Лекция 15

Уменьшение количества раундов в протоколе Артура и Мерлина

(Конспект: Н. Карпов)

Для начала заметим, что мы можем считать, что Мерлин — это функция. Действительно, Мерлин способен промоделировать работу всего протокола, и, если Мерлин хочет нас обмануть (убедить), он может выбирать наилучшее для себя сообщение, зависящее только от входа и уже известных случайных битов Артура, выбирая наилучшую для себя (в смысле вероятности успеха) ветку протокола, в которую сообщение отправит Артура.

Лемма 15.1. *Обозначим за $w(x, r_1, \ldots, r_t)$ ответ Мерлина на входе x на шаге $2t$, который Мерлин отправляет после того, как Артур пошлет до этого r_t — строчку случайных битов.*

За $A(x, r_1, w(r_1), \ldots, r_k, w(x, r_1, \ldots, r_k))$ обозначим результат проверки протокола Артуром.

Пусть в протоколе Артура и Мерлина выполнено для некоторого $\epsilon > 0$ следующее:

$$\exists w_G \; \forall x \in L \; P\{A(x, r_1, w_G(x, r_1), \ldots, w_G(x, r_1, \ldots, r_k)) = 1\} > \frac{1}{2} + \epsilon,$$

$$\forall w_B \; \forall x \notin L \; P\{A(x, r_1, w_B(x, r_1), \ldots, w_B(x, r_1, \ldots, r_k)) = 1\} < \frac{1}{2} - \epsilon.$$

Тогда можно построить протокол и алгоритм проверки Артура $\tilde{A}$ удовлетворяющий свойствам:

$$\exists \tilde{w}_G \; \forall x \in L \; P\{\tilde{A}(x, r_1, \tilde{w}_G(x, r_1), \ldots, \tilde{w}_G(x, r_1, \ldots, r_k)) = 1\} > 1 - 2^{-p(n)},$$

$$\forall \tilde{w}_B \ \forall x \notin L \ P\{\tilde{A}(x, r_1, \tilde{w}_B(x, r_1), \ldots, \tilde{w}_B(x, r_1, \ldots, r_k)) = 1\} < 2^{-p(n)},$$

где $p(n)$ — полиномиально ограниченная функция.

Доказательство. Опишем новый протокол. Запустим протокол на $c{\cdot}p(n)$ (c выберем потом) независимых случайных досках, в конце выберем ответ, который чаще всего получил Артур при проверке, и выдадим его.

Остаётся оценить вероятности.

Заметим, что выбор любого Мерлина, который "видит" случайные биты на других досках, мы можем заменить на выбор Мерлина, который не зависит от случайных битов на других досках, и при этом играет не хуже. Действительно, ведь решение Артура принять слово не зависит от случайных битов на других досках и монотонно зависит от исходов игр на отдельных досках, значит, выбор Мерлина можно определять только случайными битами на его доске (на каждой отдельной доске его цель — максимизировать вероятность принятия на ней, поэтому при принятии решения можно формально заменить в его функции информацию о других досках теми значениями, которые максимизируют вероятность принятия на данной доске, от этого вероятность успеха Мерлина только увеличится, что бы ни происходило на других досках в реальности).

Тогда если мы обозначим за $X_i = A(x, r_1^i, w(x, r_1^i) \ldots, r_k^i, w(x, r_1^i, \ldots, r_k^i))$, где r_k^i — это случайные строчки на доске i, мы знаем, что при $x \in L$ имеется w, для которого $E\{X_i\} > \frac{1}{2} + \epsilon$, а при $x \notin L$ для всякого w справедливо $E\{X_i\} < \frac{1}{2} - \epsilon$. Тогда если $x \in L$, то

$$P\{\sum_i^{c\cdot p(n)} X_i < \frac{c{\cdot}p(n)}{2}\} < 2^{-\alpha(\epsilon)cp(n)}.$$

Последнее верно как прямое применение неравенства Чернова. Аналогично вероятность оценивается в случае $x \notin L$. Выбрав $c = \frac{1}{\alpha(\epsilon)}$, мы получим нужный нам результат. □

Теорема 15.1. *Для полиномиально ограниченной функции $t(n) \geq 2$,* $\mathbf{AM}[2t(n)] = \mathbf{AM}[t(n) + 1]$.

Доказательство. Пусть Π_1 — это протокол на входе длины n, состоящий из $t = 2t(n)$ раундов. Будем пока предполагать, что t кратно 4. Мы будем моделировать протокол Π_1 протоколом Π_2, состоящим из $\frac{t}{2} + 1$ раунда. Будем считать, что у Π_1 вероятность ошибки $\epsilon = (24t)^{-t}$ (по лемме лемме 15.1) . Пусть теперь s — это суммарный размер пересылаемых сообщений, тогда выберем $m = 4st$. Для удобства мы можем предполагать, что $s > n$.

Моделирование будет происходить следующим образом. Мы разделим протокол на $\frac{t}{4}$ блока вида $AMAM$, потом в каждом таком блоке часть MAM заменим на AMA. То есть из $AMAM\ AMAM\ \cdots\ AMAM$ мы получим $AAMA\ AAMA\ \cdots\ AAMA$, что, в свою очередь, то же самое, что $AM\ AM\ \cdots\ AMA$.

Рассмотрим одну из частей MAM протокола Π_1. Она состоит из выбора Мерлином строки $x \in X$, после этого Артур случайным образом выбирает строку $y \in Y$, и по ним Мерлин выбирает строчку $z \in Z$. Тогда соответствующие части Π_2 будут выглядеть следующим образом: Артур посылает случайные строки $y_1, \cdots, y_m \in Y$, Мерлин посылает строку $x \in X$ и строки $z_1, \cdots, z_m \in Z$, затем Артур выбирает случайное $1 \leq i \leq m$ и говорит, что продолжает протокол так, как если бы в протоколе Π_1 y был равен y_i и z равен z_i. Иначе говоря, мы запускаем эту часть протокола на параллельных досках, а потом выбираем случайную из досок и продолжаем игру.

Так мы поступим с каждым из блоков. Очевидно, что размер протокола Π_2 будет полиномиален от n. Понятно, что шансы Мерлина при таком протоколе доказать Артуру принадлежность не ухудшатся. Мерлин в каждом из блоков будет присылать Артуру оптимальное x из исходного протокола, не обращая внимания на y_i, а далее присылать оптимальные z_i; поскольку i Артур выбирает случайно, вероятность при таком поведении Мерлина не изменится. Следовательно стоит только беспокоиться, не сможет ли Мерлин сильно увеличить шансы убедить Артура.

Обозначим за $f_H(x, y, z)$ вероятность, что Мерлин убедит Артура после соответствующей фазы MAM в протоколе Π_1, при предыдущей истории H. Пусть в исходном протоколе на момент начала фазы MAM вероятность того, что Мерлин обманет Артура, составляла $f_H^0 = \delta$. Оценим вероятность того, что комплект выбранных строк y_i столь плох, что для многих из них Мерлин может подобрать z_i, существенно увеличивающие вероятность убедить Артура.

Лемма 15.2. *За $C(y_1, \cdots, y_m)$ обозначим событие*

$$\exists x \in X\ |\{i : \max_{z_i} f_H(x, y_i, z_i) > 12t\delta\}| > \frac{m}{2t}.$$

Тогда для случайных $y_1, \ldots, y_m$

$$P\{C(y_1, \cdots, y_m)\} < |X| 2^{-\frac{m}{2t}}.$$

Доказательство. Обозначим за $f_H^2(x, y)$ вероятность, что Мерлин выиграет при выбранных x, y. Тогда $\forall x P_y\{f_H^2(x, y)\} \leq \delta$. Таким образом, по неравенству Маркова $P_y\{f_H^2(x, y) > 12t\delta\} < \frac{1}{12t}$. Тогда вероятность

плохого события $B(x,\vec{y})$, "$f_H^2(x,y_i) > 12t\delta$ случается более $\frac{m}{2t}$ раз из m возможных" (для фиксированного x и случайно выбранных y_i), меньше чем

$$\binom{m}{\frac{m}{2t}}(12t)^{-\frac{m}{2t}} < \left(\frac{2et}{12t}\right)^{\frac{m}{2t}} < 2^{-\frac{m}{2t}}.$$

(Тут мы пользовались неравенством $\binom{n}{k} < \left(\frac{ne}{k}\right)^k$.)

Заметим, что $C(\vec{y}) = \exists x B(x,\vec{y})$, тогда $P\{C(\vec{y})\} \leq \sum\limits_{x\in X} P\{B(x,\vec{y})\}$. Но мы выбрали параметр s и m, так чтобы $|X| \leq 2^s$ и $s > n$, а $m = 4st$, следовательно, $P\{C(\vec{y})\} \leq 2^{s-\frac{m}{2t}} = 2^{-s} < 2^{-n}$. □

Мы уже имеем все, чтобы оценить вероятность того, что Мерлин обманет Артура в протоколе Π_2. Вероятность того, что на какой-то фазе $AMAM$ Мерлин увеличит вероятность успеха хотя бы в $12t$ раз в $\frac{m}{2t}$ случаев, не превосходит 2^{-s}. Получаем, что вероятность того, что на каком-то этапе Мерлин получит более чем $\frac{m}{2t}$ строк y_i, для которых вероятность успеха Мерлина сильно повысится, не превосходит $\frac{t}{4}2^{-s} \leq \frac{t}{4}2^{-t}$. В каждом раунде Артур с вероятностью не более чем $\frac{1}{2t}$ выберет версию протокола, в которой вероятность увеличилась более чем в $12t$ раз. Тогда, если каждый шаг увеличивает вероятность успеха Мерлина не более чем в $12t$ раз, в конце вероятность успеха составит не более $\epsilon(12t)^{\frac{t}{4}}$. Но мы взяли $\epsilon = (24t)^{-t}$, что значит, что в конце вероятность успеха будет не более чем $(\frac{12t}{24^4t^4})^{\frac{t}{4}}$. В итоге вероятность того, что Мерлин обманет Артура, будет не более

$$\frac{t}{4}2^{-t} + \frac{t}{4}\frac{1}{2t} + \left(\frac{1}{27648t^3}\right)^{\frac{t}{4}} \leq \frac{1}{2e} + \frac{1}{8} + \frac{1}{16} \leq \frac{7}{16}.$$

Заметим, что если t не делится на 4, а делится только на два, мы можем сделать то же самое, только с первыми $\frac{t-2}{4}$ четверками. Сгруппировав раунды Артура и Мерлина, мы вновь получим $\frac{t}{2}+1$ раунд. □

Теорема 15.2. $\forall k \geq 2$ $\mathbf{AM}[k] = \mathbf{AM}$.

Доказательство. Применяя операцию сокращения из предыдущей теоремы, мы можем сокращать число раундов (если число раундов на каком-то этапе становится нечетным, мы можем добавлять фиктивный раунд Мерлина). Так мы сделаем константое число раз, пока не дойдем до момента, когда раундов останется три.

Теперь нам остается убрать последний раунд Артура. Из доказательства предыдущей теоремы видно, в чем состоит последний раунд Артура:

Артур выбирает случайную версию из m игр и выдает результат протокола на ней; причём с хорошей вероятностью в $\frac{3}{4}$ версий протокола ответ правильный. Тогда просто переберем каждый из m вариантов раунда и выдадим самый частый ответ. □