

Квантовые алгоритмы: возможности и ограничения.

Лекция 3: Сложность булевых функций в модели запросов

М. Вялый

Вычислительный центр
им. А.А.Дородницына
Российской Академии наук

Санкт-Петербург, 2011

- 1 Определения и основные результаты
- 2 Квантовое вычисление дизъюнкции
- 3 Вероятностное вычисление дизъюнкции: нижняя оценка
- 4 Степень многочлена, приближающего булеву функцию

Три вида запросов

Булева функция $x \mapsto f(x)$, $x \in \{0,1\}^n$, $f(x) \in \{0,1\}$.

Классический запрос

Посылаем k , $1 \leq k \leq n$.

Получаем x_k .

Вероятностный запрос

Посылаем k , выбранное по некоторому вероятностному распределению (p_k) .

Получаем x_k .

Квантовый запрос

Оператор $O_x: |k, b\rangle \mapsto |k, b \oplus x_k\rangle$ (общий случай) или фазовый запрос $O_x: |k\rangle \mapsto (-1)^{x_k} |k\rangle$.

Три вида запросов

Булева функция $x \mapsto f(x)$, $x \in \{0,1\}^n$, $f(x) \in \{0,1\}$.

Классический запрос

Посылаем k , $1 \leq k \leq n$.

Получаем x_k .

Вероятностный запрос

Посылаем k , выбранное по некоторому вероятностному распределению (p_k) .

Получаем x_k .

Квантовый запрос

Оператор $O_x: |k, b\rangle \mapsto |k, b \oplus x_k\rangle$ (общий случай) или фазовый запрос $O_x: |k\rangle \mapsto (-1)^{x_k} |k\rangle$.

Три вида запросов

Булева функция $x \mapsto f(x)$, $x \in \{0,1\}^n$, $f(x) \in \{0,1\}$.

Классический запрос

Посылаем k , $1 \leq k \leq n$.

Получаем x_k .

Вероятностный запрос

Посылаем k , выбранное по некоторому вероятностному распределению (p_k) .

Получаем x_k .

Квантовый запрос

Оператор $O_x: |k, b\rangle \mapsto |k, b \oplus x_k\rangle$ (общий случай) или фазовый запрос $O_x: |k\rangle \mapsto (-1)^{x_k} |k\rangle$.

Три вида запросов

Булева функция $x \mapsto f(x)$, $x \in \{0,1\}^n$, $f(x) \in \{0,1\}$.

Классический запрос

Посылаем k , $1 \leq k \leq n$.

Получаем x_k .

Вероятностный запрос

Посылаем k , выбранное по некоторому вероятностному распределению (p_k) .

Получаем x_k .

Квантовый запрос

Оператор $O_x: |k, b\rangle \mapsto |k, b \oplus x_k\rangle$ (общий случай) или фазовый запрос $O_x: |k\rangle \mapsto (-1)^{x_k} |k\rangle$.

Формулировка задачи

Задача(-и) вычисления булевой функции f

Дано: «Черный ящик», который выдает значения переменных из некоторого набора $(x_1, \dots, x_n)$.

Найти: значение $f(x)$.

Сложность алгоритма: количество запросов.

Вероятность ошибки: меньше $1/3$.

Определения

$D(f)$ — минимальная сложность алгоритма вычисления f по классическим запросам.

$R_{1/3}(f)$ — минимальная сложность алгоритма вычисления f по вероятностным запросам.

$Q_{1/3}(f)$ — минимальная сложность алгоритма вычисления f по квантовым запросам.

Формулировка задачи

Задача(-и) вычисления булевой функции f

Дано: «Черный ящик», который выдает значения переменных из некоторого набора $(x_1, \dots, x_n)$.

Найти: значение $f(x)$.

Сложность алгоритма: количество запросов.

Вероятность ошибки: меньше $1/3$.

Определения

$D(f)$ — минимальная сложность алгоритма вычисления f по классическим запросам.

$R_{1/3}(f)$ — минимальная сложность алгоритма вычисления f по вероятностным запросам.

$Q_{1/3}(f)$ — минимальная сложность алгоритма вычисления f по квантовым запросам.

Полиномиальная эквивалентность между сложностями

Теорема

Для любой **всюду определенной** булевой функции f

$$Q_{1/3}(f) \leq R_{1/3}(f) \leq D(f) = O(Q_{1/3}(f)^6).$$

Наилучший известный разрыв

Для дизъюнкции $OR = x_1 \vee x_2 \vee \dots \vee x_n$ выполняется

$$Q_{1/3}(OR) = O(\sqrt{n}); \quad R_{1/3}(OR) = \Omega(n); \quad D(OR) = n.$$

Открытая проблема

Какова точная величина разрыва между сложностями?

Полиномиальная эквивалентность между сложностями

Теорема

Для любой **всюду определенной** булевой функции f

$$Q_{1/3}(f) \leq R_{1/3}(f) \leq D(f) = O(Q_{1/3}(f)^6).$$

Наилучший известный разрыв

Для дизъюнкции $OR = x_1 \vee x_2 \vee \dots \vee x_n$ выполняется

$$Q_{1/3}(OR) = O(\sqrt{n}); \quad R_{1/3}(OR) = \Omega(n); \quad D(OR) = n.$$

Открытая проблема

Какова точная величина разрыва между сложностями?

Полиномиальная эквивалентность между сложностями

Теорема

Для любой **всюду определенной** булевой функции f

$$Q_{1/3}(f) \leq R_{1/3}(f) \leq D(f) = O(Q_{1/3}(f)^6).$$

Наилучший известный разрыв

Для дизъюнкции $OR = x_1 \vee x_2 \vee \dots \vee x_n$ выполняется

$$Q_{1/3}(OR) = O(\sqrt{n}); \quad R_{1/3}(OR) = \Omega(n); \quad D(OR) = n.$$

Открытая проблема

Какова точная величина разрыва между сложностями?

$$Q_{1/3}(f) \leq R_{1/3}(f) \leq D(f)$$

Классический алгоритм — это вероятностный, который использует только детерминированные распределения (одна из вероятностей равна 1).

Вероятностные и детерминированные запросы можно моделировать квантовыми, как уже объяснялось.

$$D(OR) = n$$

Дизъюнкция от нулевого набора равна 0, а от остальных — 1. Если сделать меньше n запросов противник даст нулевые ответы и затем обмануть алгоритм.

$$Q_{1/3}(f) \leq R_{1/3}(f) \leq D(f)$$

Классический алгоритм — это вероятностный, который использует только детерминированные распределения (одна из вероятностей равна 1).

Вероятностные и детерминированные запросы можно моделировать квантовыми, как уже объяснялось.

$$D(OR) = n$$

Дизъюнкция от нулевого набора равна 0, а от остальных — 1. Если сделать меньше n запросов противник даст нулевые ответы и затем обмануть алгоритм.

- 1 Определения и основные результаты
- 2 Квантовое вычисление дизъюнкции
- 3 Вероятностное вычисление дизъюнкции: нижняя оценка
- 4 Степень многочлена, приближающего булеву функцию

Квантовое вычисление дизъюнкции

Модификация алгоритма Гровера обеспечит вычисление дизъюнкции за $O(\sqrt{n})$ квантовых запросов.

Аналогично предыдущим случаям, попробуем фазовый запрос

$$O_x: |k\rangle \mapsto (-1)^{x_k} |k\rangle.$$

Будем применять итерацию Гровера $G = R_\psi O_x$, начиная с вектора $|\psi\rangle$.
Здесь, как и раньше

$$R_\psi = 2|\psi\rangle\langle\psi| - I.$$

Квантовое вычисление дизъюнкции

Модификация алгоритма Гровера обеспечит вычисление дизъюнкции за $O(\sqrt{n})$ квантовых запросов.

Аналогично предыдущим случаям, попробуем фазовый запрос

$$O_x: |k\rangle \mapsto (-1)^{x_k} |k\rangle.$$

Будем применять итерацию Гровера $G = R_\psi O_x$, начиная с вектора $|\psi\rangle$.
Здесь, как и раньше

$$R_\psi = 2|\psi\rangle\langle\psi| - I.$$

Квантовое вычисление дизъюнкции

Модификация алгоритма Гровера обеспечит вычисление дизъюнкции за $O(\sqrt{n})$ квантовых запросов.

Аналогично предыдущим случаям, попробуем фазовый запрос

$$O_x: |k\rangle \mapsto (-1)^{x_k} |k\rangle.$$

Будем применять итерацию Гровера $G = R_\psi O_x$, начиная с вектора $|\psi\rangle$.
Здесь, как и раньше

$$R_\psi = 2|\psi\rangle\langle\psi| - I.$$

Инвариантное двумерное подпространство

$$G: \mathbb{C}(|\psi\rangle, |\xi\rangle) \rightarrow \mathbb{C}(|\psi\rangle, |\xi\rangle)$$

$$|\xi\rangle = \frac{1}{\sqrt{h}} \sum_{k: x_k=1} |k\rangle$$

Проверим:

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{n}} \sum_{k: x_k=1} |k\rangle + \frac{1}{\sqrt{n}} \sum_{k: x_k=0} |k\rangle = \\ &= \sqrt{\frac{h}{n}} |\xi\rangle + \sqrt{\frac{n-h}{n}} \frac{1}{\sqrt{n-h}} \sum_{k: x_k=0} |k\rangle = \sqrt{\frac{h}{n}} |\xi\rangle + \sqrt{\frac{n-h}{n}} |\eta\rangle \end{aligned}$$

$$O_x |\xi\rangle = -|\xi\rangle$$

$$O_x |\eta\rangle = |\eta\rangle$$

Инвариантное двумерное подпространство

$$G: \mathbb{C}(|\psi\rangle, |\xi\rangle) \rightarrow \mathbb{C}(|\psi\rangle, |\xi\rangle)$$

$$|\xi\rangle = \frac{1}{\sqrt{h}} \sum_{k: x_k=1} |k\rangle$$

Проверим:

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{n}} \sum_{k: x_k=1} |k\rangle + \frac{1}{\sqrt{n}} \sum_{k: x_k=0} |k\rangle = \\ &= \sqrt{\frac{h}{n}} |\xi\rangle + \sqrt{\frac{n-h}{n}} \frac{1}{\sqrt{n-h}} \sum_{k: x_k=0} |k\rangle = \sqrt{\frac{h}{n}} |\xi\rangle + \sqrt{\frac{n-h}{n}} |\eta\rangle \end{aligned}$$

$$O_x |\xi\rangle = -|\xi\rangle$$

$$O_x |\eta\rangle = |\eta\rangle$$

Инвариантное двумерное подпространство

$$G: \mathbb{C}(|\psi\rangle, |\xi\rangle) \rightarrow \mathbb{C}(|\psi\rangle, |\xi\rangle)$$

$$|\xi\rangle = \frac{1}{\sqrt{h}} \sum_{k: x_k=1} |k\rangle$$

Проверим:

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{n}} \sum_{k: x_k=1} |k\rangle + \frac{1}{\sqrt{n}} \sum_{k: x_k=0} |k\rangle = \\ &= \sqrt{\frac{h}{n}} |\xi\rangle + \sqrt{\frac{n-h}{n}} \frac{1}{\sqrt{n-h}} \sum_{k: x_k=0} |k\rangle = \sqrt{\frac{h}{n}} |\xi\rangle + \sqrt{\frac{n-h}{n}} |\eta\rangle \end{aligned}$$

$$O_x |\xi\rangle = -|\xi\rangle$$

$$O_x |\eta\rangle = |\eta\rangle$$

Инвариантное двумерное подпространство

$$G: \mathbb{C}(|\psi\rangle, |\xi\rangle) \rightarrow \mathbb{C}(|\psi\rangle, |\xi\rangle)$$

$$|\xi\rangle = \frac{1}{\sqrt{h}} \sum_{k: x_k=1} |k\rangle$$

Проверим:

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{n}} \sum_{k: x_k=1} |k\rangle + \frac{1}{\sqrt{n}} \sum_{k: x_k=0} |k\rangle = \\ &= \sqrt{\frac{h}{n}} |\xi\rangle + \sqrt{\frac{n-h}{n}} \frac{1}{\sqrt{n-h}} \sum_{k: x_k=0} |k\rangle = \sqrt{\frac{h}{n}} |\xi\rangle + \sqrt{\frac{n-h}{n}} |\eta\rangle \end{aligned}$$

$$O_x |\xi\rangle = -|\xi\rangle$$

$$O_x |\eta\rangle = |\eta\rangle$$

Инвариантное двумерное подпространство

$$G: \mathbb{C}(|\psi\rangle, |\xi\rangle) \rightarrow \mathbb{C}(|\psi\rangle, |\xi\rangle)$$

$$|\xi\rangle = \frac{1}{\sqrt{h}} \sum_{k: x_k=1} |k\rangle$$

Проверим:

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{n}} \sum_{k: x_k=1} |k\rangle + \frac{1}{\sqrt{n}} \sum_{k: x_k=0} |k\rangle = \\ &= \sqrt{\frac{h}{n}} |\xi\rangle + \sqrt{\frac{n-h}{n}} \frac{1}{\sqrt{n-h}} \sum_{k: x_k=0} |k\rangle = \sqrt{\frac{h}{n}} |\xi\rangle + \sqrt{\frac{n-h}{n}} |\eta\rangle \end{aligned}$$

$$O_x |\xi\rangle = -|\xi\rangle$$

$$O_x |\eta\rangle = |\eta\rangle$$

Инвариантное двумерное подпространство

$$G: \mathbb{C}(|\psi\rangle, |\xi\rangle) \rightarrow \mathbb{C}(|\psi\rangle, |\xi\rangle)$$

$$|\xi\rangle = \frac{1}{\sqrt{h}} \sum_{k: x_k=1} |k\rangle$$

Проверим:

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{n}} \sum_{k: x_k=1} |k\rangle + \frac{1}{\sqrt{n}} \sum_{k: x_k=0} |k\rangle = \\ &= \sqrt{\frac{h}{n}} |\xi\rangle + \sqrt{\frac{n-h}{n}} \frac{1}{\sqrt{n-h}} \sum_{k: x_k=0} |k\rangle = \sqrt{\frac{h}{n}} |\xi\rangle + \sqrt{\frac{n-h}{n}} |\eta\rangle \end{aligned}$$

$$O_x |\xi\rangle = -|\xi\rangle$$

$$O_x |\eta\rangle = |\eta\rangle$$

Инвариантное двумерное подпространство

$$G: \mathbb{C}(|\psi\rangle, |\xi\rangle) \rightarrow \mathbb{C}(|\psi\rangle, |\xi\rangle)$$

$$|\xi\rangle = \frac{1}{\sqrt{h}} \sum_{k: x_k=1} |k\rangle$$

Проверим:

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{n}} \sum_{k: x_k=1} |k\rangle + \frac{1}{\sqrt{n}} \sum_{k: x_k=0} |k\rangle = \\ &= \sqrt{\frac{h}{n}} |\xi\rangle + \sqrt{\frac{n-h}{n}} \frac{1}{\sqrt{n-h}} \sum_{k: x_k=0} |k\rangle = \sqrt{\frac{h}{n}} |\xi\rangle + \sqrt{\frac{n-h}{n}} |\eta\rangle \end{aligned}$$

$$O_x |\xi\rangle = -|\xi\rangle$$

$$O_x |\eta\rangle = |\eta\rangle$$

$$\sin \vartheta = \langle \psi | \xi \rangle = h \frac{1}{\sqrt{n}} \frac{1}{\sqrt{h}} = \sqrt{\frac{h}{n}}$$

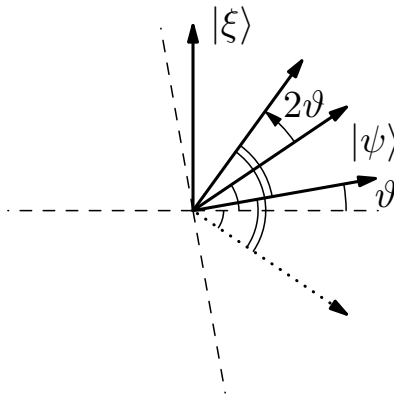


Схема алгоритма

Количество итераций зависит от числа единиц. Оно нам неизвестно. Будем выбирать случайно.

Алгоритм Q_V :

- ❶ Повторить следующие действия 5 раз:
 - (а) выбрать номер переменной k по равномерному распределению на $[1; n]$;
 - (b) запросить x_k ;
 - (с) если $x_k = 1$, то завершить алгоритм с результатом 1.
- ❷ Положить $m = \sqrt{n}$.
- ❸ Выбрать t по равномерному распределению на $[0; m - 1]$;
- ❹ Приготовить состояние $|\psi\rangle$.
- ❺ Выполнить t итераций Гровера.
- ❻ Измерить полученное состояние, результат обозначим k .
- ❼ Закончить работу с результатом x_k .

Схема алгоритма

Количество итераций зависит от числа единиц. Оно нам неизвестно. Будем выбирать случайно.

Алгоритм Q_V :

- 1 Повторить следующие действия 5 раз:
 - (a) выбрать номер переменной k по равномерному распределению на $[1; n]$;
 - (b) запросить x_k ;
 - (c) если $x_k = 1$, то завершить алгоритм с результатом 1.
- 2 Положить $m = \sqrt{n}$.
- 3 Выбрать t по равномерному распределению на $[0; m - 1]$;
- 4 Приготовить состояние $|\psi\rangle$.
- 5 Выполнить t итераций Гровера.
- 6 Измерить полученное состояние, результат обозначим k .
- 7 Закончить работу с результатом x_k .

Схема алгоритма

Количество итераций зависит от числа единиц. Оно нам неизвестно. Будем выбирать случайно.

Алгоритм Q_V :

- 1 Повторить следующие действия 5 раз:
 - (a) выбрать номер переменной k по равномерному распределению на $[1; n]$;
 - (b) запросить x_k ;
 - (c) если $x_k = 1$, то завершить алгоритм с результатом 1.
- 2 Положить $m = \sqrt{n}$.
- 3 Выбрать t по равномерному распределению на $[0; m - 1]$;
- 4 Приготовить состояние $|\psi\rangle$.
- 5 Выполнить t итераций Гровера.
- 6 Измерить полученное состояние, результат обозначим k .
- 7 Закончить работу с результатом x_k .

Схема алгоритма

Количество итераций зависит от числа единиц. Оно нам неизвестно. Будем выбирать случайно.

Алгоритм Q_V :

- 1 Повторить следующие действия 5 раз:
 - (a) выбрать номер переменной k по равномерному распределению на $[1; n]$;
 - (b) запросить x_k ;
 - (c) если $x_k = 1$, то завершить алгоритм с результатом 1.
- 2 Положить $m = \sqrt{n}$.
- 3 Выбрать t по равномерному распределению на $[0; m - 1]$;
- 4 Приготовить состояние $|\psi\rangle$.
- 5 Выполнить t итераций Гровера.
- 6 Измерить полученное состояние, результат обозначим k .
- 7 Закончить работу с результатом x_k .

Схема алгоритма

Количество итераций зависит от числа единиц. Оно нам неизвестно. Будем выбирать случайно.

Алгоритм Q_V :

- ❶ Повторить следующие действия 5 раз:
 - (a) выбрать номер переменной k по равномерному распределению на $[1; n]$;
 - (b) запросить x_k ;
 - (c) если $x_k = 1$, то завершить алгоритм с результатом 1.
- ❷ Положить $m = \sqrt{n}$.
- ❸ Выбрать t по равномерному распределению на $[0; m - 1]$;
- ❹ Приготовить состояние $|\psi\rangle$.
- ❺ Выполнить t итераций Гровера.
- ❻ Измерить полученное состояние, результат обозначим k .
- ❼ Закончить работу с результатом x_k .

Схема алгоритма

Количество итераций зависит от числа единиц. Оно нам неизвестно. Будем выбирать случайно.

Алгоритм Q_V :

- 1 Повторить следующие действия 5 раз:
 - (a) выбрать номер переменной k по равномерному распределению на $[1; n]$;
 - (b) запросить x_k ;
 - (c) если $x_k = 1$, то завершить алгоритм с результатом 1.
- 2 Положить $m = \sqrt{n}$.
- 3 Выбрать t по равномерному распределению на $[0; m - 1]$;
- 4 Приготовить состояние $|\psi\rangle$.
- 5 Выполнить t итераций Гровера.
- 6 Измерить полученное состояние, результат обозначим k .
- 7 Закончить работу с результатом x_k .

Схема алгоритма

Количество итераций зависит от числа единиц. Оно нам неизвестно. Будем выбирать случайно.

Алгоритм Q_V :

- 1 Повторить следующие действия 5 раз:
 - (a) выбрать номер переменной k по равномерному распределению на $[1; n]$;
 - (b) запросить x_k ;
 - (c) если $x_k = 1$, то завершить алгоритм с результатом 1.
- 2 Положить $m = \sqrt{n}$.
- 3 Выбрать t по равномерному распределению на $[0; m - 1]$;
- 4 Приготовить состояние $|\psi\rangle$.
- 5 Выполнить t итераций Гровера.
- 6 Измерить полученное состояние, результат обозначим k .
- 7 Закончить работу с результатом x_k .

Схема алгоритма

Количество итераций зависит от числа единиц. Оно нам неизвестно. Будем выбирать случайно.

Алгоритм Q_V :

- ❶ Повторить следующие действия 5 раз:
 - (а) выбрать номер переменной k по равномерному распределению на $[1; n]$;
 - (б) запросить x_k ;
 - (с) если $x_k = 1$, то завершить алгоритм с результатом 1.
- ❷ Положить $m = \sqrt{n}$.
- ❸ Выбрать t по равномерному распределению на $[0; m - 1]$;
- ❹ Приготовить состояние $|\psi\rangle$.
- ❺ Выполнить t итераций Гровера.
- ❻ Измерить полученное состояние, результат обозначим k .
- ❼ Закончить работу с результатом x_k .

Схема алгоритма

Количество итераций зависит от числа единиц. Оно нам неизвестно. Будем выбирать случайно.

Алгоритм Q_V :

- 1 Повторить следующие действия 5 раз:
 - (a) выбрать номер переменной k по равномерному распределению на $[1; n]$;
 - (b) запросить x_k ;
 - (c) если $x_k = 1$, то завершить алгоритм с результатом 1.
- 2 Положить $m = \sqrt{n}$.
- 3 Выбрать t по равномерному распределению на $[0; m - 1]$;
- 4 Приготовить состояние $|\psi\rangle$.
- 5 Выполнить t итераций Гровера.
- 6 Измерить полученное состояние, результат обозначим k .
- 7 Закончить работу с результатом x_k .

Схема алгоритма

Количество итераций зависит от числа единиц. Оно нам неизвестно. Будем выбирать случайно.

Алгоритм Q_V :

- ❶ Повторить следующие действия 5 раз:
 - (а) выбрать номер переменной k по равномерному распределению на $[1; n]$;
 - (б) запросить x_k ;
 - (с) если $x_k = 1$, то завершить алгоритм с результатом 1.
- ❷ Положить $m = \sqrt{n}$.
- ❸ Выбрать t по равномерному распределению на $[0; m - 1]$;
- ❹ Приготовить состояние $|\psi\rangle$.
- ❺ Выполнить t итераций Гровера.
- ❻ Измерить полученное состояние, результат обозначим k .
- ❼ Закончить работу с результатом x_k .

- Количество запросов $O(\sqrt{n})$.
- Если $OR(x) = 0$, то вероятность ошибки 0.

Утверждение

Если $OR(x) = 1$, то вероятность ошибки $< 3/4$.

Повторив алгоритм k раз, сделаем вероятность ошибки $< (3/4)^k$.

Теорема

Существует алгоритм, который вычисляет дизъюнкцию n переменных с вероятностью ошибки ϵ за $O(\sqrt{n \log \epsilon^{-1}})$ квантовых запросов.

Свойства алгоритма

- Количество запросов $O(\sqrt{n})$.
- Если $OR(x) = 0$, то вероятность ошибки 0.

Утверждение

Если $OR(x) = 1$, то вероятность ошибки $< 3/4$.

Повторив алгоритм k раз, сделаем вероятность ошибки $< (3/4)^k$.

Теорема

Существует алгоритм, который вычисляет дизъюнкцию n переменных с вероятностью ошибки ϵ за $O(\sqrt{n \log \epsilon^{-1}})$ квантовых запросов.

- Количество запросов $O(\sqrt{n})$.
- Если $OR(x) = 0$, то вероятность ошибки 0.

Утверждение

Если $OR(x) = 1$, то вероятность ошибки $< 3/4$.

Повторив алгоритм k раз, сделаем вероятность ошибки $< (3/4)^k$.

Теорема

Существует алгоритм, который вычисляет дизъюнкцию n переменных с вероятностью ошибки ϵ за $O(\sqrt{n \log \epsilon^{-1}})$ квантовых запросов.

- Количество запросов $O(\sqrt{n})$.
- Если $OR(x) = 0$, то вероятность ошибки 0.

Утверждение

Если $OR(x) = 1$, то вероятность ошибки $< 3/4$.

Повторив алгоритм k раз, сделаем вероятность ошибки $< (3/4)^k$.

Теорема

Существует алгоритм, который вычисляет дизъюнкцию n переменных с вероятностью ошибки ϵ за $O(\sqrt{n \log \epsilon^{-1}})$ квантовых запросов.

- Количество запросов $O(\sqrt{n})$.
- Если $OR(x) = 0$, то вероятность ошибки 0.

Утверждение

Если $OR(x) = 1$, то вероятность ошибки $< 3/4$.

Повторив алгоритм k раз, сделаем вероятность ошибки $< (3/4)^k$.

Теорема

Существует алгоритм, который вычисляет дизъюнкцию n переменных с вероятностью ошибки ε за $O(\sqrt{n} \log \varepsilon^{-1})$ квантовых запросов.

Оценка вероятности ошибки: два случая

1 Количество единиц велико: $h \geq n/5$.

- Вторая стадия алгоритма потребуется с вероятностью, не превосходящей

$$\left(1 - \frac{1}{5}\right)^5 \approx e^{-1}$$

и вероятность ошибки не больше этой величины.

2 Количество единиц мало: $0 < h < n/5$.

- Второй этап алгоритма не требуется, так как вероятность ошибки не превосходит $1/5$.
- В первом этапе алгоритма, который дает номер перестановки, равный h .

Оценка вероятности ошибки: два случая

① Количество единиц велико: $h \geq n/5$.

- Вторая стадия алгоритма потребуется с вероятностью, не превосходящей

$$\left(1 - \frac{1}{5}\right)^5 \approx e^{-1}$$

и вероятность ошибки не больше этой величины.

② Количество единиц мало: $0 < h < n/5$.

- Будем оценивать вероятность успеха при итерациях Гровера.
Успех: такое измерение, которое дает номер переменной, равной 1.

Оценка вероятности ошибки: два случая

① Количество единиц велико: $h \geq n/5$.

- Вторая стадия алгоритма потребуется с вероятностью, не превосходящей

$$\left(1 - \frac{1}{5}\right)^5 \approx e^{-1}$$

и вероятность ошибки не больше этой величины.

② Количество единиц мало: $0 < h < n/5$.

- Будем оценивать вероятность **успеха** при итерациях Гровера.
Успех: такое измерение, которое дает номер переменной, равной 1.

Оценка вероятности ошибки: два случая

① Количество единиц велико: $h \geq n/5$.

- Вторая стадия алгоритма потребуется с вероятностью, не превосходящей

$$\left(1 - \frac{1}{5}\right)^5 \approx e^{-1}$$

и вероятность ошибки не больше этой величины.

② Количество единиц мало: $0 < h < n/5$.

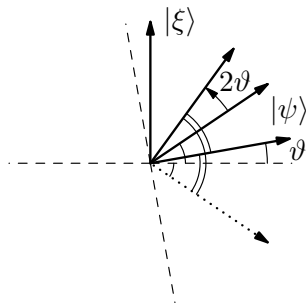
- Будем оценивать вероятность **успеха** при итерациях Гровера.
Успех: такое измерение, которое дает номер переменной, равной 1.

Оценка вероятности успеха для заданного числа итераций

Лемма

Вероятность успеха после t итераций Гровера, начиная с состояния $|\psi\rangle$, равна $\sin^2((2t + 1)\vartheta)$.

Доказательство



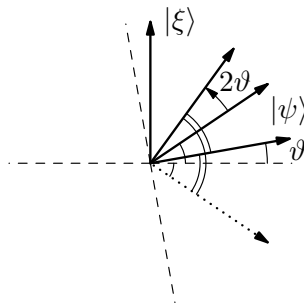
Оценка вероятности успеха для заданного числа итераций

Лемма

Вероятность успеха после t итераций Гровера, начиная с состояния $|\psi\rangle$, равна $\sin^2((2t + 1)\vartheta)$.

Доказательство

- Начальный угол ϑ .



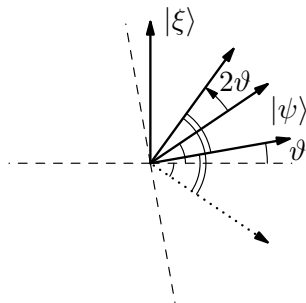
Оценка вероятности успеха для заданного числа итераций

Лемма

Вероятность успеха после t итераций Гровера, начиная с состояния $|\psi\rangle$, равна $\sin^2((2t + 1)\vartheta)$.

Доказательство

- Начальный угол ϑ .
- Каждая итерация поворачивает вектор на угол 2ϑ .



Оценка вероятности успеха для заданного числа итераций

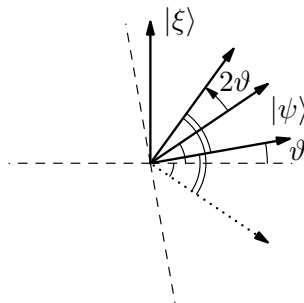
Лемма

Вероятность успеха после t итераций Гровера, начиная с состояния $|\psi\rangle$, равна $\sin^2((2t + 1)\vartheta)$.

Доказательство

- Начальный угол ϑ .
- Каждая итерация поворачивает вектор на угол 2ϑ .
- Координаты вектора после t итераций

$$(\cos((2t + 1)\vartheta), \sin((2t + 1)\vartheta))$$



Оценка вероятности успеха для заданного числа итераций

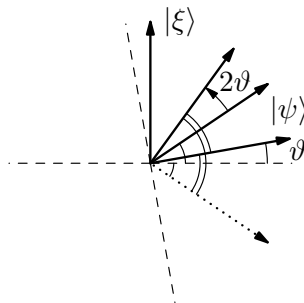
Лемма

Вероятность успеха после t итераций Гровера, начиная с состояния $|\psi\rangle$, равна $\sin^2((2t + 1)\vartheta)$.

Доказательство

- Вероятность успеха — квадрат модуля амплитуды базисного вектора $|\xi\rangle$:

$$\sin^2((2t+1)v\vartheta)$$



Случайный выбор числа итераций

Лемма

Вероятность успеха

$$P_m = \frac{1}{2} - \frac{\sin(4m\vartheta)}{4m \sin(2\vartheta)}.$$

Доказательство

- По формуле полной вероятности

$$P_m = \frac{1}{m} \sum_{j=0}^{m-1} \sin^2((2j+1)\vartheta) = \frac{1}{2m} \sum_{j=0}^{m-1} \left(1 - \cos((2j+1)2\vartheta)\right).$$

- Теперь свернем сумму косинусов, используя формулу

$$\sum_{j=0}^{m-1} \cos((2j+1)\varphi) = \frac{\sin(2m\varphi)}{2 \sin \varphi}.$$

Случайный выбор числа итераций

Лемма

Вероятность успеха

$$P_m = \frac{1}{2} - \frac{\sin(4m\vartheta)}{4m \sin(2\vartheta)}.$$

Доказательство

- По формуле полной вероятности

$$P_m = \frac{1}{m} \sum_{j=0}^{m-1} \sin^2((2j+1)\vartheta) = \frac{1}{2m} \sum_{j=0}^{m-1} \left(1 - \cos((2j+1)2\vartheta)\right).$$

- Теперь свернем сумму косинусов, используя формулу

$$\sum_{j=0}^{m-1} \cos((2j+1)\varphi) = \frac{\sin(2m\varphi)}{2 \sin \varphi}.$$

Вероятность успеха на второй стадии алгоритма

- Из второй леммы

$$P_m = \frac{1}{2} - \frac{\sin(4m\vartheta)}{4m \sin(2\vartheta)}$$

- При $m > 1/\sin(2\vartheta)$ вероятность успеха не меньше $1/4$.
- Если $h < n/5$, то $\sin(2\vartheta) > \sin \vartheta = \sqrt{h/n}$.
- Поэтому

$$\sqrt{n} > \sqrt{\frac{n}{h}} = \frac{1}{\sin \vartheta} > \frac{1}{\sin(2\vartheta)}.$$

- Вероятность успеха не меньше $1/4$.
- Вероятность ошибки меньше $3/4$.

Вероятность успеха на второй стадии алгоритма

- Из второй леммы

$$P_m = \frac{1}{2} - \frac{\sin(4m\vartheta)}{4m \sin(2\vartheta)}$$

- При $m > 1/\sin(2\vartheta)$ вероятность успеха не меньше $1/4$.
- Если $h < n/5$, то $\sin(2\vartheta) > \sin \vartheta = \sqrt{h/n}$.
- Поэтому

$$\sqrt{n} > \sqrt{\frac{n}{h}} = \frac{1}{\sin \vartheta} > \frac{1}{\sin(2\vartheta)}.$$

- Вероятность успеха не меньше $1/4$.
- Вероятность ошибки меньше $3/4$.

Вероятность успеха на второй стадии алгоритма

- Из второй леммы

$$P_m = \frac{1}{2} - \frac{\sin(4m\vartheta)}{4m \sin(2\vartheta)}$$

- При $m > 1/\sin(2\vartheta)$ вероятность успеха не меньше $1/4$.
- Если $h < n/5$, то $\sin(2\vartheta) > \sin \vartheta = \sqrt{h/n}$.
- Поэтому

$$\sqrt{n} > \sqrt{\frac{n}{h}} = \frac{1}{\sin \vartheta} > \frac{1}{\sin(2\vartheta)}.$$

- Вероятность успеха не меньше $1/4$.
- Вероятность ошибки меньше $3/4$.

Вероятность успеха на второй стадии алгоритма

- Из второй леммы

$$P_m = \frac{1}{2} - \frac{\sin(4m\vartheta)}{4m \sin(2\vartheta)}$$

- При $m > 1/\sin(2\vartheta)$ вероятность успеха не меньше $1/4$.
- Если $h < n/5$, то $\sin(2\vartheta) > \sin \vartheta = \sqrt{h/n}$.
- Поэтому

$$\sqrt{n} > \sqrt{\frac{n}{h}} = \frac{1}{\sin \vartheta} > \frac{1}{\sin(2\vartheta)}.$$

- Вероятность успеха не меньше $1/4$.
- Вероятность ошибки меньше $3/4$.

Вероятность успеха на второй стадии алгоритма

- Из второй леммы

$$P_m = \frac{1}{2} - \frac{\sin(4m\vartheta)}{4m \sin(2\vartheta)}$$

- При $m > 1/\sin(2\vartheta)$ вероятность успеха не меньше $1/4$.
- Если $h < n/5$, то $\sin(2\vartheta) > \sin \vartheta = \sqrt{h/n}$.
- Поэтому

$$\sqrt{n} > \sqrt{\frac{n}{h}} = \frac{1}{\sin \vartheta} > \frac{1}{\sin(2\vartheta)}.$$

- Вероятность успеха не меньше $1/4$.
- Вероятность ошибки меньше $3/4$.

Вероятность успеха на второй стадии алгоритма

- Из второй леммы

$$P_m = \frac{1}{2} - \frac{\sin(4m\vartheta)}{4m \sin(2\vartheta)}$$

- При $m > 1/\sin(2\vartheta)$ вероятность успеха не меньше $1/4$.
- Если $h < n/5$, то $\sin(2\vartheta) > \sin \vartheta = \sqrt{h/n}$.
- Поэтому

$$\sqrt{n} > \sqrt{\frac{n}{h}} = \frac{1}{\sin \vartheta} > \frac{1}{\sin(2\vartheta)}.$$

- Вероятность успеха не меньше $1/4$.
- Вероятность ошибки меньше $3/4$.

- 1 Определения и основные результаты
- 2 Квантовое вычисление дизъюнкции
- 3 Вероятностное вычисление дизъюнкции: нижняя оценка
- 4 Степень многочлена, приближающего булеву функцию

Определение

Чувствительность $s_x(f)$ функции f в точке x равна количеству переменных x_k , для которых $f(x) \neq f(x \oplus e_k)$. Здесь $e_k = (\underbrace{0, \dots, 0}_{k-1}, 1, 0, \dots, 0)$.

(Сколько соседей на булевом кубе имеют другое значение функции.)

Чувствительность $s(f)$ функции f равна $\max_x s_x(f)$.

Пример

$s(OR) = n$, так как $s_{0^n}(OR) = n$ (у всех соседей точки 0^n значение 1, а у самой точки — 0).

Чувствительность

Определение

Чувствительность $s_x(f)$ функции f в точке x равна количеству переменных x_k , для которых $f(x) \neq f(x \oplus e_k)$. Здесь $e_k = (\underbrace{0, \dots, 0}_{k-1}, 1, 0, \dots, 0)$.

(Сколько соседей на булевом кубе имеют другое значение функции.)

Чувствительность $s(f)$ функции f равна $\max_x s_x(f)$.

Пример

$s(OR) = n$, так как $s_{0^n}(OR) = n$ (у всех соседей точки 0^n значение 1, а у самой точки — 0).

Чувствительность

Определение

Чувствительность $s_x(f)$ функции f в точке x равна количеству переменных x_k , для которых $f(x) \neq f(x \oplus e_k)$. Здесь $e_k = (\underbrace{0, \dots, 0}_{k-1}, 1, 0, \dots, 0)$.

(Сколько соседей на булевом кубе имеют другое значение функции.)

Чувствительность $s(f)$ функции f равна $\max_x s_x(f)$.

Пример

$s(OR) = n$, так как $s_{0^n}(OR) = n$ (у всех соседей точки 0^n значение 1, а у самой точки — 0).

Чувствительность

Определение

Чувствительность $s_x(f)$ функции f в точке x равна количеству переменных x_k , для которых $f(x) \neq f(x \oplus e_k)$. Здесь $e_k = (\underbrace{0, \dots, 0}_{k-1}, 1, 0, \dots, 0)$.

(Сколько соседей на булевом кубе имеют другое значение функции.)

Чувствительность $s(f)$ функции f равна $\max_x s_x(f)$.

Пример

$s(OR) = n$, так как $s_{0^n}(OR) = n$ (у всех соседей точки 0^n значение 1, а у самой точки — 0).

Теорема

$$s(f) \leq 3R_{1/3}(f)$$

Доказательство

Аналогично оценке для числа вероятностных запросов в задаче поиска.

Пусть в x достигается максимум $s_x(f) = s$, а $x_1, \dots, x_s$ — соответствующие переменные.

Если алгоритм делает $k \leq s/3$ запросов, то вероятность того, что одна из этих переменных пропущена, не меньше $1/3$.

Но в этом случае противник может **гарантировать** ошибку, так как $f(x) \neq f(x \oplus e_j)$.

Теорема

$$s(f) \leq 3R_{1/3}(f)$$

Доказательство

Аналогично оценке для числа вероятностных запросов в задаче поиска.

Пусть в x достигается максимум $s_x(f) = s$, а $x_1, \dots, x_s$ — соответствующие переменные.

Если алгоритм делает $k \leq s/3$ запросов, то вероятность того, что одна из этих переменных пропущена, не меньше $1/3$.

Но в этом случае противник может **гарантировать** ошибку, так как $f(x) \neq f(x \oplus e_j)$.

Теорема

$$s(f) \leq 3R_{1/3}(f)$$

Доказательство

Аналогично оценке для числа вероятностных запросов в задаче поиска.

Пусть в x достигается максимум $s_x(f) = s$, а $x_1, \dots, x_s$ — соответствующие переменные.

Если алгоритм делает $k \leq s/3$ запросов, то вероятность того, что одна из этих переменных пропущена, не меньше $1/3$.

Но в этом случае противник может **гарантировать** ошибку, так как $f(x) \neq f(x \oplus e_j)$.

Теорема

$$s(f) \leq 3R_{1/3}(f)$$

Доказательство

Аналогично оценке для числа вероятностных запросов в задаче поиска.

Пусть в x достигается максимум $s_x(f) = s$, а $x_1, \dots, x_s$ — соответствующие переменные.

Если алгоритм делает $k \leq s/3$ запросов, то вероятность того, что одна из этих переменных пропущена, не меньше $1/3$.

Но в этом случае противник может **гарантировать** ошибку, так как $f(x) \neq f(x \oplus e_j)$.

Теорема

$$s(f) \leq 3R_{1/3}(f)$$

Доказательство

Аналогично оценке для числа вероятностных запросов в задаче поиска.

Пусть в x достигается максимум $s_x(f) = s$, а $x_1, \dots, x_s$ — соответствующие переменные.

Если алгоритм делает $k \leq s/3$ запросов, то вероятность того, что одна из этих переменных пропущена, не меньше $1/3$.

Но в этом случае противник может **гарантировать** ошибку, так как $f(x) \neq f(x \oplus e_j)$.

- 1 Определения и основные результаты
- 2 Квантовое вычисление дизъюнкции
- 3 Вероятностное вычисление дизъюнкции: нижняя оценка
- 4 Степень многочлена, приближающего булеву функцию

Многочлены и булевы функции

Определения

Многочлен $p: \mathbb{R}^n \rightarrow \mathbb{R}$ **приближает** булеву функцию $f: \{0, 1\}^n \rightarrow \{0, 1\}$, если для любого $x \in \{0, 1\}^n$ выполняется

$$|p(x) - f(x)| < \frac{1}{3}.$$

Степенью (приближения) $\widetilde{\deg}(f)$ булевой функции f называется наименьшая степень многочлена, приближающего f .

Задача

Докажите, что для любой булевой функции f от n переменных существует единственный мультилинейный многочлен p степени не выше n , который точно представляет f : равенство $f(x) = p(x)$ выполняется для всех $x \in \{0, 1\}^n$.

Многочлены и булевы функции

Определения

Многочлен $p: \mathbb{R}^n \rightarrow \mathbb{R}$ **приближает** булеву функцию $f: \{0, 1\}^n \rightarrow \{0, 1\}$, если для любого $x \in \{0, 1\}^n$ выполняется

$$|p(x) - f(x)| < \frac{1}{3}.$$

Степенью (приближения) $\widetilde{\deg}(f)$ булевой функции f называется наименьшая степень многочлена, приближающего f .

Задача

Докажите, что для любой булевой функции f от n переменных существует единственный мультилинейный многочлен p степени не выше n , который точно представляет f : равенство $f(x) = p(x)$ выполняется для всех $x \in \{0, 1\}^n$.

Многочлены и булевы функции

Определения

Многочлен $p: \mathbb{R}^n \rightarrow \mathbb{R}$ **приближает** булеву функцию $f: \{0, 1\}^n \rightarrow \{0, 1\}$, если для любого $x \in \{0, 1\}^n$ выполняется

$$|p(x) - f(x)| < \frac{1}{3}.$$

Степенью (приближения) $\widetilde{\deg}(f)$ булевой функции f называется наименьшая степень многочлена, приближающего f .

Задача

Докажите, что для любой булевой функции f от n переменных существует единственный мультилинейный многочлен p степени не выше n , который точно представляет f : равенство $f(x) = p(x)$ выполняется для всех $x \in \{0, 1\}^n$.

Многочлены и булевы функции

Определения

Многочлен $p: \mathbb{R}^n \rightarrow \mathbb{R}$ **приближает** булеву функцию $f: \{0, 1\}^n \rightarrow \{0, 1\}$, если для любого $x \in \{0, 1\}^n$ выполняется

$$|p(x) - f(x)| < \frac{1}{3}.$$

Степенью (приближения) $\widetilde{\deg}(f)$ булевой функции f называется наименьшая степень многочлена, приближающего f .

Задача

Докажите, что для любой булевой функции f от n переменных существует единственный мультилинейный многочлен p степени не выше n , который точно представляет f : равенство $f(x) = p(x)$ выполняется для всех $x \in \{0, 1\}^n$.

Оценка $Q_{1/3}(f)$ через степень приближения

Теорема

Для любой булевой функции $\widetilde{\deg}(f) \leq 2Q_{1/3}(f)$.

Лемма

Если алгоритм вычисления f делает d квантовых запросов, то состояние его памяти перед финальным измерением имеет вид

$$\sum_{w \in W} \alpha_w(x) |w\rangle,$$

где w — состояния памяти алгоритма, а $\alpha_w(x)$ — (комплексные) многочлены от x степени не выше d .

Оценка $Q_{1/3}(f)$ через степень приближения

Теорема

Для любой булевой функции $\widetilde{\deg}(f) \leq 2Q_{1/3}(f)$.

Лемма

Если алгоритм вычисления f делает d квантовых запросов, то состояние его памяти перед финальным измерением имеет вид

$$\sum_{w \in W} \alpha_w(x) |w\rangle,$$

где w — состояния памяти алгоритма, а $\alpha_w(x)$ — (комплексные) многочлены от x степени не выше d .

Оценка $Q_{1/3}(f)$ через степень приближения

Перед измерением: $\sum_{w \in W} \alpha_w(x) |w\rangle$, $\deg \alpha_w(x) \leq d$.

Вывод теоремы из леммы

Исход w наблюдается при измерении с вероятностью

$$p_w(x) = |\alpha_w(x)|^2.$$

W_1 — множество тех состояний памяти, в которых алгоритм выдает ответ «1». Вероятность ответа 1 равна

$$p_1(x) = \sum_w p_w(x).$$

Это многочлен от x степени $\leq 2d$ и такой, что

- $1 \geq p_1(x) > 2/3$ при $f(x) = 1$;
- $1/3 > p_1(x) \geq 0$ при $f(x) = 0$.

Таким образом, $\widetilde{\deg}(f) \leq \deg p_1(x) \leq 2d$.

Оценка $Q_{1/3}(f)$ через степень приближения

Перед измерением: $\sum_{w \in W} \alpha_w(x) |w\rangle$, $\deg \alpha_w(x) \leq d$.

Вывод теоремы из леммы

Исход w наблюдается при измерении с вероятностью

$$p_w(x) = |\alpha_w(x)|^2.$$

W_1 — множество тех состояний памяти, в которых алгоритм выдает ответ «1». Вероятность ответа 1 равна

$$p_1(x) = \sum_w p_w(x).$$

Это многочлен от x степени $\leq 2d$ и такой, что

- $1 \geq p_1(x) > 2/3$ при $f(x) = 1$;
- $1/3 > p_1(x) \geq 0$ при $f(x) = 0$.

Таким образом, $\widetilde{\deg}(f) \leq \deg p_1(x) \leq 2d$.

Оценка $Q_{1/3}(f)$ через степень приближения

Перед измерением: $\sum_{w \in W} \alpha_w(x) |w\rangle$, $\deg \alpha_w(x) \leq d$.

Вывод теоремы из леммы

Исход w наблюдается при измерении с вероятностью

$$p_w(x) = |\alpha_w(x)|^2.$$

W_1 — множество тех состояний памяти, в которых алгоритм выдает ответ «1». Вероятность ответа 1 равна

$$p_1(x) = \sum_w p_w(x).$$

Это многочлен от x степени $\leq 2d$ и такой, что

- $1 \geq p_1(x) > 2/3$ при $f(x) = 1$;
- $1/3 > p_1(x) \geq 0$ при $f(x) = 0$.

Таким образом, $\widetilde{\deg}(f) \leq \deg p_1(x) \leq 2d$.

Оценка $Q_{1/3}(f)$ через степень приближения

Перед измерением: $\sum_{w \in W} \alpha_w(x) |w\rangle$, $\deg \alpha_w(x) \leq d$.

Вывод теоремы из леммы

Исход w наблюдается при измерении с вероятностью

$$p_w(x) = |\alpha_w(x)|^2.$$

W_1 — множество тех состояний памяти, в которых алгоритм выдает ответ «1». Вероятность ответа 1 равна

$$p_1(x) = \sum_w p_w(x).$$

Это многочлен от x степени $\leq 2d$ и такой, что

- $1 \geq p_1(x) > 2/3$ при $f(x) = 1$;
- $1/3 > p_1(x) \geq 0$ при $f(x) = 0$.

Таким образом, $\widetilde{\deg}(f) \leq \deg p_1(x) \leq 2d$.

Оценка $Q_{1/3}(f)$ через степень приближения

Перед измерением: $\sum_{w \in W} \alpha_w(x) |w\rangle$, $\deg \alpha_w(x) \leq d$.

Вывод теоремы из леммы

Исход w наблюдается при измерении с вероятностью

$$p_w(x) = |\alpha_w(x)|^2.$$

W_1 — множество тех состояний памяти, в которых алгоритм выдает ответ «1». Вероятность ответа 1 равна

$$p_1(x) = \sum_w p_w(x).$$

Это многочлен от x степени $\leq 2d$ и такой, что

- $1 \geq p_1(x) > 2/3$ при $f(x) = 1$;
- $1/3 > p_1(x) \geq 0$ при $f(x) = 0$.

Таким образом, $\widetilde{\deg}(f) \leq \deg p_1(x) \leq 2d$.

$\widetilde{\deg}(f) \leq 2Q_{1/3}(f)$: доказательство леммы

Состояние памяти алгоритма после k запросов:

$$|\psi_k\rangle = U_k O_x U_{k-1} O_x \dots U_1 O_x |\psi_0\rangle.$$

- Доказательство индукцией по k .
- Для $k = 0$ амплитуды не зависят от x , степень 0.
- Применение запроса.

- Унитарное преобразование: новая амплитуда — линейная комбинация старых (коэффициенты от x не зависят). Степень не увеличивается.

$\widetilde{\deg}(f) \leq 2Q_{1/3}(f)$: доказательство леммы

Состояние памяти алгоритма после k запросов:

$$|\psi_k\rangle = U_k O_x U_{k-1} O_x \dots U_1 O_x |\psi_0\rangle.$$

- Доказательство индукцией по k .
- Для $k = 0$ амплитуды не зависят от x , степень 0.
- Применение запроса.

• Было

$$|\psi_k\rangle = \alpha_0 |w, k, 0\rangle + \alpha_1 |w, k, 1\rangle + \dots$$

• Стало

$$|\psi_{k+1}\rangle = U_{k+1} O_x |\psi_k\rangle = \alpha_0' |w, k+1, 0\rangle + \alpha_1' |w, k+1, 1\rangle + \dots$$

• Степень увеличилась, если применили O_x

- Унитарное преобразование: новая амплитуда — линейная комбинация старых (коэффициенты от x не зависят). Степень не увеличивается.

$\widetilde{\deg}(f) \leq 2Q_{1/3}(f)$: доказательство леммы

Состояние памяти алгоритма после k запросов:

$$|\psi_k\rangle = U_k O_x U_{k-1} O_x \dots U_1 O_x |\psi_0\rangle.$$

- Доказательство индукцией по k .
- Для $k = 0$ амплитуды не зависят от x , степень 0.
- Применение запроса.

- Было

$$\dots + \alpha(x)|w, k, 0\rangle + \beta(x)|w, k, 1\rangle + \dots$$

- Стало

$$\dots + (\beta(x)x_k + \alpha(x)(1-x_k))|w, k, 0\rangle + (\alpha(x)x_k + \beta(x)(1-x_k))|w, k, 1\rangle + \dots$$

- Степень увеличилась самое большее на 1.

- Унитарное преобразование: новая амплитуда — линейная комбинация старых (коэффициенты от x не зависят). Степень не увеличивается.

$\widetilde{\deg}(f) \leq 2Q_{1/3}(f)$: доказательство леммы

Состояние памяти алгоритма после k запросов:

$$|\psi_k\rangle = U_k O_x U_{k-1} O_x \dots U_1 O_x |\psi_0\rangle.$$

- Доказательство индукцией по k .
- Для $k = 0$ амплитуды не зависят от x , степень 0.
- Применение запроса.

- Было

$$\dots + \alpha(x)|w, k, 0\rangle + \beta(x)|w, k, 1\rangle + \dots$$

- Стало

$$\dots + (\beta(x)x_k + \alpha(x)(1-x_k))|w, k, 0\rangle + (\alpha(x)x_k + \beta(x)(1-x_k))|w, k, 1\rangle + \dots$$

- Степень увеличилась самое большее на 1.
- Унитарное преобразование: новая амплитуда — линейная комбинация старых (коэффициенты от x не зависят). Степень не увеличивается.

$\widetilde{\deg}(f) \leq 2Q_{1/3}(f)$: доказательство леммы

Состояние памяти алгоритма после k запросов:

$$|\psi_k\rangle = U_k O_x U_{k-1} O_x \dots U_1 O_x |\psi_0\rangle.$$

- Доказательство индукцией по k .
- Для $k = 0$ амплитуды не зависят от x , степень 0.
- Применение запроса.

- Было

$$\dots + \alpha(x)|w, k, 0\rangle + \beta(x)|w, k, 1\rangle + \dots$$

- Стало

$$\dots + (\beta(x)x_k + \alpha(x)(1-x_k))|w, k, 0\rangle + (\alpha(x)x_k + \beta(x)(1-x_k))|w, k, 1\rangle + \dots$$

- Степень увеличилась самое большее на 1.
 - Унитарное преобразование: новая амплитуда — линейная комбинация старых (коэффициенты от x не зависят). Степень не увеличивается.

$\widetilde{\deg}(f) \leq 2Q_{1/3}(f)$: доказательство леммы

Состояние памяти алгоритма после k запросов:

$$|\psi_k\rangle = U_k O_x U_{k-1} O_x \dots U_1 O_x |\psi_0\rangle.$$

- Доказательство индукцией по k .
- Для $k = 0$ амплитуды не зависят от x , степень 0.
- Применение запроса.

- Было

$$\dots + \alpha(x)|w, k, 0\rangle + \beta(x)|w, k, 1\rangle + \dots$$

- Стало

$$\dots + (\beta(x)x_k + \alpha(x)(1-x_k))|w, k, 0\rangle + (\alpha(x)x_k + \beta(x)(1-x_k))|w, k, 1\rangle + \dots$$

- Степень увеличилась самое большее на 1.
- Унитарное преобразование: новая амплитуда — линейная комбинация старых (коэффициенты от x не зависят). Степень не увеличивается.

$\widetilde{\deg}(f) \leq 2Q_{1/3}(f)$: доказательство леммы

Состояние памяти алгоритма после k запросов:

$$|\psi_k\rangle = U_k O_x U_{k-1} O_x \dots U_1 O_x |\psi_0\rangle.$$

- Доказательство индукцией по k .
- Для $k = 0$ амплитуды не зависят от x , степень 0.
- Применение запроса.

- Было

$$\dots + \alpha(x)|w, k, 0\rangle + \beta(x)|w, k, 1\rangle + \dots$$

- Стало

$$\dots + (\beta(x)x_k + \alpha(x)(1-x_k))|w, k, 0\rangle + (\alpha(x)x_k + \beta(x)(1-x_k))|w, k, 1\rangle + \dots$$

- Степень увеличилась самое большее на 1.
- Унитарное преобразование: новая амплитуда — линейная комбинация старых (коэффициенты от x не зависят). Степень не увеличивается.

Насколько хорошо степень приближает $Q_\varepsilon(f)$?

- Амбайнис (2006) построил семейство функций, для которых $\deg(f_k) = 2^k$, а $Q_{1/3}(f) = \Omega(2.5^k)$.
- Для доказательства нижней оценки на квантовую сложность он использовал **метод квантового противника** (Амбайнис, 2002).
- Рейхарт (2010) доказал для одной из версий метода квантового противника, что она дает оценку $Q_\varepsilon(f)$ с точностью до мультипликативной константы.

Насколько хорошо степень приближает $Q_\epsilon(f)$?

- Амбайнис (2006) построил семейство функций, для которых $\deg(f_k) = 2^k$, а $Q_{1/3}(f) = \Omega(2.5^k)$.
- Для доказательства нижней оценки на квантовую сложность он использовал **метод квантового противника** (Амбайнис, 2002).
- Рейхарт (2010) доказал для одной из версий метода квантового противника, что она дает оценку $Q_\epsilon(f)$ с точностью до мультипликативной константы.

Насколько хорошо степень приближает $Q_\varepsilon(f)$?

- Амбайнис (2006) построил семейство функций, для которых $\deg(f_k) = 2^k$, а $Q_{1/3}(f) = \Omega(2.5^k)$.
- Для доказательства нижней оценки на квантовую сложность он использовал **метод квантового противника** (Амбайнис, 2002).
- Рейхарт (2010) доказал для одной из версий метода квантового противника, что она дает оценку $Q_\varepsilon(f)$ с точностью до мультипликативной константы.

Теорема

$$\widetilde{\deg}(OR) \geq \sqrt{n/6}.$$

Доказательство

- $p(x_1, \dots, x_n)$ приближает $OR(x_1, \dots, x_n)$.

- Симметризация многочлена:

$$p^{sym}(x_1, \dots, x_n) = \frac{1}{n!} \sum_{\sigma \in S_n} p(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}).$$

- Специализация

$$\tilde{p}(t) = p^{sym}(t, t, \dots, t).$$

- Свойства специализации

- Отсюда следует

$$\deg p \geq \deg p^{sym} \geq \deg \tilde{p} \geq \sqrt{n/6}.$$

Доказательство

- $p(x_1, \dots, x_n)$ приближает $OR(x_1, \dots, x_n)$.
- Симметризация многочлена:

$$p^{sym}(x_1, \dots, x_n) = \frac{1}{n!} \sum_{\sigma \in S_n} p(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}).$$

- Специализация

$$\tilde{p}(t) = p^{sym}(t, t, \dots, t).$$

- Свойства специализации

$$\deg p \geq \deg p^{sym} \geq \deg \tilde{p} \geq \sqrt{n/6}.$$

- Отсюда следует

$$\deg p \geq \deg p^{sym} \geq \deg \tilde{p} \geq \sqrt{n/6}.$$

Доказательство

- $p(x_1, \dots, x_n)$ приближает $OR(x_1, \dots, x_n)$.
- Симметризация многочлена:

$$p^{sym}(x_1, \dots, x_n) = \frac{1}{n!} \sum_{\sigma \in S_n} p(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}).$$

- Специализация

$$\tilde{p}(t) = p^{sym}(t, t, \dots, t).$$

- Свойства специализации

$$|p(0)| \leq 1/3;$$

$$|p(1)| \leq 1/3;$$

- Отсюда следует

$$\deg p \geq \deg p^{sym} \geq \deg \tilde{p} \geq \sqrt{n/6}.$$

Доказательство

- $p(x_1, \dots, x_n)$ приближает $OR(x_1, \dots, x_n)$.
- Симметризация многочлена:

$$p^{sym}(x_1, \dots, x_n) = \frac{1}{n!} \sum_{\sigma \in S_n} p(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}).$$

- Специализация

$$\tilde{p}(t) = p^{sym}(t, t, \dots, t).$$

- Свойства специализации

- $|\tilde{p}(0)| < 1/3$;
- $|\tilde{p}(k) - 1| < 1/3$ при $1 \leq k \leq n$.

- Отсюда следует

$$\deg p \geq \deg p^{sym} \geq \deg \tilde{p} \geq \sqrt{n/6}.$$

Доказательство

- $p(x_1, \dots, x_n)$ приближает $OR(x_1, \dots, x_n)$.
- Симметризация многочлена:

$$p^{sym}(x_1, \dots, x_n) = \frac{1}{n!} \sum_{\sigma \in S_n} p(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}).$$

- Специализация

$$\tilde{p}(t) = p^{sym}(t, t, \dots, t).$$

- Свойства специализации

- $|\tilde{p}(0)| < 1/3$;
- $|\tilde{p}(k) - 1| < 1/3$ при $1 \leq k \leq n$.
- Отсюда следует

$$\deg p \geq \deg p^{sym} \geq \deg \tilde{p} \geq \sqrt{n/6}.$$

Доказательство

- $p(x_1, \dots, x_n)$ приближает $OR(x_1, \dots, x_n)$.
- Симметризация многочлена:

$$p^{sym}(x_1, \dots, x_n) = \frac{1}{n!} \sum_{\sigma \in S_n} p(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}).$$

- Специализация

$$\tilde{p}(t) = p^{sym}(t, t, \dots, t).$$

- Свойства специализации
 - $|\tilde{p}(0)| < 1/3$;
 - $|\tilde{p}(k) - 1| < 1/3$ при $1 \leq k \leq n$.

- Отсюда следует

$$\deg p \geq \deg p^{sym} \geq \deg \tilde{p} \geq \sqrt{n/6}.$$

Доказательство

- $p(x_1, \dots, x_n)$ приближает $OR(x_1, \dots, x_n)$.
- Симметризация многочлена:

$$p^{sym}(x_1, \dots, x_n) = \frac{1}{n!} \sum_{\sigma \in S_n} p(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}).$$

- Специализация

$$\tilde{p}(t) = p^{sym}(t, t, \dots, t).$$

- Свойства специализации
 - $|\tilde{p}(0)| < 1/3$;
 - $|\tilde{p}(k) - 1| < 1/3$ при $1 \leq k \leq n$.
- Отсюда следует

$$\deg p \geq \deg p^{sym} \geq \deg \tilde{p} \geq \sqrt{n/6}.$$

Теорема (нижняя оценка на степень многочлена)

Пусть $f(x)$ — многочлен и $|f(0)| < 1/3$, $|f(1) - 1| < 1/3$, а $-1/3 < f(k) < 4/3$ при $2 \leq k \leq n$.

Тогда $\deg f \geq \sqrt{n/6}$.

Теорема (Марков, 1889)

Если $|f(x)| \leq 1$ на отрезке $[-1; 1]$, то $|f'(x)| \leq (\deg f)^2$ на отрезке $[-1; 1]$.

Задача

Выведите нижнюю оценку на степень многочлена из неравенства Маркова.

Теорема (нижняя оценка на степень многочлена)

Пусть $f(x)$ — многочлен и $|f(0)| < 1/3$, $|f(1) - 1| < 1/3$, а $-1/3 < f(k) < 4/3$ при $2 \leq k \leq n$.

Тогда $\deg f \geq \sqrt{n/6}$.

Теорема (Марков, 1889)

Если $|f(x)| \leq 1$ на отрезке $[-1; 1]$, то $|f'(x)| \leq (\deg f)^2$ на отрезке $[-1; 1]$.

Задача

Выведите нижнюю оценку на степень многочлена из неравенства Маркова.

Теорема (нижняя оценка на степень многочлена)

Пусть $f(x)$ — многочлен и $|f(0)| < 1/3$, $|f(1) - 1| < 1/3$, а $-1/3 < f(k) < 4/3$ при $2 \leq k \leq n$.

Тогда $\deg f \geq \sqrt{n/6}$.

Теорема (Марков, 1889)

Если $|f(x)| \leq 1$ на отрезке $[-1; 1]$, то $|f'(x)| \leq (\deg f)^2$ на отрезке $[-1; 1]$.

Задача

Выведите нижнюю оценку на степень многочлена из неравенства Маркова.

Теорема (нижняя оценка на степень многочлена)

Пусть $f(x)$ — многочлен и $|f(0)| < 1/3$, $|f(1) - 1| < 1/3$, а $-1/3 < f(k) < 4/3$ при $2 \leq k \leq n$.

Тогда $\deg f \geq \sqrt{n/6}$.

Теорема (Марков, 1889)

Если $|f(x)| \leq 1$ на отрезке $[-1; 1]$, то $|f'(x)| \leq (\deg f)^2$ на отрезке $[-1; 1]$.

Задача

Выведите нижнюю оценку на степень многочлена из неравенства Маркова.

Теорема

$$\frac{1}{\sqrt{24}}\sqrt{n} \leq Q_{1/3}(OR) \leq \sqrt{n}.$$

Зазор между вероятностной и квантовой сложностью

$$\frac{1}{3}\sqrt{n} \leq \frac{R_{1/3}(OR)}{Q_{1/3}(OR)} \leq \sqrt{24}\sqrt{n}$$