bmatrix} -0.5 & 0.5 & -0.5 & 0.5 \\ 0.5 & -0.5 & -0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & -0.5 & -0.5 \end{bmatrix} \begin{bmatrix} r_0 \\ r_0 \\ s_0 \\ r_0 \end{bmatrix} = \begin{bmatrix} 0.5r_0 - 0.5s_0 \\ 0.5r_0 - 0.5s_0 \\ 1.5r_0 + 0.5s_0 \\ 0.5r_0 - 0.5s_0 \end{bmatrix}.$$

Видим, что получается вектор $\begin{bmatrix} r_1 \\ r_1 \\ s_1 \\ r_1 \end{bmatrix}$ с $r_1 = 0.5r_0 - 0.5s_0$ и $s_1 = 1.5r_0 + 0.5s_0$.

Выполним оператор DT над произвольным вектором вида $\begin{bmatrix} r_0 \\ r_0 \\ s_0 \\ r_0 \end{bmatrix}$.

$$DT \begin{bmatrix} r_0 \\ r_0 \\ s_0 \\ r_0 \end{bmatrix} = \begin{bmatrix} -0.5 & 0.5 & -0.5 & 0.5 \\ 0.5 & -0.5 & -0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & -0.5 & -0.5 \end{bmatrix} \begin{bmatrix} r_0 \\ r_0 \\ s_0 \\ r_0 \end{bmatrix} = \begin{bmatrix} 0.5r_0 - 0.5s_0 \\ 0.5r_0 - 0.5s_0 \\ 1.5r_0 + 0.5s_0 \\ 0.5r_0 - 0.5s_0 \end{bmatrix}.$$

Видим, что получается вектор $\begin{bmatrix} r_1 \\ r_1 \\ s_1 \\ r_1 \end{bmatrix}$ с $r_1 = 0.5r_0 - 0.5s_0$ и $s_1 = 1.5r_0 + 0.5s_0$.

Умножение на DT сохраняет длину вектора, откуда $3r_0^2 + s_0^2 = 3r_1^2 + s_1^2$.

Выполним оператор DT над произвольным вектором вида $\begin{bmatrix} r_0 \\ r_0 \\ s_0 \\ r_0 \end{bmatrix}$.

$$DT \begin{bmatrix} r_0 \\ r_0 \\ s_0 \\ r_0 \end{bmatrix} = \begin{bmatrix} -0.5 & 0.5 & -0.5 & 0.5 \\ 0.5 & -0.5 & -0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & -0.5 & -0.5 \end{bmatrix} \begin{bmatrix} r_0 \\ r_0 \\ s_0 \\ r_0 \end{bmatrix} = \begin{bmatrix} 0.5r_0 - 0.5s_0 \\ 0.5r_0 - 0.5s_0 \\ 1.5r_0 + 0.5s_0 \\ 0.5r_0 - 0.5s_0 \end{bmatrix}.$$

Видим, что получается вектор $\begin{bmatrix} r_1 \\ r_1 \\ s_1 \\ r_1 \end{bmatrix}$ с $r_1 = 0.5r_0 - 0.5s_0$ и $s_1 = 1.5r_0 + 0.5s_0$.

Умножение на DT сохраняет длину вектора, откуда $3r_0^2 + s_0^2 = 3r_1^2 + s_1^2$.
Сделаем замену переменных $a_i := \sqrt{3}r_i$, $b_i := s_i$. Тогда $a_0^2 + b_0^2 = a_1^2 + b_1^2 = 1$
и $\begin{cases} \frac{1}{\sqrt{3}}a_1 & = \frac{1}{2\sqrt{3}}a_0 - \frac{1}{2}b_0 \\ b_1 & = \frac{3}{2\sqrt{3}}a_0 + \frac{1}{2}b_0 \end{cases}$, откуда $\begin{cases} a_1 & = \frac{1}{2}a_0 - \frac{\sqrt{3}}{2}b_0 = a_0 \cos\frac{\pi}{3} - b_0 \sin\frac{\pi}{3} \\ b_1 & = \frac{\sqrt{3}}{2}a_0 + \frac{1}{2}b_0 = a_0 \sin\frac{\pi}{3} + b_0 \cos\frac{\pi}{3} \end{cases}$.

Выполним оператор DT над произвольным вектором вида $\begin{bmatrix} r_0 \\ r_0 \\ s_0 \\ r_0 \end{bmatrix}$.

$$DT \begin{bmatrix} r_0 \\ r_0 \\ s_0 \\ r_0 \end{bmatrix} = \begin{bmatrix} -0.5 & 0.5 & -0.5 & 0.5 \\ 0.5 & -0.5 & -0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & -0.5 & -0.5 \end{bmatrix} \begin{bmatrix} r_0 \\ r_0 \\ s_0 \\ r_0 \end{bmatrix} = \begin{bmatrix} 0.5r_0 - 0.5s_0 \\ 0.5r_0 - 0.5s_0 \\ 1.5r_0 + 0.5s_0 \\ 0.5r_0 - 0.5s_0 \end{bmatrix}.$$

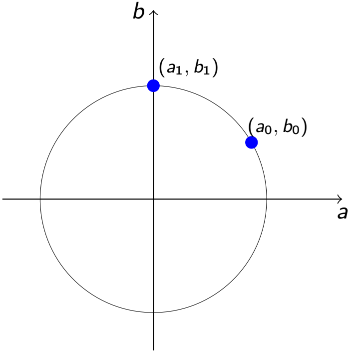
Видим, что получается вектор $\begin{bmatrix} r_1 \\ r_1 \\ s_1 \\ r_1 \end{bmatrix}$ с $r_1 = 0.5r_0 - 0.5s_0$ и $s_1 = 1.5r_0 + 0.5s_0$.

Умножение на DT сохраняет длину вектора, откуда $3r_0^2 + s_0^2 = 3r_1^2 + s_1^2$. Сделаем замену переменных $a_i := \sqrt{3}r_i$, $b_i := s_i$. Тогда $a_0^2 + b_0^2 = a_1^2 + b_1^2 = 1$ и $\begin{cases} \frac{1}{\sqrt{3}}a_1 & = \frac{1}{2\sqrt{3}}a_0 - \frac{1}{2}b_0 \\ b_1 & = \frac{3}{2\sqrt{3}}a_0 + \frac{1}{2}b_0 \end{cases}$, откуда $\begin{cases} a_1 & = \frac{1}{2}a_0 - \frac{\sqrt{3}}{2}b_0 = a_0\cos\frac{\pi}{3} - b_0\sin\frac{\pi}{3} \\ b_1 & = \frac{\sqrt{3}}{2}a_0 + \frac{1}{2}b_0 = a_0\sin\frac{\pi}{3} + b_0\cos\frac{\pi}{3} \end{cases}$.

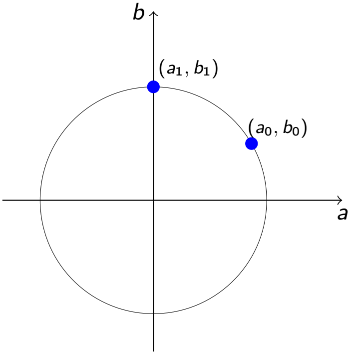
Итак, точки (a_0, b_0) и (a_1, b_1) лежат на единичной окружности и вторая получается из первой поворотом на угол $\frac{\pi}{3}$ против часовой стрелки.

Поскольку $r_0 = s_0 = \frac{1}{2}$, имеем $a_0 = \frac{\sqrt{3}}{2} = \cos\frac{\pi}{6}$, а $b_0 = \frac{1}{2} = \sin\frac{\pi}{6}$.

Поскольку $r_0 = s_0 = \frac{1}{2}$, имеем $a_0 = \frac{\sqrt{3}}{2} = \cos\frac{\pi}{6}$, а $b_0 = \frac{1}{2} = \sin\frac{\pi}{6}$.

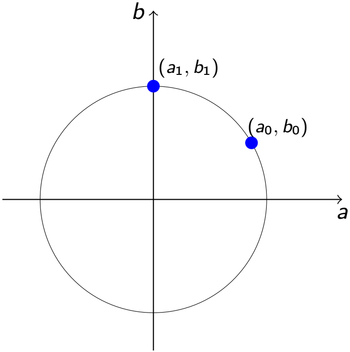


Поскольку $r_0 = s_0 = \frac{1}{2}$, имеем $a_0 = \frac{\sqrt{3}}{2} = \cos\frac{\pi}{6}$, а $b_0 = \frac{1}{2} = \sin\frac{\pi}{6}$.



Так как $\frac{\pi}{6} + \frac{\pi}{3} = \frac{\pi}{2}$, точка (a_1, b_1) — это точка $(0, 1)$.

Поскольку $r_0 = s_0 = \frac{1}{2}$, имеем $a_0 = \frac{\sqrt{3}}{2} = \cos\frac{\pi}{6}$, а $b_0 = \frac{1}{2} = \sin\frac{\pi}{6}$.



Так как $\frac{\pi}{6} + \frac{\pi}{3} = \frac{\pi}{2}$, точка (a_1, b_1) — это точка $(0, 1)$. В этом положении модуль коэффициента при «правильном» векторе наибольший, а модули коэффициентов при «неправильных» векторах наименьшие.

Проанализируем общий случай. Пусть r_i и s_i — коэффициенты при «неправильных» векторах и «правильном» векторе соответственно перед $(i+1)$-й итерацией на шаге 3 алгоритма $(i = 0, 1, \ldots, m-1)$.

Проанализируем общий случай. Пусть r_i и s_i — коэффициенты при «неправильных» векторах и «правильном» векторе соответственно перед $(i+1)$-й итерацией на шаге 3 алгоритма $(i = 0, 1, \dots, m-1)$. Если $f(x) = 1$ только при $x = x_0$, то матрица T, отвечающая применению U_f, есть

$$\begin{array}{cc} & \begin{array}{ccccc} & & x_0 & & \end{array} \\ x_0 & \begin{bmatrix} 1 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & -1 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & 1 \end{bmatrix} \end{array}.$$

Алгоритм Гровера: геометрический анализ

Проанализируем общий случай. Пусть r_i и s_i — коэффициенты при «неправильных» векторах и «правильном» векторе соответственно перед $(i+1)$-й итерацией на шаге 3 алгоритма $(i = 0, 1, \ldots, m-1)$. Если $f(x) = 1$ только при $x = x_0$, то матрица T, отвечающая применению U_f, есть

$$\begin{array}{cc} & \begin{array}{ccccc} & & x_0 & & \end{array} \\ x_0 & \begin{bmatrix} 1 & \ldots & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \ldots & -1 & \ldots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \ldots & 0 & \ldots & 1 \end{bmatrix} \end{array}.$$

Матрица $D = \dfrac{2J}{N} - E$ имеет вид

$$\begin{bmatrix} \frac{2}{N} - 1 & \frac{2}{N} & \ldots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} - 1 & \ldots & \frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \ldots & \frac{2}{N} - 1 \end{bmatrix}$$

Алгоритм Гровера: геометрический анализ

Проанализируем общий случай. Пусть r_i и s_i — коэффициенты при «неправильных» векторах и «правильном» векторе соответственно перед $(i+1)$-й итерацией на шаге 3 алгоритма $(i = 0, 1, \dots, m-1)$.

Если $f(x) = 1$ только при $x = x_0$, то матрица T, отвечающая применению U_f, есть

$$
\begin{array}{cc}
 & \begin{array}{ccccc} & & x_0 & & \end{array} \\
x_0 & \begin{bmatrix}
1 & \dots & 0 & \dots & 0 \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
0 & \dots & -1 & \dots & 0 \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
0 & \dots & 0 & \dots & 1
\end{bmatrix}
\end{array}.
$$

Матрица $D = \dfrac{2J}{N} - E$ имеет вид

$$
\begin{bmatrix}
\frac{2}{N} - 1 & \frac{2}{N} & \dots & \frac{2}{N} \\
\frac{2}{N} & \frac{2}{N} - 1 & \dots & \frac{2}{N} \\
\vdots & \vdots & \ddots & \vdots \\
\frac{2}{N} & \frac{2}{N} & \dots & \frac{2}{N} - 1
\end{bmatrix},
$$

а

$$
DT =
\begin{array}{c}
\begin{array}{cccccc} \phantom{\frac{2}{N}-1} & \phantom{\frac{2}{N}} & & x_0 & & \phantom{\frac{2}{N}} \end{array} \\
\begin{bmatrix}
\frac{2}{N} - 1 & \frac{2}{N} & \dots & -\frac{2}{N} & \dots & \frac{2}{N} \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
\frac{2}{N} & \frac{2}{N} & \dots & 1 - \frac{2}{N} & \dots & \frac{2}{N} \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
\frac{2}{N} & \frac{2}{N} & \dots & -\frac{2}{N} & \dots & \frac{2}{N} - 1
\end{bmatrix}
\end{array}.
$$

Алгоритм Гровера: геометрический анализ (2)

$$DT\begin{bmatrix} r_i \\ \vdots \\ r_i \\ s_i \\ r_i \\ \vdots \\ r_i \end{bmatrix} = \begin{bmatrix} \frac{2}{N}-1 & \frac{2}{N} & \dots & -\frac{2}{N} & \dots & \frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \dots & 1-\frac{2}{N} & \dots & \frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \dots & -\frac{2}{N} & \dots & \frac{2}{N}-1 \end{bmatrix} \begin{bmatrix} r_i \\ \vdots \\ r_i \\ s_i \\ r_i \\ \vdots \\ r_i \end{bmatrix} = \begin{bmatrix} (1-\frac{2}{N})r_i - \frac{2}{N}s_i \\ \vdots \\ (1-\frac{2}{N})r_i - \frac{2}{N}s_i \\ (2-\frac{2}{N})r_i + (1-\frac{2}{N})s_i \\ (1-\frac{2}{N})r_i - \frac{2}{N}s_i \\ \vdots \\ (1-\frac{2}{N})r_i - \frac{2}{N}s_i \end{bmatrix}.$$

$$DT\begin{bmatrix} r_i \\ \vdots \\ r_i \\ s_i \\ r_i \\ \vdots \\ r_i \end{bmatrix} = \begin{bmatrix} \frac{2}{N}-1 & \frac{2}{N} & \dots & -\frac{2}{N} & \dots & \frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \dots & 1-\frac{2}{N} & \dots & \frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \dots & -\frac{2}{N} & \dots & \frac{2}{N}-1 \end{bmatrix} \begin{bmatrix} r_i \\ \vdots \\ r_i \\ s_i \\ r_i \\ \vdots \\ r_i \end{bmatrix} = \begin{bmatrix} (1-\frac{2}{N})r_i - \frac{2}{N}s_i \\ \vdots \\ (1-\frac{2}{N})r_i - \frac{2}{N}s_i \\ (2-\frac{2}{N})r_i + (1-\frac{2}{N})s_i \\ (1-\frac{2}{N})r_i - \frac{2}{N}s_i \\ \vdots \\ (1-\frac{2}{N})r_i - \frac{2}{N}s_i \end{bmatrix}.$$

Итак, $r_{i+1} = (1-\dfrac{2}{N})r_i - \dfrac{2}{N}s_i$, а $s_{i+1} = (2-\dfrac{2}{N})r_i + (1-\dfrac{2}{N})s_i$. При этом $(N-1)r_{i+1}^2 + s_{i+1}^2 = (N-1)r_i^2 + s_i^2$, ибо умножение на DT сохраняет длину.

$$DT\begin{bmatrix} r_i \\ \vdots \\ r_i \\ s_i \\ r_i \\ \vdots \\ r_i \end{bmatrix} = \begin{bmatrix} \frac{2}{N}-1 & \frac{2}{N} & \dots & -\frac{2}{N} & \dots & \frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \dots & 1-\frac{2}{N} & \dots & \frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \dots & -\frac{2}{N} & \dots & \frac{2}{N}-1 \end{bmatrix} \begin{bmatrix} r_i \\ \vdots \\ r_i \\ s_i \\ r_i \\ \vdots \\ r_i \end{bmatrix} = \begin{bmatrix} (1-\frac{2}{N})r_i - \frac{2}{N}s_i \\ \vdots \\ (1-\frac{2}{N})r_i - \frac{2}{N}s_i \\ (2-\frac{2}{N})r_i + (1-\frac{2}{N})s_i \\ (1-\frac{2}{N})r_i - \frac{2}{N}s_i \\ \vdots \\ (1-\frac{2}{N})r_i - \frac{2}{N}s_i \end{bmatrix}.$$

Итак, $r_{i+1} = (1-\dfrac{2}{N})r_i - \dfrac{2}{N}s_i$, а $s_{i+1} = (2-\dfrac{2}{N})r_i + (1-\dfrac{2}{N})s_i$. При этом $(N-1)r_{i+1}^2 + s_{i+1}^2 = (N-1)r_i^2 + s_i^2$, ибо умножение на DT сохраняет длину. Сделаем замену $a_i := \sqrt{N-1}r_i$, $b_i := s_i$. Тогда $a_i^2 + b_i^2 = a_{i+1}^2 + b_{i+1}^2 = 1$

и $\begin{cases} a_{i+1} &= (1-\dfrac{2}{N})a_i - \dfrac{2\sqrt{N-1}}{N}b_i = a_i\cos\theta - b_i\sin\theta \\ b_{i+1} &= \dfrac{2\sqrt{N-1}}{N}a_i + (1-\dfrac{2}{N})b_i = a_i\sin\theta + b_i\cos\theta \end{cases}$ для некоторого θ.

$$DT\begin{bmatrix} r_i \\ \vdots \\ r_i \\ s_i \\ r_i \\ \vdots \\ r_i \end{bmatrix} = \begin{bmatrix} \frac{2}{N}-1 & \frac{2}{N} & \dots & -\frac{2}{N} & \dots & \frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \dots & 1-\frac{2}{N} & \dots & \frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \dots & -\frac{2}{N} & \dots & \frac{2}{N}-1 \end{bmatrix} \begin{bmatrix} r_i \\ \vdots \\ r_i \\ s_i \\ r_i \\ \vdots \\ r_i \end{bmatrix} = \begin{bmatrix} (1-\frac{2}{N})r_i - \frac{2}{N}s_i \\ \vdots \\ (1-\frac{2}{N})r_i - \frac{2}{N}s_i \\ (2-\frac{2}{N})r_i + (1-\frac{2}{N})s_i \\ (1-\frac{2}{N})r_i - \frac{2}{N}s_i \\ \vdots \\ (1-\frac{2}{N})r_i - \frac{2}{N}s_i \end{bmatrix}.$$

Итак, $r_{i+1} = (1-\dfrac{2}{N})r_i - \dfrac{2}{N}s_i$, а $s_{i+1} = (2-\dfrac{2}{N})r_i + (1-\dfrac{2}{N})s_i$. При этом $(N-1)r_{i+1}^2 + s_{i+1}^2 = (N-1)r_i^2 + s_i^2$, ибо умножение на DT сохраняет длину. Сделаем замену $a_i := \sqrt{N-1}r_i$, $b_i := s_i$. Тогда $a_i^2 + b_i^2 = a_{i+1}^2 + b_{i+1}^2 = 1$ и

$$\begin{cases} a_{i+1} &= (1-\dfrac{2}{N})a_i - \dfrac{2\sqrt{N-1}}{N}b_i = a_i\cos\theta - b_i\sin\theta \\ b_{i+1} &= \dfrac{2\sqrt{N-1}}{N}a_i + (1-\dfrac{2}{N})b_i = a_i\sin\theta + b_i\cos\theta \end{cases}$$

для некоторого θ.

Итак, точки (a_i, b_i) и (a_{i+1}, b_{i+1}) лежат на единичной окружности и вторая получается из первой поворотом на угол θ против часовой стрелки.

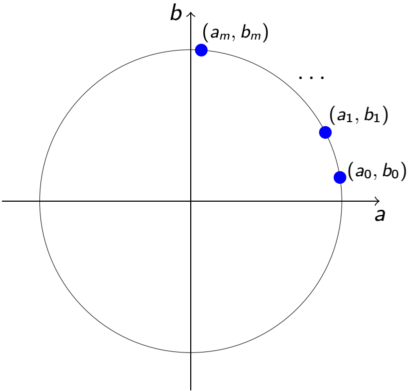
Поскольку $r_0 = s_0 = \dfrac{1}{\sqrt{N}}$, имеем $a_0 = \dfrac{\sqrt{N-1}}{\sqrt{N}}$, а $b_0 = \dfrac{1}{\sqrt{N}}$.

Поскольку $r_0 = s_0 = \dfrac{1}{\sqrt{N}}$, имеем $a_0 = \dfrac{\sqrt{N-1}}{\sqrt{N}}$, а $b_0 = \dfrac{1}{\sqrt{N}}$.

Отсюда точка (a_0, b_0) на единичной окружности соответствует углу $\dfrac{\theta}{2}$.

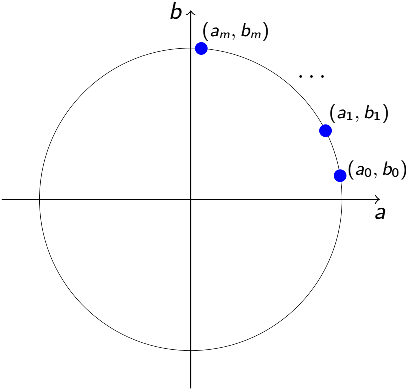
Поскольку $r_0 = s_0 = \dfrac{1}{\sqrt{N}}$, имеем $a_0 = \dfrac{\sqrt{N-1}}{\sqrt{N}}$, а $b_0 = \dfrac{1}{\sqrt{N}}$.

Отсюда точка (a_0, b_0) на единичной окружности соответствует углу $\dfrac{\theta}{2}$.



Поскольку $r_0 = s_0 = \dfrac{1}{\sqrt{N}}$, имеем $a_0 = \dfrac{\sqrt{N-1}}{\sqrt{N}}$, а $b_0 = \dfrac{1}{\sqrt{N}}$.

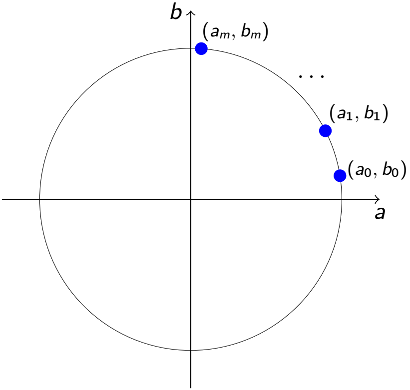
Отсюда точка (a_0, b_0) на единичной окружности соответствует углу $\dfrac{\theta}{2}$.



Точка (a_m, b_m) отвечает углу $m\theta + \dfrac{\theta}{2}$.

Поскольку $r_0 = s_0 = \dfrac{1}{\sqrt{N}}$, имеем $a_0 = \dfrac{\sqrt{N-1}}{\sqrt{N}}$, а $b_0 = \dfrac{1}{\sqrt{N}}$.

Отсюда точка (a_0, b_0) на единичной окружности соответствует углу $\dfrac{\theta}{2}$.



Точка (a_m, b_m) отвечает углу $m\theta + \dfrac{\theta}{2}$. Ищем m из уравнения $m\theta + \dfrac{\theta}{2} \approx \dfrac{\pi}{2}$.

Решая уравнение $m\theta + \dfrac{\theta}{2} \approx \dfrac{\pi}{2}$, находим $m \approx \dfrac{\pi}{2\theta} - \dfrac{1}{2}$.

Решая уравнение $m\theta + \frac{\theta}{2} \approx \frac{\pi}{2}$, находим $m \approx \frac{\pi}{2\theta} - \frac{1}{2}$.

Угол θ ищем из равенства $\cos\theta = 1 - \frac{2}{N}$. Если N велико, то угол θ мал и $\cos\theta \approx 1 - \frac{\theta^2}{2}$.

Алгоритм Гровера: число итераций

Решая уравнение $m\theta + \dfrac{\theta}{2} \approx \dfrac{\pi}{2}$, находим $m \approx \dfrac{\pi}{2\theta} - \dfrac{1}{2}$.

Угол θ ищем из равенства $\cos\theta = 1 - \dfrac{2}{N}$. Если N велико, то угол θ мал и $\cos\theta \approx 1 - \dfrac{\theta^2}{2}$. Отсюда $\theta^2 \approx \dfrac{4}{N}$ и $\theta \approx \dfrac{2}{\sqrt{N}}$.

Решая уравнение $m\theta + \frac{\theta}{2} \approx \frac{\pi}{2}$, находим $m \approx \frac{\pi}{2\theta} - \frac{1}{2}$.

Угол θ ищем из равенства $\cos\theta = 1 - \frac{2}{N}$. Если N велико, то угол θ мал и $\cos\theta \approx 1 - \frac{\theta^2}{2}$. Отсюда $\theta^2 \approx \frac{4}{N}$ и $\theta \approx \frac{2}{\sqrt{N}}$. Итак, $m \approx \frac{\pi}{2\theta} - \frac{1}{2} \approx \frac{\pi\sqrt{N}}{4} - \frac{1}{2}$.

Мы вывели формулу для оптимального числа итераций $m \approx \frac{\pi\sqrt{N}}{4} - \frac{1}{2}$.

Алгоритм Гровера: число итераций

Решая уравнение $m\theta + \frac{\theta}{2} \approx \frac{\pi}{2}$, находим $m \approx \frac{\pi}{2\theta} - \frac{1}{2}$.

Угол θ ищем из равенства $\cos\theta = 1 - \frac{2}{N}$. Если N велико, то угол θ мал и $\cos\theta \approx 1 - \frac{\theta^2}{2}$. Отсюда $\theta^2 \approx \frac{4}{N}$ и $\theta \approx \frac{2}{\sqrt{N}}$. Итак, $m \approx \frac{\pi}{2\theta} - \frac{1}{2} \approx \frac{\pi\sqrt{N}}{4} - \frac{1}{2}$.

Мы вывели формулу для оптимального числа итераций $m \approx \frac{\pi\sqrt{N}}{4} - \frac{1}{2}$. Видно, что алгоритм Гровера дает существенное ускорение, но не является полиномиальным от n.

Решая уравнение $m\theta + \frac{\theta}{2} \approx \frac{\pi}{2}$, находим $m \approx \frac{\pi}{2\theta} - \frac{1}{2}$.

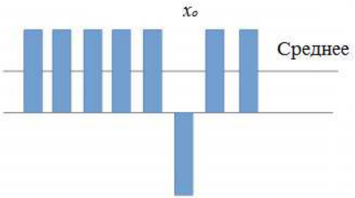
Угол θ ищем из равенства $\cos\theta = 1 - \frac{2}{N}$. Если N велико, то угол θ мал и $\cos\theta \approx 1 - \frac{\theta^2}{2}$. Отсюда $\theta^2 \approx \frac{4}{N}$ и $\theta \approx \frac{2}{\sqrt{N}}$. Итак, $m \approx \frac{\pi}{2\theta} - \frac{1}{2} \approx \frac{\pi\sqrt{N}}{4} - \frac{1}{2}$.

Мы вывели формулу для оптимального числа итераций $m \approx \frac{\pi\sqrt{N}}{4} - \frac{1}{2}$. Видно, что алгоритм Гровера дает существенное ускорение, но не является полиномиальным от n.

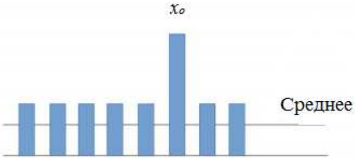
Известно, что алгоритм Гровера оптимален в следующем смысле:

- большее квантовое ускорение, чем квадратичное, невозможно (Беннет, Берштейн, Брассар и Вазирани, 1997);
- константу $\frac{\pi}{4}$ нельзя улучшить (Залка, 1999).

Наглядно (но нестрого) алгоритм Гровера объясняют с помощью такой картинки, поясняющей смысл операторов T и D:



Оператор *T* умножает нужный коэффициент на -1



Оператор *D* отражает все коэффициенты относительно их среднего значения