Нижняя оценка на функцию расстояние Хэмминга k с оракулом равенства

Мекешкин Г.А.

12 июня 2024 г.

1 Введение

Пусть изначально задана некоторая функция $f\colon X \times Y \to Z$, где $X = Y = \{0,1\}^n$, $Z = \{0,1\}$. Алиса получает элемент $x \in X$, Боб получает $y \in Y$. Обмениваясь друг с другом сообщениями по одному биту (используя некоторый заранее определённый протокол связи), Алиса и Боб хотят вычислить значение $z = f(x,y)$ так, чтобы в конце общения каждый из них знал значение z.

Коммуникационная сложность вычисления функции f обозначается как $C(f)$ и определяется как минимальное количество бит коммуникации, которого достаточно для решения поставленной задачи в худшем случае (то есть этого количества битов должно быть достаточно для любой пары x,y).

Опираясь на это определение удобно думать о функции f, как о функции, заданной матрицей M, в которой строки индексированы элементами $x \in X$, а столбцы, соответственно, элементами $y \in Y$. В каждой клетке этой матрицы, индексированной элементами x и y, записано соответствующее значение f. Алиса и Боб знают функцию f, а следовательно знают матрицу M. Далее, Алисе выдаётся номер строчки x, а Бобу — номер столбца y, и их задача — определить значение, записанное в соответствующей клетке. Поэтому, если в какой-то момент один из игроков будет знать одновременно и номер столбца и номер строчки, то он будет знать и значение в соответствующей клетке. В начале коммуникации каждый игрок ничего не знает про номер другого игрока, поэтому с точки зрения Алисы ответом может быть любое значение в строчке с номером x, а с точки зрения Боба — любое значение в столбце y. В процессе коммуникации с каждым переданным битом появляется новая информация, которая позволяет игрокам отсекать часть возможных клеток. Например, если в какой-то момент Алиса передаёт бит a, то с точки зрения Боба все возможные к этому моменту входы Алисы делятся на два множества: те, для которых Алиса послала бы 0, и те, для которых Алиса послала бы 1. Зная значение бита a Боб отсекает часть возможных входов Алисы и таким образом сужает множество возможных с его точки зрения клеток. При этом с точки зрения внешнего наблюдателя после каждого сообщения сужается либо множество возможных строк, либо множество возможных столбцов, и таким образом множество возможных клеток сужается на некоторую подматрицу матрицы M. Таким образом, становится понятно, что конечным разультатом должно быть разбиение матрицы M на одноцветные комбинаторные прямоугольники.

Определение 1.1

Точное расстояние Хэмминга $\mathrm{EHD}_k(x,y) = 1$ тогда и только тогда, когда расстояние Хэмминга (количество различающихся битов) между x и y равно k, где $x,y \in \{0,1\}^n$.

Определение 1.2

Функция $\mathrm{EQ}_n\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ проверяет две битовые строки длины n на равенство: $\mathrm{EQ}_n(x,y) = 1$ тогда и только тогда, когда $x = y$.

Существует множество различных моделей общения между Алисой и Бобом. В данной работе мы будем использовать модель с оракулом. В этой модели Алиса и Боб отправляют сообщения третьему игроку Чарли, выполняющему роль оракула, он вычисляет некоторую функцию g и отправляет результат игрокам, цель Алисы и Боба — вычислить с помощью Чарли функцию f.

Одним из наиболее исследованных оракулов в коммуникационной сложности является задача равенства EQ. В коммуникационной сложности с оракулом EQ Алиса и Боб каждый раунд отправляют некоторые битовые строки третьему игроку, Чарли, который сообщает в ответ, равны ли они.

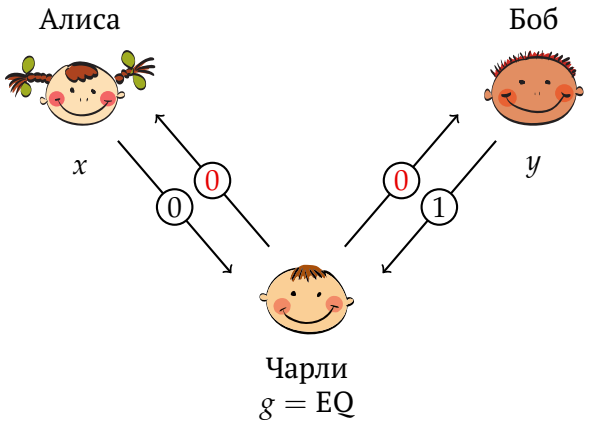

Рис. 1. Общение Алисы и Боба с оракулом Чарли.

Определение 1.3

Будем обозначать за $C^g(f)$ коммуникационную сложность функции f с оракулом g, т.е. минимальное количество раундов, необходимых Алисе и Бобу для вычисления функции f с оракулом g.

Задача 1.1

Оценка сложности $C^{\mathrm{EQ}}(\mathrm{EHD}_k)$ в зависимости от k.

Задача 1.2

Оценка сложности $C^{\mathrm{EHD}_\ell}(\mathrm{EHD}_k)$.

2 Результаты

Для начала давайте построим план доказательства. Мы хотим использовать меру введенную в определении. Идея заключается в том, что меру у начальной матрицы мы знаем, меру у 1-прямоугольника мы, наверное, как-то сможем оценить (впоследствии мы

это увидим). Если мы научимся уменьшать меру в какое-то небольшое количество раз (с помощью разбиения на одноцветные прямоугольники матрицы оракула), то сможем оценить количество раундов, необходимых для того чтобы мера стала достаточно маленькой.

Определение 2.1

Пусть $\mu(R) = \dfrac{g(R)}{p(R)}$, где R — это комбинаторный прямоугольник, $g(R)$ — количество 1 в прямоугольнике R в матрице f, $p(R)$ — полупериметр данного прямоугольника.

Лемма 2.1

Существует разбиение матрицы оракула прямоугольника R на одноцветные прямоугольники такое, что для какого-то прямоугольника разбиения R_i:

$$\mu(R_i) \geqslant \frac{\mu(R)}{5}.$$

Лемма 2.2

Для любого 1-прямоугольника R матрицы EHD_k, верно $|R| \leqslant 3^k\binom{n}{k}$.

Доказательство. Идею доказательства данного утверждения можно прочитать тут. В данной статье было доказано более слабое утверждение $|R| \leqslant 2n^k$. Обозначим $f(k,n) = 2n^k$ Заметим, что данное доказательство работает и с нашей функцией $h(k,n) = 3^k\binom{n}{k}$.

В базе $(k = 1)$ было доказано, что 1-прямоугольники - это либо полоска $1 \times b$, где $b \leqslant n$, либо квадрат 2×2. Заметим, что $\max(4,n) \leqslant 3^1\binom{n}{1} = 3n$, при $n \geqslant 2$ (при $n = 1$, квадарата 2×2 быть не может, поэтому неравенство $n \leqslant 3n$ верно).

Для совершения перехода нам достаточно, чтобы выполнялось следующее неравенство $3f(k,n) + f(k+1,n) \leqslant f(k+1,n+1)$. Заметим, что для нашей функции h данное неравенство верно:

$$3h(k,n) + h(k+1,n) = 3 \cdot 3^k\binom{n}{k} + 3^{k+1}\binom{n}{k+1} =$$

$$= 3^{k+1}\left(\binom{n}{k} + \binom{n}{k+1}\right) = 3^{k+1}\binom{n+1}{k+1} = h(k+1,n+1)$$

□

Лемма 2.3

$C(\mathrm{EHD}_k^n) = C(\mathrm{EHD}_{n-k}^n)$ для любой коммуникационной модели игры.

Доказательство. Пусть у Алисы и Боба есть стратегия, при котрой они за c раундов определяют значение функции EHD_k^n для входов $x, y \in \{0,1\}^n$. Теперь мы хотим построить стратегию за Алису и Боба для функции EHD_{n-k}^n. Пусть Алиса в самом начале игры инвертирует свою строку. Если мы хотим проверить, что $\mathrm{EHD}_{n-k}^n(x,y) = 1$, то достаточно проверить, что $\mathrm{EHD}_k^n(\overline{x},y) = 1$. А для EHD_k^n у нас есть стратегия за c раундов. Таким образом, мы получаем, что $C(\mathrm{EHD}_k^n) \geqslant C(\mathrm{EHD}_{n-k}^n)$. Неравенство в другую сторону получается аналогично. Значит $C(\mathrm{EHD}_k^n) = C(\mathrm{EHD}_{n-k}^n)$. □

Определение 2.2

$M(\mathrm{EHD}_k)$ — матрица соответствующая функции EHD_k.

Теорема 2.1

$C^{\text{EQ}}(\text{EHD}_k) \geqslant \frac{1}{2}\left(\log_5 \binom{n}{k} - k\log_5 3\right)$.

Доказательство. Пользуясь леммой 2.3 можно считать, что $k \leqslant \frac{n}{2}$. Рассмотирм меру μ, введенную в определении. Заметим, что $\mu(M(\text{EHD}_k)) = \frac{\binom{n}{k}\cdot 2^n}{2^{n+1}} = \frac{\binom{n}{k}}{2}$ так как для каждой строки существует ровно $\binom{n}{k}$ строк с точным расстоянием Хэмминга равным k. Всего бинарных строк длины n равно 2^n, $p(M(\text{EHD}_k)) = 2^{n+1}$. А мера 1-прямоугольника R, $R = A \times B$ ($|A| = a, |B| = b$), будет равна $\frac{ab}{a+b} \leqslant \frac{ab}{2\sqrt{ab}} = \frac{\sqrt{ab}}{2}$, по лемме 2.2 $\mu(R) = \frac{\sqrt{ab}}{2} \leqslant \frac{\sqrt{3^k\binom{n}{k}}}{2}$.

По лемме 2.1 можно разбить матрицу оракула таким образом, чтобы мера одного из прямоугольников разбиения уменьшилась не более, чем в 5 раз. Пусть $c = C^{\text{EQ}}(\text{EHD}_k)$. Тогда должно быть выполнено следующее неравенство:

$$\mu(M(\text{EHD}_k)) \leqslant 5^c\mu(R)$$

Прологарифмируем данное неравеснто:

$$c \geqslant \log_5 \frac{\mu(M(\text{EHD}_k))}{\mu(R)} \geqslant \log_5 \frac{\binom{n}{k}}{\sqrt{3^k\binom{n}{k}}} = \frac{1}{2}\log_5 \frac{\binom{n}{k}}{3^k} =$$

$$= \frac{1}{2}\left(\log_5 \binom{n}{k} - \log_5 3^k\right) = \frac{1}{2}\left(\log_5 \binom{n}{k} - k\log_5 3\right)$$

$$c \geqslant \frac{1}{2}\left(\log_5 \binom{n}{k} - k\log_5 3\right)$$

Таким образом, мы получили требуемое. Давайте преобразуем полученную оценку:

$$c \geqslant \frac{1}{2}\left(\log_5 \binom{n}{k} - k\log_5 3\right) \geqslant \frac{1}{2}\left(\log_5 (\frac{n}{k})^k - k\log_5 3\right) = \frac{1}{2}k\left(\log_5 n - \log_5 k - \log_5 3\right)$$

$$c \geqslant \frac{1}{2}k\left(\log_5 n - \log_5 k - \log_5 3\right)$$

Заметим, что такая оценка является асиптотически точной для $k = \mathcal{O}(1)$. Хочется отметить, что данная оценка имеет смысл только при $k \leqslant \frac{n}{3}$ (при $k \geqslant \frac{n}{3}$ выражение в скобках отрицательное).

Попробуем по-другому преобразовать полученное неравенство. Для этого асиптотически оценим $\binom{n}{k}$

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \approx \frac{\left(\frac{n}{e}\right)^n\sqrt{2\pi n}}{\left(\frac{k}{e}\right)^k\sqrt{2\pi k}\cdot\left(\frac{n-k}{e}\right)^{n-k}\sqrt{2\pi(n-k)}} = \frac{n^n}{k^k\cdot(n-k)^{n-k}}\cdot\sqrt{\frac{n}{2\pi k(n-k)}}$$

Здесь мы воспользовались формулой Стирлинга. Подставим полученное выражение в изначальное неравеснтво. Получаем, что

$$c \geqslant \frac{1}{2}\left(n\log_5 n - k\log_5 k - (n-k)\log_5(n-k) + \frac{1}{2}\log_5 \frac{n}{2\pi k(n-k)} - k\log_5 3\right)$$

□

Следствие 2.1

Рассмотрим полученные результаты при различных асимптотиках k.

1. $k = \mathcal{O}(n)$;
2. $k = \mathcal{O}\left(\sqrt{n}\right)$;
3. $k = \mathcal{O}(1)$.

Доказательство. 1. Подставим в последнее полученное выражение $k = \frac{n}{2}$

$$c \geqslant \frac{1}{2}\left(n\log_5 n - \frac{n}{2}\log_5\frac{n}{2} - \left(n-\frac{n}{2}\right)\log_5\left(n-\frac{n}{2}\right) + \frac{1}{2}\log_5\frac{n}{2\pi\frac{n}{2}\left(n-\frac{n}{2}\right)} - \frac{n}{2}\log_5 3\right) =$$

$$= \frac{1}{2}\left(n\log_5 2 - \mathcal{O}(\log_5 n) - \frac{n}{2}\log_5 3\right) \approx \frac{n}{2}\left(\log_5 2 - \frac{\log 5_3}{2}\right)$$

2. Подставим в первое полученное выражение $k = \sqrt{n}$

$$c \geqslant \frac{1}{2}\sqrt{n}\left(\log_5 n - \log_5\sqrt{n} - \log_5 3\right) = \frac{1}{2}\sqrt{n}\left(\frac{1}{2}\log_5 n - \log_5 3\right)\log_5 n \approx \frac{1}{4}\sqrt{n}\log_5 n$$

3. Здесь удобнее посмотреть на первое полученное неравенство:

$$c \geqslant \frac{1}{2}k(\log_5 n - \log_5 k - \log_5 3) \approx \frac{k}{2}\log_5 n$$

Тогда сразу понятно, что при $k = \mathcal{O}(1)$, данное выражение будет асиптотически равно $\mathcal{O}\left(\frac{k}{2}\log_5 n\right)$

□

Теорема 2.2

$$C^{\mathrm{EHD}_\ell}(\mathrm{EHD}_k) \geqslant \frac{\frac{1}{2}\left(\log\binom{n}{k} - k\log 3\right) - \log 2}{\log\left(2(n+1)^\ell\right)}.$$

Доказательство. В работе, на которую мы уже ссылались было сделано следующее наблюдение:

$$2^{n+1}\left(2(n+1)^{\ell+1}\right)^c \geqslant \rho(\mathcal{R}) \geqslant 2\left\lfloor\frac{\alpha}{\beta}\right\rfloor\sqrt{\beta},$$

где α — количество едениц в $M(EHD_k)$, а β — это оценка на площадь 1-прямоугольника. Заметим, что $\lfloor x\rfloor \geqslant \frac{x}{2}$, при $x \geqslant 2$. Посмотрим чему равно $\frac{\alpha}{\beta} = \frac{2^n\binom{n}{k}}{3^k\binom{n}{k}} = \frac{2^n}{3^k} \geqslant 2$, при $n \geqslant 3$. Ведь также как и в теореме 2.1 можно считать, что $k \leqslant \frac{n}{2}$. Поэтому $\left\lfloor\frac{\alpha}{\beta}\right\rfloor\sqrt{\beta} \geqslant \frac{\alpha}{2\sqrt{\beta}} = 2^{n-1}\sqrt{\frac{\binom{n}{k}}{3^k}}$

$$2^{n+1}\left(2(n+1)^{\ell+1}\right)^c \geqslant 2\left\lfloor\frac{\alpha}{\beta}\right\rfloor\sqrt{\beta} \geqslant 2^n\sqrt{\frac{\binom{n}{k}}{3^k}}$$

$$2\left(2(n+1)^{\ell+1}\right)^c \geqslant \sqrt{\frac{\binom{n}{k}}{3^k}}$$

Прологарифмируем данное неравенство:

$$\log 2 + c\log\left(2(n+1)^{\ell}\right) \geqslant \frac{1}{2}\left(\log\binom{n}{k} - k\log 3\right)$$

$$c \geqslant \frac{\frac{1}{2}\left(\log\binom{n}{k} - k\log 3\right) - \log 2}{\log\left(2(n+1)^{\ell}\right)}$$

Мы поллучили требуемое. Теперь давайте посмотрим на это неравенство асимптотически:

$$c \geqslant \frac{\frac{1}{2}\left(\log\binom{n}{k} - k\log 3\right) - \log 2}{\log\left(2(n+1)^{\ell}\right)} \geqslant \frac{\frac{1}{2}\left(\log\binom{n}{k} - k\log 3\right) - \log 2}{\log\left(4n^{\ell}\right)} \approx \frac{\frac{1}{2}\left(\log\binom{n}{k} - k\log 3\right)}{\ell\log n}$$

Числитель полученной дроби совпадает с выражением в теореме 2.1. Поэтому все оценки полученные в процессе доказательства теоремы можно получить здесь. Тогда все асипмтотики будут делиться на $\ell\log n$. Отметим, что можно считать, что $\ell \leqslant k$, так как в инном случае Алиса и Боб могут узнать значение функции за 1 раунд. Пусть у Алисы строка x, а у Боба строка y. Тогда Алиса добавит к своей строке $\ell - k - 0$, а Боб довавит к свой строке $\ell - k - 1$. Пусть они получили строки z и t. Тогда $\mathrm{EHD}_k(x,y) = 1$ тогда и только тогда $\mathrm{EHD}_\ell(z,t) = 1$. Поэтому при рассмотрении разных асимптотик k, мы также сможем оценить асимптотику ℓ.

□