

Содержание

1	Детерминированные протоколы	2
1.1	Модель вычислений и основные определения	2
1.2	Детерминированная коммуникационная сложность	3
1.3	Одноцветные декартовы прямоугольники	4
1.4	Метод трудных множества	4
2	Недетерминированные протоколы	4
3	Вероятностные протоколы	7
4	Классы коммуникационной сложности	8

1 Детерминированные протоколы

1.1 Модель вычислений и основные определения

Будем рассматривать следующую задачу. Есть два участника процесса (два человека или два компьютера), которые должны совместно вычислить значение функции $f: X \times Y \rightarrow Z$, где X, Y, Z некоторые конечные множества. В качестве Z обычно будем рассматривать множество значений бита $\{0, 1\}$. Традиционно этих участников называют Алиса и Боб, поэтому для удобства и соответствия литературе будем называть их так же. Сложность их задачи состоит в том, что аргумент, на котором необходимо посчитать значение функции, разделен на две части: у Алисы есть только $x \in X$, а у Боба только $y \in Y$.

Однако в их распоряжении есть некий абстрактный канал связи, через который они могут передавать друг другу данные. Передача по этому каналу связи может быть дорогой (или занимать значительное время), поэтому необходимо минимизировать количество битов, передаваемых в процессе вычисления функции.

Так же предполагается, что Алиса и Боб заранее знают функцию f и договариваются о протоколе - наборе соглашений о том, как и в каком порядке будет происходить обмен информацией. В коммуникационной сложности учитывается только количество передаваемых битов, а время вычислений у каждого участника игнорируется.

Определение 1 *Коммуникационным протоколом для вычисления некоторой функции $f: X \times Y \rightarrow Z$ называется ориентированное двоичное дерево, такое что:*

1. *Каждой **листовой** вершине ставится в соответствие некоторый элемент из Z .*
2. *Каждая **внутренняя** вершина помечена значением из $\{A, B\}$*
3. *Для каждой вершины v_i с пометкой A задана функция $g_i: X \rightarrow \{0, 1\}$*
4. *Для каждой вершины v_j с пометкой B задана функция $h_j: Y \rightarrow \{0, 1\}$*

5. Каждому ребру приписано значение из $\{0, 1\}$, а из каждой вершины, не являющегося листом, исходит ровно одно ребро с пометкой 0 и ровно одно с пометкой 1.

Выполнение протокола участниками вычисления начинается в корневой вершине. На каждом шаге, переход осуществляется следующим образом. Пусть пометка очередной вершины v_i равна A . Это означает, что сейчас Алиса должна применить функцию $g_i(x)$ (соответствующую вершине v_i) к ее значению x . Если результат 0, то она отправляет Бобу значение 0 и переходит по ребру с меткой 0. Аналогично с 1. Если же пометка B , то аналогично действовать должен Боб, применяя функцию $h_j(y)$ к его значению y .

Если текущая вершина это лист, то соответствующее ему значение $z \in Z$ объявляется результатом выполнения. Это отражает идею, что к этому моменту все участники знают этот ответ.

Определение 2 Протокол вычисляет функцию $f: X \times Y \rightarrow Z$, если $\forall x \in X \forall y \in Y$ при движении по графу протокола по описанным правилам исполнители попадут в лист, которому соответствует $z = f(x, y)$.

1.2 Детерминированная коммуникационная сложность

Определение 3 Сложностью коммуникационного протокола называется его глубина. Детерминированной коммуникационной сложностью функции f называется минимальная сложность коммуникационного протокола, вычисляющего f . Обозначается $CC(f)$.

Утверждение 1 Для функции $f: X \times Y \rightarrow Z$ справедливы следующие тривиальные оценки:

1. $CC(f) \leq \lceil \log |X| \rceil + \lceil \log |Y| \rceil$
2. $CC(f) \leq \lceil \log |X| \rceil + \lceil \log |Z| \rceil$
3. $CC(f) \leq \lceil \log |Y| \rceil + \lceil \log |Z| \rceil$
4. Если f сюръективна, то $CC(f) \geq \lceil \log |Z| \rceil$

Заметим, что в пункте 4 если $Z = \{0, 1\}$, то $\log_2 |Z| = 1$, а значит в случае такого множества этот метод доказательства нижней оценки не эффективен.

1.3 Одноцветные декартовы прямоугольники

Утверждение 2 Пусть Π - некоторый коммуникационный протокол, а l - произвольный его лист. Обозначим через S_l множество таких пар $(x, y) \in X \times Y$, что на входе (x, y) протокол Π остановится в листе l . Тогда $\exists A \subset X, B \subset Y$ такие что $S_l = A \times B$, а декартов прямоугольник $A \times B$ должен быть одноцветным с точки зрения значения функции f .

Определение 4 В силу конечности множеств X и Y можно занумеровать их элементы. Тогда коммуникационной матрицей будем называть матрицу M_f размера $|X| \times |Y|$, такую что каждый ее элемент $m_{ij} = f(x_i, y_j), x_i \in X, y_j \in Y \forall i, j$

Определение 5 $C^D(f)$ (англ. *Disjoint Cover*) - минимальное количество одноцветных прямоугольников, на которые можно разбить $X \times Y$. А величина $C^P(f)$ - минимально число листьев в протоколе.

Утверждение 3

$$C^D \leq C^P \leq 2^{CC(f)}$$

1.4 Метод трудных множества

Определение 6 Для функции $f: X \times Y \rightarrow Z$ множество $S \subset X \times Y$ называется трудным (*fooling set*), если

1. $\exists z \in Z \forall (x, y) \in S f(x, y) = z$
2. $\forall (x, y) \neq (x', y') \in S$ выполнено $f(x, y') \neq z$ или $f(x', y) \neq z$

Теорема 1 Пусть K - трудное множество для функции $f: X \times Y \rightarrow Z$ Тогда $CC(f) > \log(|K|)$.

2 Недетерминированные протоколы

В недетерминированном случае каждое действие не определяется однозначно. Мы считаем, что участники вычислений "угадывают" подсказки adv_a и adv_b , что позволяет им действовать эффективнее. Если подсказка оказалась удачной, то будет получен правильный ответ. Каковы бы ни была подсказка, участники не могут ошибиться, воспользовавшись ей: либо они получают верный ответ, либо не получают ответ вообще.

Определение 7 Коммуникационным недетерминированным протоколом для вычисления некоторой функции $f: X \times Y \rightarrow Z$ называется ориентированное двоичное дерево, такое что:

1. Каждой **листовой** вершине ставится в соответствие некоторый элемент из Z или $?$ - неопределенность.
2. Каждая **внутренняя** вершина помечена значением из $\{A, B\}$
3. Для каждой вершины v_i с пометкой A задана функция $g_i: X \times Adv_a \rightarrow \{0, 1\}$
4. Для каждой вершины v_j с пометкой B задана функция $h_j: Y \times Adv_b \rightarrow \{0, 1\}$
5. Каждому ребру приписано значение из $\{0, 1\}$, а из каждой вершины, не являющегося листом, исходит ровно одно ребро с пометкой 0 и ровно одно с пометкой 1.

Определение 8 Недетерминированный протокол P вычисляет функцию $f: X \times Y \rightarrow Z$ если:

1. $\forall x \in X \forall y \in Y \exists adv_a \in Adv_a \exists adv_b \in Adv_b$ такие что следуя пути, соответствующему adv_a и adv_b участники попадут в лист с меткой $f(x, y)$
2. $\forall x \in X \forall y \in Y \forall adv_a \in Adv_a \forall adv_b \in Adv_b$ такие что следуя пути, соответствующему adv_a и adv_b участники попадут в лист либо с меткой $f(x, y)$ либо с меткой неопределенности $?$.

Определение 9 Сложностью недетерминированного коммуникационного протокола называется его глубина. Недетерминированной коммуникационной сложностью функции f называется минимальная сложность коммуникационного протокола, вычисляющего f . Обозначается $NCC(f)$.

Рассмотрим матрицу функции M_f . Листьям по-прежнему соответствуют f -одноцветные прямоугольники. Однако прямоугольники могут пересекаться, так как одна и та же пара (x, y) может приводить в разные листья в зависимости от "советов". Поэтому необходимо рассмотреть не разбиение M_f , а его покрытие.

Определение 10 Назовем $cov_z(f)$ минимальное число прямоугольников, покрывающих все элементы матрицы M_f со значением z (и никакие другие). Обозначаем $cov(f)$ минимальное число f -одноцветных прямоугольников, покрывающих всю матрицу M_f ($cov(f) = \sum cov_z(f)$).

Утверждение 4 Для любой функции $f: X \times Y \rightarrow Z$ выполнено:

1. $NCC(f) \leq \lceil \log(cov(f)) \rceil + 1$
2. $cov(f) \leq 2^{CC(f)}$

Теорема 2 Для любой функции $f: X \times Y \rightarrow Z$

$$CC(f) = O(NCC(f)^2)$$

Доказательство: На самом деле докажем более точное утверждение, а именно

$$CC(f) = O(\log(cov_0(f)) \cdot (\log(cov_1(f)) + 2))$$

Зафиксируем минимальное покрытие одноцветными прямоугольниками M_f . Заметим справедливость следующего утверждения:

Утверждение 5 Два комбинаторных прямоугольника R_0 и R_1 соответствующие цветам 0 и 1 не имеют общих строк или не имеют общих столбцов.

Действительно, если бы они имели и общую строку и общий столбец, то по определению комбинаторного прямоугольника они бы пересекались, что противоречит их одноцветности.

Утверждение 6 (Следствие) Пусть R_1 прямоугольник цвета 1 из покрытия M_f . $R_0^1 \dots R_0^s$ набор прямоугольников цвета 0 из того же покрытия. Тогда R_1 либо не имеет общих строк с $k \geq \frac{s}{2}$ прямоугольниками из набора, либо не имеет общих столбцов с $k \geq \frac{s}{2}$ прямоугольниками из данного набора.

Детерминированный коммуникационный протокол будет устроен следующим образом. Он будет построен из нескольких одинаковых шагов. Изначально имеется $cov_0(f)$ прямоугольников цвета 0 покрывающих все 0. На каждом шаге Алиса и Боб будут исключать не менее половины из оставшихся к этому моменту таких прямоугольников.

Шаг будет осуществляться следующим образом. Алиса пытается найти такой прямоугольник цвета 1, что он пересекает строку x и не имеет общих столбцов не менее чем с половиной оставшихся прямоугольников цвета 0 из покрытия M_f . Если Алисе это удастся, то она сообщает номер прямоугольника Бобу. После этого они оба исключают из дальнейшего рассмотрения все прямоугольники цвета 0, не пересекающиеся по столбцам с указанным прямоугольником. Затем они переходят к следующему шагу. Иначе, если Алиса не нашла такого прямоугольника цвета 1, то она сообщает об этом Бобу. Боб в свою очередь аналогично пытается найти такой прямоугольник цвета 1, такой что он пересекает столбец y и не имеет общих строк не менее чем с половиной оставшихся прямоугольников цвета 0. Если ему это удалось, то он сообщает Алисе номер прямоугольника и совершенно аналогичным образом они исключают из дальнейшего рассмотрения все прямоугольники цвета 0, не пересекающиеся по столбцам с указанным прямоугольником. Затем они переходят к следующему шагу.

Протокол завершается, если выполнено одно из двух условий. Первое, если все прямоугольники цвета 0 были исключены в процессе работы. В этом случае ответ 1. Второе, на некотором шаге ни Алиса, ни Боб не смогли найти искомое ими множество цвета 1. В это случае ответ 0.

Покажем корректность протокола. Если $f(x, y) = 0$, то пара (x, y) должна быть покрыта хотя бы одним прямоугольником цвета 0. Согласно описанию протокола, такой прямоугольник не может быть удален ни на каком шаге. Следовательно протокол получит в результате ответ 0, что корректно. Пусть теперь $f(x, y) = 1$

Оценим коммуникационную сложность протокола. Число шагов не превосходит $\lceil \log(\text{cov}_0(f)) \rceil$, так как на каждом шаге число прямоугольников уменьшается как минимум вдвое, а изначально их $\text{cov}_0(f)$. Каждая итерация в свою очередь требует передачи номера прямоугольника и двух дополнительных битов(сообщающих об успехе/неудаче Алисы или Боба соответственно). В итоге получается коммуникационная сложность $CC(f) = O(\log(\text{cov}_0(f)) \cdot (\log(\text{cov}_1(f)) + 2)) = O(\log^2(\text{cov}(f))) = O(NCC(f)^2)$

3 Вероятностные протоколы

В вероятностном случае Алиса и Боб независимо выбирают последовательность из равномерно распределенных случайных битов $r_a = \{0, 1\}^{l_a}$

и $r_b = \{0, 1\}^{l_b}$ соответственно. Для каждой пары аргументов (x, y) появляется вероятность попасть в каждый из листов. Соответственно также появляется возможность получить неправильный ответ, однако в отличие от недетерминированного случая ответ обязательно будет получен.

Определение 11 Для каждого вероятностного протокола и входа (x, y) введем функцию вероятности ошибки протокола на заданном входе $\varepsilon(x, y)$.

Определение 12 Для $\varepsilon > 0$ вероятностной коммуникационной сложности $RCC_\varepsilon(f)$ назовем минимальную глубину вероятностного протокола, вероятность ошибки которого не превосходит ε .

Определение 13 Средней коммуникационной сложностью вероятностного протокола для фиксированных (x, y) назовем математическое ожидание числа пересылаемых битов.

Определение 14 Вероятностной коммуникационной сложностью с нулевой ошибкой $RCC_0(f)$ называется наилучшая средняя коммуникационная сложность вероятностных протоколов с нулевой ошибкой.

Утверждение 7 Для любой функции $f: X \times Y \rightarrow Z$

$$NCC(f) \leq RCC_0$$

4 Классы коммуникационной сложности

Определение 15 $P^{CC} = \{f \mid \exists k \ CC(f) \leq \log^k(n)\}$

Определение 16 $NP^{CC} = \{f \mid \exists k \ NCC(f) \leq \log^k(n)\}$