Сжатие протоколов

31 марта 2017 г.

Теорема 1. *Пусть даны функция $f(x, y)$, распределение μ на парах (x, y) и вероятностный протокол π высоты l вычисления f с вероятности ошибки не более δ в среднем по распределению μ. Тогда для каждого ε можно построить протокол вычисления f со средней длиной коммуникации*

$$O\Big(\sqrt{I_\mu(\pi)l}\log(l/\varepsilon)\Big)$$

и вероятностью ошибки не более $\delta + \varepsilon$.

Доказательство. Докажем утверждение сначала для протоколов без общих случайных битов. Прежде чем составлять новый протокол, представим работу протокола π следующим образом. Пусть для каждой вершины v дерева протокола выбрано случайное число r_v. Пусть M обозначает случайную величину, равную последовательности пересланных битов в протоколе. Будем считать, что бит, посылаемый в вершине v на высоте i равен 1, если $r_v < \Pr[M_i = 1 \,|\, M_{<i} = v, X = x, Y = y]$. Распределение тройки (X, Y, M) в этом протоколе точно такое же, как и в исходном, поэтому без ограничения общности мы можем считать, что он так и устроен.

Новый протокол работает так. Будем считать, что биты r_v доступны обоим участникам (они берутся из общего источника). На каждом шаге Алиса и Боб двигают фишку по дереву исходного протокола, стремясь к тому, чтобы она двигалась так же, как и в исходном протоколе. Алиса действует следующим образом. Пусть v_{Alice} есть текущее положение фишки с её точки зрения. Она вычисляет продолжение протокола, используя биты r_w и распределение $M \,|\, _{M_{<i}=v,X=x}$ вместо $M \,|\, _{M_{<i}=v,X=x,Y=y}$, которое ей неизвестно, для выбора следующего бита. Полученный таким

образом лист протокола обозначим через $C_{\text{Alice}}(v_{\text{Alice}})$. Аналогичным образом Боб определяет $C_{\text{Bob}}(v_{\text{Bob}})$. Затем они находят наименьшее i, в котором различаются последовательности $C_{\text{Alice}}(v_{\text{Alice}})$ и $C_{\text{Bob}}(v_{\text{Bob}})$, используя для этого вероятностный протокол $\text{LCP}(l, \varepsilon/l^2)$ с общими случайными битами и вероятностью ошибки не более ε/l^2 для нахождения первого различия в битовых словах длины l. После этого Алиса смещает свою фишку в вершину $C_{\text{Alice}}(v_{\text{Alice}})_{\leqslant i}$, если в этой вершине ее очередь входа, и в ее брата $C_{\text{Bob}}(v_{\text{Bob}})_{\leqslant i}$ иначе (поскольку она считает, что правильный i бит у Боба, а не у неё). Аналогичным образом действует Боб. Когда они дойдут до листа, каждый выдаст пометку того листа, в который он пришёл.

Объясним смысл этого протокола. Допустим, что в данный момент фишка у Алисы и Боба находится в одной вершине, то есть, $v_{\text{Alice}} = v_{\text{Bob}}$. Пусть, скажем, в этой вершине сообщение должна посылать Алиса. Тогда распределения случайных величин $M \mid_{M_{<i}=v, X=x}$ и $M \mid_{M_{<i}=v, X=x, Y=y}$ совпадают, поэтому Алиса первое движение фишки у Алисы будет правильным. Если у Боба i-ый бит последовательности тот же, что и у Алисы, то его первое движение будет правильным. Таким образом, у обоих движение фишки будет правильным до того места, где их последовательности расходятся. В этом месте тот, у которого позиция неправильна, скорректирует её. В этом рассуждении мы считаем, что протокол LCP выдал правильный ответ. Поскольку всего будет не более l вызовов LCP, для всех x, y, r с вероятностью не менее чем $1 - l(\varepsilon/l^2) \geqslant 1 - \varepsilon$ они сдвинут фишку в один и тот же лист — тот самый, в который пришёл бы и исходный протокол при этих x, y, r. Значит вероятность правильной работы построенного протокола не меньше $(1 - \delta)(1 - \varepsilon) \geqslant 1 - \varepsilon - \delta$.

Осталось оценить среднее число переданных бит. Оно равно среднему количеству вызовов протокола LCP, умноженному на его коммуникационную сложность. Поэтому нам нужно оценить среднее количество вызовов LCP. Сначала сделаем это, предполагая, что LCP не дает ошибки. В этом случае фишки Алисы и Боба двигаются одинаково — вдоль того пути, который получился бы в исходном протоколе. Всякий раз (кроме последнего), когда мы вызываем LCP, мы находим новое i для которого i-ые биты последовательностей $C_{\text{Alice}}(M_{<i})$ и $C_{\text{Bob}}(M_{<i})$ различаются (в самом деле, если первый различный бит последовательностей $C_{\text{Alice}}(M_{\leqslant j})$ и $C_{\text{Bob}}(M_{\leqslant j})$ равен i, то последовательности $C_{\text{Alice}}(M_{<i})$ и $C_{\text{Bob}}(M_{<i})$ различаются в i-ом бите). Поэтому нам надо оценить среднее количество таких i, что i-ые биты последовательностей $C_{\text{Alice}}(M_{<i})$ и $C_{\text{Bob}}(M_{<i})$ раз-

личаются, то есть среднее значение суммы

$$\sum_{i=1}^{l} \mathrm{E}_{m \leftarrow M} \Pr[i\text{-ые биты последовательностей } C_{\mathrm{Alice}}(m_{<i}) \text{ и } C_{\mathrm{Bob}}(m_{<i}) \text{ различаются}].$$

По построению протокола i-ое слагаемое в этой сумме равно среднему значению по x, y, v статистического расстояния между распределениями $M_i \mid_{M_{<i}=v, X=x}$ и $M_i \mid_{M_{<i}=v, Y=y}$. Оценка этого среднего следует из такой леммы:

Лемма 1. *Пусть дано $i \leqslant l$. Тогда среднее по вершинам v на высоте i в дереве протокола π и по x, y статистического расстояния между распределениями $M_i \mid_{M_{<i}=v, X=x}$ и $M_i \mid_{M_{<i}=v, Y=y}$ не превосходит*

$$\sqrt{I(M_i : X \mid M_{<i}, Y) + I(M_i : Y \mid M_{<i}, X)}.$$

Доказательство. В виду вогнутости корня, нам достаточно доказать, что для фиксированных v, x, y статистическое расстояние между распределениями $M_i \mid_{M_{<i}=v, X=x}$ и $M_i \mid_{M_{<i}=v, Y=y}$ не превосходит

$$\sqrt{I(M_i : X \mid M_{<i} = v, Y = y) + I(M_i : Y \mid M_{<i} = v, X = x)}.$$

Будем различать два случая.

Случай 1: в вершине v бит посылает Алиса. Тогда второе слагаемое под корнем равно нулю. Кроме того, распределение $M_i \mid_{M_{<i}=v, X=x}$ совпадает с распределением $M_i \mid_{M_{<i}=v, X=x, Y=y}$. По неравенству Пинскера, статистическое расстояние между последним и распределением $M_i \mid_{M_{<i}=v, Y=y}$ не превосходит корня из $I(M_i : X \mid M_{<i} = v, Y = y)$, что и требовалось установить.

Случай 2: в вершине v бит посылает Боб. Тогда, наоборот, первое слагаемое под корнем равно нулю и можно применить неравенство Пинскера. □

Из леммы и цепного правила следует, что среднее по x, y, m (где m — лист протокола π) суммы по i статистических расстояние между распределениями $M_i \mid_{M_{<i}=m_{<i}, X=x}$ и $M_i \mid_{M_{<i}=m_{<i}, Y=y}$ не превосходит $\sqrt{I_\mu(\pi) l}$.

Вспомним, что мы предполагали, что протокол LCP не ошибается. Насколько его ошибки могут увеличить среднее значение количества встреченных различий. Мы только что доказали, что среднее количество встреченных различий при условии, что ошибки не было, не больше

$\sqrt{I_\mu(\pi)l}$. Вероятность того, что ошибка была не больше ε/l. Среднее значение количества встреченных различий при условии, что ошибка была, очевидно не больше l, поэтому в целом среднее количество встреченных различий не больше $\sqrt{I_\mu(\pi)l} + l(\varepsilon/l) \leqslant \sqrt{I_\mu(\pi)l} + 1$.

Как изменятся наши подсчеты для протоколов, имеющих (кроме частных) и общие случайные биты. Пусть π — такой протокол. При фиксации общих случайных битов получается протокол π_r без общих случайных битов. Для таких протоколов мы уже доказали, что среднее количество различий не больше $\sqrt{I_\mu(\pi_r)l}$. Пользуясь вогнутостью корня, мы можем заключить, что среднее по r значение этой величины не больше $\sqrt{I_\mu(\pi)l}$, что и требовалось доказать. $\square$