Алгоритм Шора, часть III

М. В. Волков

Уральский федеральный университет

Институт естественных наук и математики

кафедра алгебры и фундаментальной информатики

2020/2021 учебный год

Алгоритм Шора: заполнение пробелов

Дано натуральное число N, о котором заранее известно, что оно есть произведение двух простых чисел p и q.

Алгоритм Шора: заполнение пробелов

Дано натуральное число N, о котором заранее известно, что оно есть произведение двух простых чисел p и q. Требуется найти p и q за время, полиномиальное *от длины записи* числа N, т.е. от $\log N$.

Алгоритм Шора: заполнение пробелов

Дано натуральное число N, о котором заранее известно, что оно есть произведение двух простых чисел p и q. Требуется найти p и q за время, полиномиальное *от длины записи* числа N, т.е. от $\log N$. Для этого достаточно найти такое число y, взаимно простое с N, что его период по модулю N есть четное число $2s$ и притом $y^s + 1$ не делится на N.

Алгоритм Шора: заполнение пробелов

Дано натуральное число N, о котором заранее известно, что оно есть произведение двух простых чисел p и q. Требуется найти p и q за время, полиномиальное *от длины записи* числа N, т.е. от $\log N$. Для этого достаточно найти такое число y, взаимно простое с N, что его период по модулю N есть четное число $2s$ и притом $y^s + 1$ не делится на N.

Выбираем наугад взаимно простое с N число y и пытаемся найти его период r по модулю N.

Алгоритм Шора: заполнение пробелов

Дано натуральное число N, о котором заранее известно, что оно есть произведение двух простых чисел p и q. Требуется найти p и q за время, полиномиальное *от длины записи* числа N, т.е. от $\log N$. Для этого достаточно найти такое число y, взаимно простое с N, что его период по модулю N есть четное число $2s$ и притом $y^s + 1$ не делится на N.

Выбираем наугад взаимно простое с N число y и пытаемся найти его период r по модулю N. Для этого проделываем над квантовой системой $H := H_S \otimes H_S$, где $N^2 \leq S := 2^n < 2N^2$, некоторую последовательность унитарных преобразований, а потом замеряем первый регистр.

Алгоритм Шора: заполнение пробелов

Дано натуральное число N, о котором заранее известно, что оно есть произведение двух простых чисел p и q. Требуется найти p и q за время, полиномиальное *от длины записи* числа N, т.е. от $\log N$. Для этого достаточно найти такое число y, взаимно простое с N, что его период по модулю N есть четное число $2s$ и притом $y^s + 1$ не делится на N.

Выбираем наугад взаимно простое с N число y и пытаемся найти его период r по модулю N. Для этого проделываем над квантовой системой $H := H_S \otimes H_S$, где $N^2 \leq S := 2^n < 2N^2$, некоторую последовательность унитарных преобразований, а потом замеряем первый регистр. Замер дает один из базисных векторов $|u\rangle$ с вероятностью примерно $r|b_u|^2$, где

$$b_u := \frac{1}{S} \sum_{j=0}^{A-1} e^{\frac{2\pi i u j r}{S}}, \quad A := \left\lceil \frac{S}{r} \right\rceil.$$

Алгоритм Шора: заполнение пробелов

Дано натуральное число N, о котором заранее известно, что оно есть произведение двух простых чисел p и q. Требуется найти p и q за время, полиномиальное *от длины записи* числа N, т.е. от $\log N$. Для этого достаточно найти такое число y, взаимно простое с N, что его период по модулю N есть четное число $2s$ и притом $y^s + 1$ не делится на N.

Выбираем наугад взаимно простое с N число y и пытаемся найти его период r по модулю N. Для этого проделываем над квантовой системой $H := H_S \otimes H_S$, где $N^2 \leq S := 2^n < 2N^2$, некоторую последовательность унитарных преобразований, а потом замеряем первый регистр. Замер дает один из базисных векторов $|u\rangle$ с вероятностью примерно $r|b_u|^2$, где

$$b_u := \frac{1}{S} \sum_{j=0}^{A-1} e^{\frac{2\pi i u j r}{S}}, \quad A := \left\lceil \frac{S}{r} \right\rceil.$$

Утверждается, что вероятность получить при этом один из векторов $|u\rangle$, для которых существует k со свойством $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$, не меньше 0.4, а количество таких векторов примерно равно r.

Алгоритм Шора: заполнение пробелов

Дано натуральное число N, о котором заранее известно, что оно есть произведение двух простых чисел p и q. Требуется найти p и q за время, полиномиальное *от длины записи* числа N, т.е. от $\log N$. Для этого достаточно найти такое число y, взаимно простое с N, что его период по модулю N есть четное число $2s$ и притом $y^s + 1$ не делится на N.

Выбираем наугад взаимно простое с N число y и пытаемся найти его период r по модулю N. Для этого проделываем над квантовой системой $H := H_S \otimes H_S$, где $N^2 \leq S := 2^n < 2N^2$, некоторую последовательность унитарных преобразований, а потом замеряем первый регистр. Замер дает один из базисных векторов $|u\rangle$ с вероятностью примерно $r|b_u|^2$, где

$$b_u := \frac{1}{S} \sum_{j=0}^{A-1} e^{\frac{2\pi iujr}{S}}, \quad A := \left\lceil \frac{S}{r} \right\rceil.$$

Утверждается, что вероятность получить при этом один из векторов $|u\rangle$, для которых существует k со свойством $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$, не меньше 0.4, а количество таких векторов примерно равно r.

Проверкой этих утверждений мы сейчас и займемся.

Неравенство $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$ можно переписать так:

$$-\frac{1}{2} \leq u - k\frac{S}{r} \leq \frac{1}{2}. \qquad (\star)$$

Неравенство $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$ можно переписать так:

$$-\frac{1}{2} \leq u - k\frac{S}{r} \leq \frac{1}{2}. \qquad (\star)$$

Поскольку $\frac{S}{r} \approx A$, а $u \leq S$, количество чисел u, для которых есть k такое, что выполнено $(\star)$, примерно равно r: такие u отвечают кратным числа A.

Неравенство $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$ можно переписать так:

$$-\frac{1}{2} \leq u - k\frac{S}{r} \leq \frac{1}{2}. \qquad (\star)$$

Поскольку $\frac{S}{r} \approx A$, а $u \leq S$, количество чисел u, для которых есть k такое, что выполнено $(\star)$, примерно равно r: такие u отвечают кратным числа A. А именно, для $u \approx A$ годится $k = 1$, для $u \approx 2A$ подходит $k = 2$, и т.д.

Неравенство $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$ можно переписать так:

$$-\frac{1}{2} \leq u - k\frac{S}{r} \leq \frac{1}{2}. \qquad (\star)$$

Поскольку $\frac{S}{r} \approx A$, а $u \leq S$, количество чисел u, для которых есть k такое, что выполнено $(\star)$, примерно равно r: такие u отвечают кратным числа A. А именно, для $u \approx A$ годится $k = 1$, для $u \approx 2A$ подходит $k = 2$, и т.д.

Теперь оценим $r|b_u|^2$. Суммируя геометрическую прогрессию, получаем

$$b_u := \frac{1}{S}\sum_{j=0}^{A-1} e^{\frac{2\pi iujr}{S}} = \frac{1}{S}\frac{1 - e^{\frac{2\pi iuAr}{S}}}{1 - e^{\frac{2\pi iur}{S}}}.$$

Неравенство $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$ можно переписать так:

$$-\frac{1}{2} \leq u - k\frac{S}{r} \leq \frac{1}{2}. \qquad (\star)$$

Поскольку $\frac{S}{r} \approx A$, а $u \leq S$, количество чисел u, для которых есть k такое, что выполнено $(\star)$, примерно равно r: такие u отвечают кратным числа A. А именно, для $u \approx A$ годится $k = 1$, для $u \approx 2A$ подходит $k = 2$, и т.д.

Теперь оценим $r|b_u|^2$. Суммируя геометрическую прогрессию, получаем

$$b_u := \frac{1}{S}\sum_{j=0}^{A-1} e^{\frac{2\pi iujr}{S}} = \frac{1}{S}\frac{1 - e^{\frac{2\pi iuAr}{S}}}{1 - e^{\frac{2\pi iur}{S}}}.$$

Отсюда и из формулы $\cos\varphi = \frac{1}{2}(e^{i\varphi} + e^{-i\varphi})$ получаем:

$$|b_u|^2 = b_u\overline{b_u} = \frac{1}{S^2}\frac{(1 - e^{\frac{2\pi iuAr}{S}})(1 - e^{-\frac{2\pi iuAr}{S}})}{(1 - e^{\frac{2\pi iur}{S}})(1 - e^{-\frac{2\pi iur}{S}})}$$

$$= \frac{1}{S^2}\frac{2 - \left(e^{\frac{2\pi iuAr}{S}} + e^{-\frac{2\pi iuAr}{S}}\right)}{2 - \left(e^{\frac{2\pi iur}{S}} + e^{-\frac{2\pi iur}{S}}\right)} = \frac{1}{S^2}\frac{1 - \cos\frac{2\pi uAr}{S}}{1 - \cos\frac{2\pi ur}{S}}.$$

Вычисление вероятности (2)

Итак, $r|b_u|^2 = \dfrac{r}{S^2}\dfrac{1-\cos\frac{2\pi uAr}{S}}{1-\cos\frac{2\pi ur}{S}} = \dfrac{r}{S^2}\dfrac{\sin^2\frac{\pi uAr}{S}}{\sin^2\frac{\pi ur}{S}}$.

Вычисление вероятности (2)

Итак, $r|b_u|^2 = \frac{r}{S^2}\frac{1-\cos\frac{2\pi uAr}{S}}{1-\cos\frac{2\pi ur}{S}} = \frac{r}{S^2}\frac{\sin^2\frac{\pi uAr}{S}}{\sin^2\frac{\pi ur}{S}}$. Мы хотим оценить дробь $\frac{\sin^2\frac{\pi uAr}{S}}{\sin^2\frac{\pi ur}{S}}$ снизу. Оценим ее знаменатель сверху, а числитель снизу.

Вычисление вероятности (2)

Итак, $r|b_u|^2 = \frac{r}{S^2}\frac{1-\cos\frac{2\pi uAr}{S}}{1-\cos\frac{2\pi ur}{S}} = \frac{r}{S^2}\frac{\sin^2\frac{\pi uAr}{S}}{\sin^2\frac{\pi ur}{S}}$. Мы хотим оценить дробь $\frac{\sin^2\frac{\pi uAr}{S}}{\sin^2\frac{\pi ur}{S}}$ снизу. Оценим ее знаменатель сверху, а числитель снизу.

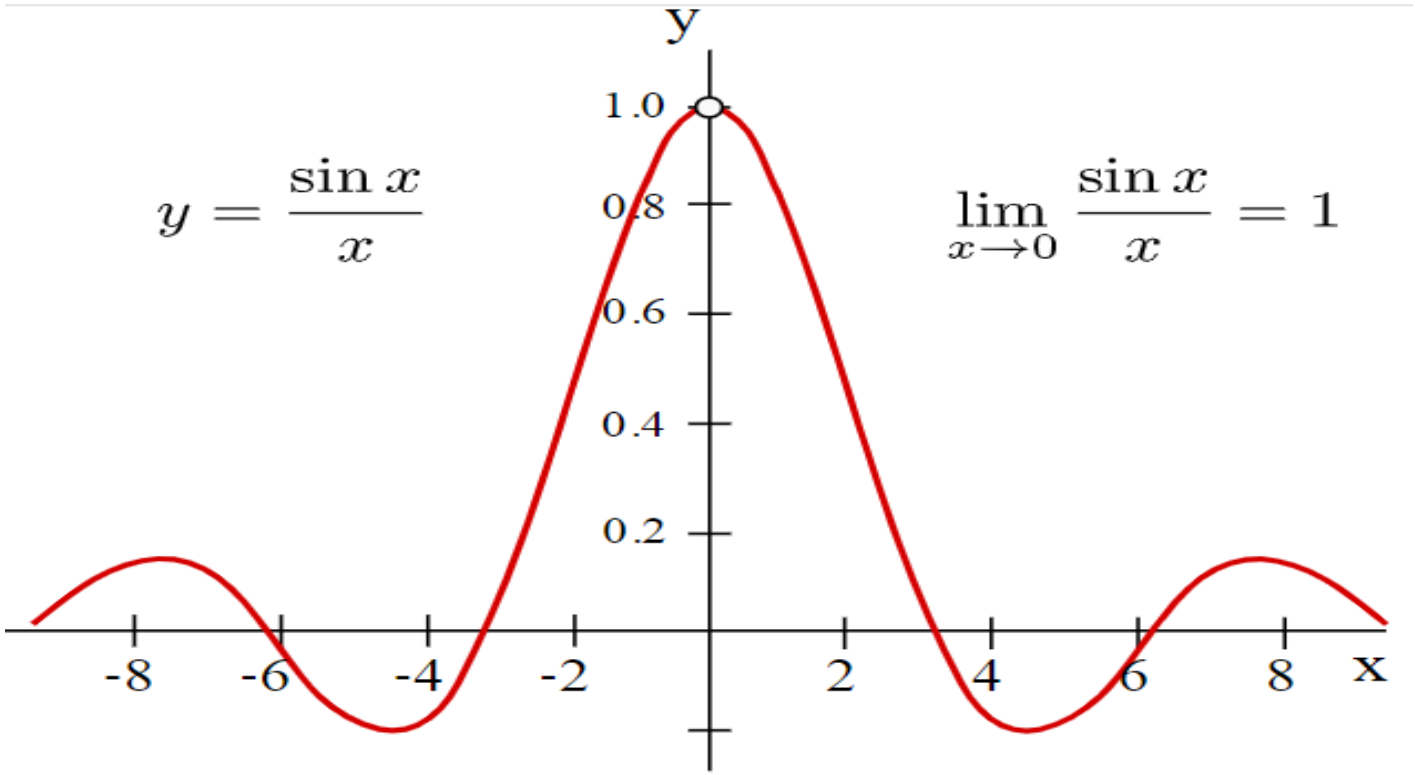
В силу неравенства $-\frac{r}{2} \le ur - kS \le \frac{r}{2}$ имеем $\frac{ur}{S} = k + t$, где $|t| \le \frac{1}{2}$.

Вычисление вероятности (2)

Итак, $r|b_u|^2 = \frac{r}{S^2}\frac{1-\cos\frac{2\pi uAr}{S}}{1-\cos\frac{2\pi ur}{S}} = \frac{r}{S^2}\frac{\sin^2\frac{\pi uAr}{S}}{\sin^2\frac{\pi ur}{S}}$. Мы хотим оценить дробь $\frac{\sin^2\frac{\pi uAr}{S}}{\sin^2\frac{\pi ur}{S}}$ снизу. Оценим ее знаменатель сверху, а числитель снизу.

В силу неравенства $-\frac{r}{2} \le ur - kS \le \frac{r}{2}$ имеем $\frac{ur}{S} = k + t$, где $|t| \le \frac{1}{2}$.

Рассмотрим функцию $g(x) := \frac{\sin x}{x}$.



Вычисление вероятности (2)

Итак, $r|b_u|^2 = \frac{r}{S^2}\frac{1-\cos\frac{2\pi uAr}{S}}{1-\cos\frac{2\pi ur}{S}} = \frac{r}{S^2}\frac{\sin^2\frac{\pi uAr}{S}}{\sin^2\frac{\pi ur}{S}}$. Мы хотим оценить дробь $\frac{\sin^2\frac{\pi uAr}{S}}{\sin^2\frac{\pi ur}{S}}$ снизу. Оценим ее знаменатель сверху, а числитель снизу.

В силу неравенства $-\frac{r}{2} \le ur - kS \le \frac{r}{2}$ имеем $\frac{ur}{S} = k + t$, где $|t| \le \frac{1}{2}$.

Рассмотрим функцию $g(x) := \frac{\sin x}{x}$. Имеем $|g(x)| \le 1$ при всех x, откуда

$$\sin^2\frac{\pi ur}{S} = \sin^2(\pi k + \pi t) = \sin^2(\pi t) = (\pi t)^2 g^2(\pi t) \le (\pi t)^2.$$

Вычисление вероятности (2)

Итак, $r|b_u|^2 = \frac{r}{S^2}\frac{1-\cos\frac{2\pi uAr}{S}}{1-\cos\frac{2\pi ur}{S}} = \frac{r}{S^2}\frac{\sin^2\frac{\pi uAr}{S}}{\sin^2\frac{\pi ur}{S}}$. Мы хотим оценить дробь $\frac{\sin^2\frac{\pi uAr}{S}}{\sin^2\frac{\pi ur}{S}}$ снизу. Оценим ее знаменатель сверху, а числитель снизу.

В силу неравенства $-\frac{r}{2} \le ur - kS \le \frac{r}{2}$ имеем $\frac{ur}{S} = k + t$, где $|t| \le \frac{1}{2}$.

Рассмотрим функцию $g(x) := \frac{\sin x}{x}$. Имеем $|g(x)| \le 1$ при всех x, откуда

$$\sin^2\frac{\pi ur}{S} = \sin^2(\pi k + \pi t) = \sin^2(\pi t) = (\pi t)^2 g^2(\pi t) \le (\pi t)^2.$$

Теперь займемся числителем. В силу неравенства $-\frac{r}{2} \le ur - kS \le \frac{r}{2}$ имеем

$$-\frac{Ar}{2S} \le \frac{Aur}{S} - Ak = At \le \frac{Ar}{2S}. \qquad (\dagger)$$

Вычисление вероятности (2)

Итак, $r|b_u|^2 = \frac{r}{S^2}\frac{1-\cos\frac{2\pi uAr}{S}}{1-\cos\frac{2\pi ur}{S}} = \frac{r}{S^2}\frac{\sin^2\frac{\pi uAr}{S}}{\sin^2\frac{\pi ur}{S}}$. Мы хотим оценить дробь $\frac{\sin^2\frac{\pi uAr}{S}}{\sin^2\frac{\pi ur}{S}}$ снизу. Оценим ее знаменатель сверху, а числитель снизу.

В силу неравенства $-\frac{r}{2} \le ur - kS \le \frac{r}{2}$ имеем $\frac{ur}{S} = k + t$, где $|t| \le \frac{1}{2}$.

Рассмотрим функцию $g(x) := \frac{\sin x}{x}$. Имеем $|g(x)| \le 1$ при всех x, откуда

$$\sin^2\frac{\pi ur}{S} = \sin^2(\pi k + \pi t) = \sin^2(\pi t) = (\pi t)^2 g^2(\pi t) \le (\pi t)^2.$$

Теперь займемся числителем. В силу неравенства $-\frac{r}{2} \le ur - kS \le \frac{r}{2}$ имеем

$$-\frac{Ar}{2S} \le \frac{Aur}{S} - Ak = At \le \frac{Ar}{2S}. \qquad (\dagger)$$

Напомним, что $A = \left\lceil \frac{S}{r} \right\rceil$, откуда $A - 1 < \frac{S}{r} \le A$. Деля на A и переворачивая, получаем $1 \le \frac{Ar}{S} < \frac{A}{A-1} = 1 + \frac{1}{A-1}$.

Вычисление вероятности (2)

Итак, $r|b_u|^2 = \frac{r}{S^2}\frac{1-\cos\frac{2\pi uAr}{S}}{1-\cos\frac{2\pi ur}{S}} = \frac{r}{S^2}\frac{\sin^2\frac{\pi uAr}{S}}{\sin^2\frac{\pi ur}{S}}$. Мы хотим оценить дробь $\frac{\sin^2\frac{\pi uAr}{S}}{\sin^2\frac{\pi ur}{S}}$ снизу. Оценим ее знаменатель сверху, а числитель снизу.

В силу неравенства $-\frac{r}{2} \le ur - kS \le \frac{r}{2}$ имеем $\frac{ur}{S} = k + t$, где $|t| \le \frac{1}{2}$.

Рассмотрим функцию $g(x) := \frac{\sin x}{x}$. Имеем $|g(x)| \le 1$ при всех x, откуда

$$\sin^2\frac{\pi ur}{S} = \sin^2(\pi k + \pi t) = \sin^2(\pi t) = (\pi t)^2 g^2(\pi t) \le (\pi t)^2.$$

Теперь займемся числителем. В силу неравенства $-\frac{r}{2} \le ur - kS \le \frac{r}{2}$ имеем

$$-\frac{Ar}{2S} \le \frac{Aur}{S} - Ak = At \le \frac{Ar}{2S}. \qquad (\dagger)$$

Напомним, что $A = \left\lceil \frac{S}{r} \right\rceil$, откуда $A - 1 < \frac{S}{r} \le A$. Деля на A и переворачивая, получаем $1 \le \frac{Ar}{S} < \frac{A}{A-1} = 1 + \frac{1}{A-1}$. Используя это, выводим из $(\dagger)$ неравенство

$$-\frac{\pi}{2}\left(1 + \frac{1}{A-1}\right) < \pi At < \frac{\pi}{2}\left(1 + \frac{1}{A-1}\right).$$

Вычисление вероятности (3)

Имеем $r < N$ и $N^2 \leq S$, откуда $N < \frac{S}{r} \leq A$.

Имеем $r < N$ и $N^2 \leq S$, откуда $N < \frac{S}{r} \leq A$. Поэтому замена A на N в крайних выражениях двойного неравенства

$$-\frac{\pi}{2}\left(1+\frac{1}{A-1}\right) < \pi A t < \frac{\pi}{2}\left(1+\frac{1}{A-1}\right)$$

показывает, что

$$-\frac{\pi}{2}\left(1+\frac{1}{N-1}\right) < \pi A t < \frac{\pi}{2}\left(1+\frac{1}{N-1}\right).$$

Вычисление вероятности (3)

Имеем $r < N$ и $N^2 \leq S$, откуда $N < \dfrac{S}{r} \leq A$. Поэтому замена A на N в крайних выражениях двойного неравенства

$$-\frac{\pi}{2}\left(1+\frac{1}{A-1}\right) < \pi A t < \frac{\pi}{2}\left(1+\frac{1}{A-1}\right)$$

показывает, что

$$-\frac{\pi}{2}\left(1+\frac{1}{N-1}\right) < \pi A t < \frac{\pi}{2}\left(1+\frac{1}{N-1}\right).$$

В частности, $|\pi A t| < \pi$, а на $[0, \pi]$ функция $g(x) = \dfrac{\sin x}{x}$ убывает.

Вычисление вероятности (3)

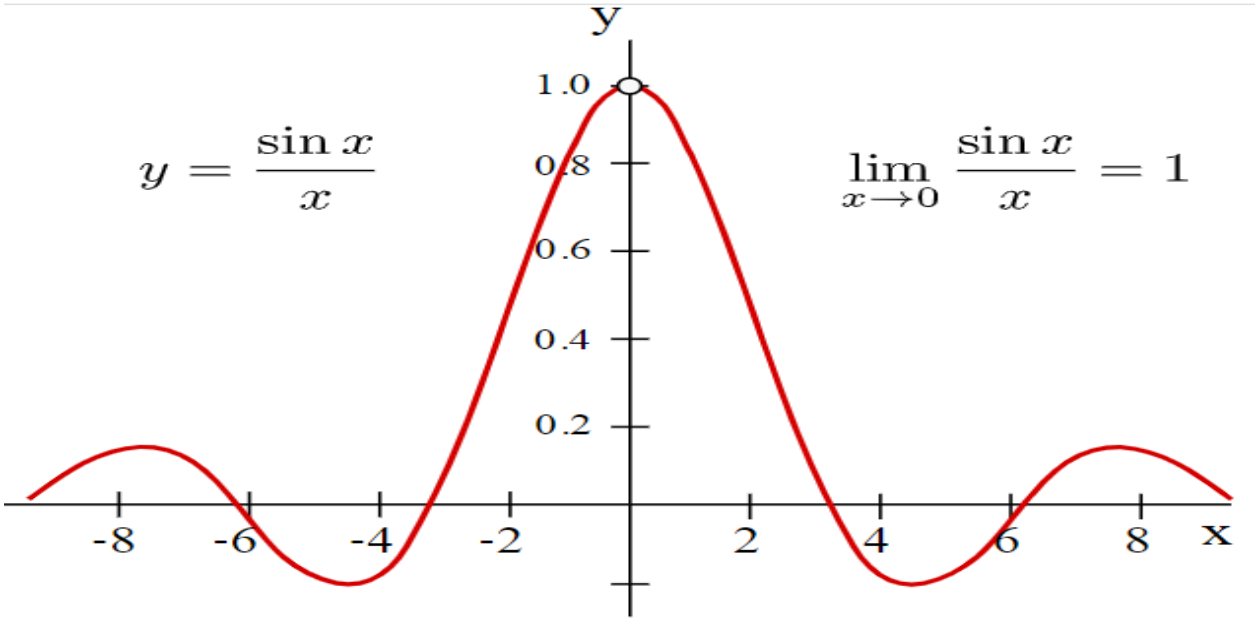
Имеем $r < N$ и $N^2 \leq S$, откуда $N < \dfrac{S}{r} \leq A$. Поэтому замена A на N в крайних выражениях двойного неравенства

$$-\frac{\pi}{2}\left(1+\frac{1}{A-1}\right) < \pi A t < \frac{\pi}{2}\left(1+\frac{1}{A-1}\right)$$

показывает, что

$$-\frac{\pi}{2}\left(1+\frac{1}{N-1}\right) < \pi A t < \frac{\pi}{2}\left(1+\frac{1}{N-1}\right).$$

В частности, $|\pi A t| < \pi$, а на $[0, \pi]$ функция $g(x) = \dfrac{\sin x}{x}$ убывает.



Имеем $r < N$ и $N^2 \leq S$, откуда $N < \frac{S}{r} \leq A$. Поэтому замена A на N в крайних выражениях двойного неравенства

$$-\frac{\pi}{2}\left(1+\frac{1}{A-1}\right) < \pi A t < \frac{\pi}{2}\left(1+\frac{1}{A-1}\right)$$

показывает, что

$$-\frac{\pi}{2}\left(1+\frac{1}{N-1}\right) < \pi A t < \frac{\pi}{2}\left(1+\frac{1}{N-1}\right).$$

В частности, $|\pi A t| < \pi$, а на $[0,\pi]$ функция $g(x) = \frac{\sin x}{x}$ убывает. Отсюда

$$\sin^2\frac{\pi A u r}{S} = \sin^2(\pi A k + \pi A t) = \sin^2(\pi A t) = (\pi A t)^2 g^2(A\pi t) \geq$$
$$\geq (\pi A t)^2 g^2\left(\frac{\pi}{2}\left(1+\frac{1}{N-1}\right)\right).$$

Вычисление вероятности (4)

Напомним цель: оценить снизу выражение $r|b_u|^2 = \frac{r}{S^2} \frac{\sin^2 \frac{\pi u A r}{S}}{\sin^2 \frac{\pi u r}{S}}$.

Вычисление вероятности (4)

Напомним цель: оценить снизу выражение $r|b_u|^2 = \frac{r}{S^2} \frac{\sin^2 \frac{\pi u A r}{S}}{\sin^2 \frac{\pi u r}{S}}$. Мы оценили знаменатель сверху как $\sin^2 \frac{\pi u r}{S} \leq (\pi t)^2$, а числитель снизу как $\sin^2 \frac{\pi A u r}{S} \geq (\pi A t)^2 g^2 \left(\frac{\pi}{2} \left(1 + \frac{1}{N-1} \right) \right)$.

Вычисление вероятности (4)

Напомним цель: оценить снизу выражение $r|b_u|^2 = \frac{r}{S^2} \frac{\sin^2 \frac{\pi u A r}{S}}{\sin^2 \frac{\pi u r}{S}}$. Мы оценили знаменатель сверху как $\sin^2 \frac{\pi u r}{S} \leq (\pi t)^2$, а числитель снизу как $\sin^2 \frac{\pi A u r}{S} \geq (\pi A t)^2 g^2 \left(\frac{\pi}{2} \left(1 + \frac{1}{N-1} \right) \right)$. Деля второе на первое, имеем

$$r|b_u|^2 \geq \frac{rA^2}{S^2} g^2 \left(\frac{\pi}{2} \left(1 + \frac{1}{N-1} \right) \right) = \frac{rA^2}{S^2} \frac{4}{\pi^2} \left(\frac{N-1}{N} \right)^2 \sin^2 \left(\frac{\pi}{2} \left(1 + \frac{1}{N-1} \right) \right).$$

Вычисление вероятности (4)

Напомним цель: оценить снизу выражение $r|b_u|^2 = \frac{r}{S^2} \frac{\sin^2 \frac{\pi u A r}{S}}{\sin^2 \frac{\pi u r}{S}}$. Мы оценили знаменатель сверху как $\sin^2 \frac{\pi u r}{S} \leq (\pi t)^2$, а числитель снизу как $\sin^2 \frac{\pi A u r}{S} \geq (\pi A t)^2 g^2 \left(\frac{\pi}{2} \left(1 + \frac{1}{N-1} \right) \right)$. Деля второе на первое, имеем

$$r|b_u|^2 \geq \frac{rA^2}{S^2} g^2 \left(\frac{\pi}{2} \left(1 + \frac{1}{N-1} \right) \right) = \frac{rA^2}{S^2} \frac{4}{\pi^2} \left(\frac{N-1}{N} \right)^2 \sin^2 \left(\frac{\pi}{2} \left(1 + \frac{1}{N-1} \right) \right).$$

Разберемся с непостоянными сомножителями.

Вычисление вероятности (4)

Напомним цель: оценить снизу выражение $r|b_u|^2 = \frac{r}{S^2}\frac{\sin^2\frac{\pi uAr}{S}}{\sin^2\frac{\pi ur}{S}}$. Мы оценили знаменатель сверху как $\sin^2\frac{\pi ur}{S} \leq (\pi t)^2$, а числитель снизу как $\sin^2\frac{\pi Aur}{S} \geq (\pi At)^2 g^2\left(\frac{\pi}{2}\left(1+\frac{1}{N-1}\right)\right)$. Деля второе на первое, имеем

$$r|b_u|^2 \geq \frac{rA^2}{S^2}g^2\left(\frac{\pi}{2}\left(1+\frac{1}{N-1}\right)\right) = \frac{rA^2}{S^2}\frac{4}{\pi^2}\left(\frac{N-1}{N}\right)^2\sin^2\left(\frac{\pi}{2}\left(1+\frac{1}{N-1}\right)\right).$$

Разберемся с непостоянными сомножителями. $A = \left\lceil\frac{S}{r}\right\rceil$, откуда $\frac{S}{r} \leq A$.

Поэтому $\frac{rA}{S} \geq 1$ и $\frac{rA^2}{S^2} \geq \frac{1}{r}$.

Вычисление вероятности (4)

Напомним цель: оценить снизу выражение $r|b_u|^2 = \frac{r}{S^2}\frac{\sin^2\frac{\pi uAr}{S}}{\sin^2\frac{\pi ur}{S}}$. Мы оценили знаменатель сверху как $\sin^2\frac{\pi ur}{S} \leq (\pi t)^2$, а числитель снизу как $\sin^2\frac{\pi Aur}{S} \geq (\pi At)^2 g^2\left(\frac{\pi}{2}\left(1+\frac{1}{N-1}\right)\right)$. Деля второе на первое, имеем

$$r|b_u|^2 \geq \frac{rA^2}{S^2}g^2\left(\frac{\pi}{2}\left(1+\frac{1}{N-1}\right)\right) = \frac{rA^2}{S^2}\frac{4}{\pi^2}\left(\frac{N-1}{N}\right)^2\sin^2\left(\frac{\pi}{2}\left(1+\frac{1}{N-1}\right)\right).$$

Разберемся с непостоянными сомножителями. $A = \left\lceil\frac{S}{r}\right\rceil$, откуда $\frac{S}{r} \leq A$. Поэтому $\frac{rA}{S} \geq 1$ и $\frac{rA^2}{S^2} \geq \frac{1}{r}$. 3-й сомножитель с точностью до $\frac{1}{N^2}$ равен $1-\frac{2}{N}$.

Вычисление вероятности (4)

Напомним цель: оценить снизу выражение $r|b_u|^2 = \frac{r}{S^2}\frac{\sin^2\frac{\pi uAr}{S}}{\sin^2\frac{\pi ur}{S}}$. Мы оценили знаменатель сверху как $\sin^2\frac{\pi ur}{S} \le (\pi t)^2$, а числитель снизу как $\sin^2\frac{\pi Aur}{S} \ge (\pi At)^2 g^2\left(\frac{\pi}{2}\left(1+\frac{1}{N-1}\right)\right)$. Деля второе на первое, имеем

$$r|b_u|^2 \ge \frac{rA^2}{S^2}g^2\left(\frac{\pi}{2}\left(1+\frac{1}{N-1}\right)\right) = \frac{rA^2}{S^2}\frac{4}{\pi^2}\left(\frac{N-1}{N}\right)^2\sin^2\left(\frac{\pi}{2}\left(1+\frac{1}{N-1}\right)\right).$$

Разберемся с непостоянными сомножителями. $A = \left\lceil\frac{S}{r}\right\rceil$, откуда $\frac{S}{r} \le A$. Поэтому $\frac{rA}{S} \ge 1$ и $\frac{rA^2}{S^2} \ge \frac{1}{r}$. 3-й сомножитель с точностью до $\frac{1}{N^2}$ равен $1-\frac{2}{N}$. Наконец, $\sin\left(\frac{\pi}{2}\left(1+\frac{1}{N-1}\right)\right) = \cos\frac{\pi}{2(N-1)} = 1-\frac{\pi^2}{8(N-1)^2}+\cdots$, поэтому точностью до $\left(\frac{1}{N-1}\right)^\alpha$, где $\alpha \ge 2$, 4-й сомножитель равен 1.

Вычисление вероятности (4)

Напомним цель: оценить снизу выражение $r|b_u|^2 = \frac{r}{S^2}\frac{\sin^2\frac{\pi uAr}{S}}{\sin^2\frac{\pi ur}{S}}$. Мы оценили знаменатель сверху как $\sin^2\frac{\pi ur}{S} \le (\pi t)^2$, а числитель снизу как $\sin^2\frac{\pi Aur}{S} \ge (\pi At)^2 g^2\left(\frac{\pi}{2}\left(1+\frac{1}{N-1}\right)\right)$. Деля второе на первое, имеем

$$r|b_u|^2 \ge \frac{rA^2}{S^2}g^2\left(\frac{\pi}{2}\left(1+\frac{1}{N-1}\right)\right) = \frac{rA^2}{S^2}\frac{4}{\pi^2}\left(\frac{N-1}{N}\right)^2\sin^2\left(\frac{\pi}{2}\left(1+\frac{1}{N-1}\right)\right).$$

Разберемся с непостоянными сомножителями. $A = \left\lceil\frac{S}{r}\right\rceil$, откуда $\frac{S}{r} \le A$. Поэтому $\frac{rA}{S} \ge 1$ и $\frac{rA^2}{S^2} \ge \frac{1}{r}$. 3-й сомножитель с точностью до $\frac{1}{N^2}$ равен $1-\frac{2}{N}$. Наконец, $\sin\left(\frac{\pi}{2}\left(1+\frac{1}{N-1}\right)\right) = \cos\frac{\pi}{2(N-1)} = 1-\frac{\pi^2}{8(N-1)^2}+\cdots$, поэтому точностью до $\left(\frac{1}{N-1}\right)^\alpha$, где $\alpha \ge 2$, 4-й сомножитель равен 1. Итак, $r|b_u|^2 \ge \frac{1}{r}\frac{4}{\pi^2}\left(1-\frac{2}{N}\right) \ge \frac{0.4}{r}$.

Вычисление вероятности (4)

Напомним цель: оценить снизу выражение $r|b_u|^2 = \frac{r}{S^2}\frac{\sin^2\frac{\pi uAr}{S}}{\sin^2\frac{\pi ur}{S}}$. Мы оценили знаменатель сверху как $\sin^2\frac{\pi ur}{S} \le (\pi t)^2$, а числитель снизу как $\sin^2\frac{\pi Aur}{S} \ge (\pi At)^2 g^2\left(\frac{\pi}{2}\left(1+\frac{1}{N-1}\right)\right)$. Деля второе на первое, имеем

$$r|b_u|^2 \ge \frac{rA^2}{S^2}g^2\left(\frac{\pi}{2}\left(1+\frac{1}{N-1}\right)\right) = \frac{rA^2}{S^2}\frac{4}{\pi^2}\left(\frac{N-1}{N}\right)^2\sin^2\left(\frac{\pi}{2}\left(1+\frac{1}{N-1}\right)\right).$$

Разберемся с непостоянными сомножителями. $A = \left\lceil\frac{S}{r}\right\rceil$, откуда $\frac{S}{r} \le A$. Поэтому $\frac{rA}{S} \ge 1$ и $\frac{rA^2}{S^2} \ge \frac{1}{r}$. 3-й сомножитель с точностью до $\frac{1}{N^2}$ равен $1-\frac{2}{N}$. Наконец, $\sin\left(\frac{\pi}{2}\left(1+\frac{1}{N-1}\right)\right) = \cos\frac{\pi}{2(N-1)} = 1-\frac{\pi^2}{8(N-1)^2}+\cdots$, поэтому точностью до $\left(\frac{1}{N-1}\right)^\alpha$, где $\alpha \ge 2$, 4-й сомножитель равен 1.

Итак, $r|b_u|^2 \ge \frac{1}{r}\frac{4}{\pi^2}\left(1-\frac{2}{N}\right) \ge \frac{0.4}{r}$. Поэтому вероятность получить один из r «хороших» векторов $|u\rangle$ не меньше 0.4.

Нахождение периода по $|u\rangle$

На прошлой лекции мы показали, что вероятность угадать «правильное» число y не меньше 0.5, а сейчас проверили, что вероятность получить как результат алгоритма Шора один из векторов $|u\rangle$, для которых существует k со свойством $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$, не меньше 0.4.

Нахождение периода по $|u\rangle$

На прошлой лекции мы показали, что вероятность угадать «правильное» число y не меньше 0.5, а сейчас проверили, что вероятность получить как результат алгоритма Шора один из векторов $|u\rangle$, для которых существует k со свойством $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$, не меньше 0.4.

Объясним, как по такому u найти период r.

Нахождение периода по $|u\rangle$

На прошлой лекции мы показали, что вероятность угадать «правильное» число y не меньше 0.5, а сейчас проверили, что вероятность получить как результат алгоритма Шора один из векторов $|u\rangle$, для которых существует k со свойством $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$, не меньше 0.4.

Объясним, как по такому u найти период r.

Неравенство $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$ можно переписать так:

$$\left|\frac{u}{S} - \frac{k}{r}\right| \leq \frac{1}{2S} < \frac{1}{2N^2}.$$

Нахождение периода по $|u\rangle$

На прошлой лекции мы показали, что вероятность угадать «правильное» число y не меньше 0.5, а сейчас проверили, что вероятность получить как результат алгоритма Шора один из векторов $|u\rangle$, для которых существует k со свойством $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$, не меньше 0.4.

Объясним, как по такому u найти период r.

Неравенство $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$ можно переписать так:

$$\left|\frac{u}{S} - \frac{k}{r}\right| \leq \frac{1}{2S} < \frac{1}{2N^2}.$$

Итак, мы приближаем *известную* дробь $\frac{u}{S}$ *неизвестной* дробью $\frac{k}{r}$ со знаменателем $r < N$ с точностью, лучшей, чем $\frac{1}{2N^2}$.

Нахождение периода по $|u\rangle$

На прошлой лекции мы показали, что вероятность угадать «правильное» число y не меньше 0.5, а сейчас проверили, что вероятность получить как результат алгоритма Шора один из векторов $|u\rangle$, для которых существует k со свойством $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$, не меньше 0.4.

Объясним, как по такому u найти период r.

Неравенство $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$ можно переписать так:

$$\left|\frac{u}{S} - \frac{k}{r}\right| \leq \frac{1}{2S} < \frac{1}{2N^2}.$$

Итак, мы приближаем *известную* дробь $\frac{u}{S}$ *неизвестной* дробью $\frac{k}{r}$ со знаменателем $r < N$ с точностью, лучшей, чем $\frac{1}{2N^2}$. Если такая дробь $\frac{k}{r}$ существует, то равная ей *несократимая* дробь может быть вычислена за полиномиальное время от длины записи N с помощью известного в теории чисел алгоритма.

Нахождение периода по $|u\rangle$

На прошлой лекции мы показали, что вероятность угадать «правильное» число y не меньше 0.5, а сейчас проверили, что вероятность получить как результат алгоритма Шора один из векторов $|u\rangle$, для которых существует k со свойством $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$, не меньше 0.4.

Объясним, как по такому u найти период r.

Неравенство $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$ можно переписать так:

$$\left|\frac{u}{S} - \frac{k}{r}\right| \leq \frac{1}{2S} < \frac{1}{2N^2}.$$

Итак, мы приближаем *известную* дробь $\frac{u}{S}$ *неизвестной* дробью $\frac{k}{r}$ со знаменателем $r < N$ с точностью, лучшей, чем $\frac{1}{2N^2}$. Если такая дробь $\frac{k}{r}$ существует, то равная ей *несократимая* дробь может быть вычислена за полиномиальное время от длины записи N с помощью известного в теории чисел алгоритма. Опишем этот алгоритм.

Цепная дробь — это конечное или бесконечное выражение вида

$$[a_0; a_1, a_2, a_3, \cdots] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ldots}}},$$

где a_0 — целое число, а все остальные a_n — натуральные числа.

Цепная дробь — это конечное или бесконечное выражение вида

$$[a_0; a_1, a_2, a_3, \cdots] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ldots}}},$$

где a_0 — целое число, а все остальные a_n — натуральные числа. Любое действительное число представимо в виде цепной дроби.

Цепная дробь — это конечное или бесконечное выражение вида

$$[a_0; a_1, a_2, a_3, \cdots] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}},$$

где a_0 — целое число, а все остальные a_n — натуральные числа.
Любое действительное число представимо в виде цепной дроби.
Нам цепные дроби понадобятся только для рациональных чисел. Цепная дробь, представляющая данное рациональное число $\frac{P}{Q}$, где P целое, а Q натуральное, всегда конечна, и ее элементы $a_0, a_1, a_2, a_3, \dots, a_n$ суть в точности неполные частные в алгоритме Евклида, примененном к P и Q:

$$\begin{aligned} P &= Qa_0 + r_1 \\ Q &= r_1 a_1 + r_2 \\ r_1 &= r_2 a_2 + r_3 \\ &\dots\dots\dots\dots\dots \\ r_{n-1} &= r_n a_n \end{aligned}$$

Цепная дробь — это конечное или бесконечное выражение вида

$$[a_0; a_1, a_2, a_3, \cdots] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}},$$

где a_0 — целое число, а все остальные a_n — натуральные числа.
Любое действительное число представимо в виде цепной дроби.
Нам цепные дроби понадобятся только для рациональных чисел. Цепная дробь, представляющая данное рациональное число $\frac{P}{Q}$, где P целое, а Q натуральное, всегда конечна, и ее элементы $a_0, a_1, a_2, a_3, \dots, a_n$ суть в точности неполные частные в алгоритме Евклида, примененном к P и Q:

$$P = Qa_0 + r_1$$
$$Q = r_1 a_1 + r_2$$
$$r_1 = r_2 a_2 + r_3$$
$$\dots\dots\dots\dots\dots$$
$$r_{n-1} = r_n a_n$$

Поэтому $a_0, a_1, a_2, \dots, a_n$ вычислимы за полиномиальное от $\log PQ$ время.

Подходящие дроби

Пусть $x = [a_0; a_1, a_2, a_3, \cdots]$ — число, представленное цепной дробью.

Подходящие дроби

Пусть $x = [a_0; a_1, a_2, a_3, \cdots]$ — число, представленное цепной дробью. *n-й подходящей дробью* для x называется конечная цепная дробь $[a_0; a_1, \cdots, a_n]$, значение которой есть некоторое рациональное число $\frac{p_n}{q_n}$.

Подходящие дроби

Пусть $x = [a_0; a_1, a_2, a_3, \cdots]$ — число, представленное цепной дробью. *n-й подходящей дробью* для x называется конечная цепная дробь $[a_0; a_1, \cdots, a_n]$, значение которой есть некоторое рациональное число $\frac{p_n}{q_n}$.

Есть несложные рекуррентные формулы для вычисления числителей и знаменателей подходящих дробей:

$$p_{-1} = 1, \quad p_0 = a_0, \quad p_n = a_n p_{n-1} + p_{n-2};$$
$$q_{-1} = 0, \quad q_0 = 1, \quad q_n = a_n q_{n-1} + q_{n-2}.$$

Подходящие дроби

Пусть $x = [a_0; a_1, a_2, a_3, \cdots]$ — число, представленное цепной дробью. *n-й подходящей дробью* для x называется конечная цепная дробь $[a_0; a_1, \cdots, a_n]$, значение которой есть некоторое рациональное число $\frac{p_n}{q_n}$.

Есть несложные рекуррентные формулы для вычисления числителей и знаменателей подходящих дробей:

$$p_{-1} = 1, \quad p_0 = a_0, \quad p_n = a_n p_{n-1} + p_{n-2};$$
$$q_{-1} = 0, \quad q_0 = 1, \quad q_n = a_n q_{n-1} + q_{n-2}.$$

Поэтому подходящие дроби к рациональному числу $\frac{P}{Q}$ вычислимы за полиномиальное от $\log PQ$ время.

Подходящие дроби

Пусть $x = [a_0; a_1, a_2, a_3, \cdots]$ — число, представленное цепной дробью. *n-й подходящей дробью* для x называется конечная цепная дробь $[a_0; a_1, \cdots, a_n]$, значение которой есть некоторое рациональное число $\frac{p_n}{q_n}$.

Есть несложные рекуррентные формулы для вычисления числителей и знаменателей подходящих дробей:

$$p_{-1} = 1, \quad p_0 = a_0, \quad p_n = a_n p_{n-1} + p_{n-2};$$
$$q_{-1} = 0, \quad q_0 = 1, \quad q_n = a_n q_{n-1} + q_{n-2}.$$

Поэтому подходящие дроби к рациональному числу $\frac{P}{Q}$ вычислимы за полиномиальное от $\log PQ$ время.

По индукции легко доказывается, что числители и знаменатели соседних подходящих дробей связаны равенством:

$$p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}.$$

Из него следует, что все подходящие дроби несократимы.

Приближения подходящими дробями

Подходящие дроби отлично приближают «свое» число:

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2}.$$

Приближения подходящими дробями

Подходящие дроби отлично приближают «свое» число:

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2}.$$

Пример: подходящие дроби для $\pi - 3$, $\frac{22}{7}$, $\frac{333}{106}$, $\frac{355}{113}$, $\frac{103993}{33102}$.

Подходящие дроби отлично приближают «свое» число:

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2}.$$

Пример: подходящие дроби для $\pi - 3$, $\frac{22}{7}$, $\frac{333}{106}$, $\frac{355}{113}$, $\frac{103993}{33102}$.

Но для нас важнее обратный результат:

Теорема

Если целое число a и натуральное число b взаимно просты и удовлетворяют неравенству

$$\left| x - \frac{a}{b} \right| < \frac{1}{2b^2}, \qquad (!)$$

то $\frac{a}{b}$ — одна из подходящих дробей к x.

Приближения подходящими дробями

Подходящие дроби отлично приближают «свое» число:

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2}.$$

Пример: подходящие дроби для $\pi - 3$, $\frac{22}{7}$, $\frac{333}{106}$, $\frac{355}{113}$, $\frac{103993}{33102}$.

Но для нас важнее обратный результат:

Теорема

Если целое число a и натуральное число b взаимно просты и удовлетворяют неравенству

$$\left| x - \frac{a}{b} \right| < \frac{1}{2b^2}, \qquad (!)$$

то $\frac{a}{b}$ — одна из подходящих дробей к x.

В частности, если $x = \frac{P}{Q}$, найти дробь $\frac{a}{b}$, удовлетворяющую неравенству (!), если она существует, можно за полиномиальное от $\log PQ$ время.

Алгоритм Шора: итоги

Итак, из неравенства

$$\left|\frac{u}{S} - \frac{k}{r}\right| \leq \frac{1}{2S} < \frac{1}{2N^2}$$

можно за полиномиальное от длины записи числа N найти несократимую дробь, равную дроби $\frac{k}{r}$.

Итак, из неравенства

$$\left|\frac{u}{S} - \frac{k}{r}\right| \leq \frac{1}{2S} < \frac{1}{2N^2}$$

можно за полиномиальное от длины записи числа N найти несократимую дробь, равную дроби $\frac{k}{r}$.

Как обсуждалось в конце прошлой лекции, вероятность того, что дробь $\frac{k}{r}$ несократима, равна $\frac{\varphi(r)}{r}$, а для $\frac{\varphi(r)}{r}$ есть нижняя оценка вида $\frac{0.56}{\log\log N}$.

Алгоритм Шора: итоги

Итак, из неравенства

$$\left|\frac{u}{S} - \frac{k}{r}\right| \leq \frac{1}{2S} < \frac{1}{2N^2}$$

можно за полиномиальное от длины записи числа N найти несократимую дробь, равную дроби $\frac{k}{r}$.

Как обсуждалось в конце прошлой лекции, вероятность того, что дробь $\frac{k}{r}$ несократима, равна $\frac{\varphi(r)}{r}$, а для $\frac{\varphi(r)}{r}$ есть нижняя оценка вида $\frac{0.56}{\log\log N}$.

Значит, запуская алгоритм Шора $\log\log N$ раз, мы определим верное значение r с вероятностью по крайней мере

$$\underbrace{0.5}_{\text{нужное } y} \cdot \underbrace{0.4}_{\text{нужное } u} \cdot \underbrace{0.56}_{\text{нужное } k} > 0.1.$$