Лекция 6

Доказательства с нулевым разглашением (*zero-knowledge*)

(Конспект: И. Монахов)

6.1 Интерактивные системы доказательств

Определение 6.1. Для пары алгоритмов V и P, обменивающихся сообщениями по протоколу $c(V, P)$, таких что алгоритм P (решатель) произвольный, а V (верификатор) полиномиальный вероятностный, обозначим через $\langle V, P\rangle(x)$ случайную величину, которая является последним сообщением от верификатора V в последовательсности сообщений $view(c(V(x), P(x)))$, где x – общая строчка входа V и P. Назовём (V, P) *интерактивной системой доказательств* для языка L, если

1. (V, P) полная: верификатор V принимает с ограниченной вероятностью ошибки доказательство решателя P для любой теоремы $x \in L$

$$\forall x \in L \quad \Pr\{\langle V, P\rangle(x) = 1\} \geq \frac{3}{4}.$$

2. (V, P) корректная: верификатор V отвергает с ограниченной вероятностью ошибки доказательство решателей P^* для всех строчек не из L

$$\forall x \notin L \quad \Pr\{\langle V, P^*\rangle(x) = 0\} \geq \frac{3}{4}.$$

Пример 6.1. Рассмотрим язык `NGI`, состоящий из пар неизоморфных простых конечных графов. Следующий протокол будет интерактивным доказательством с нулевым разглашением для `NGI`:

- Общий вход решателя P и верификатора V: два простых конечных графа $G_1 = (V_1, E_1)$ и $G_2 = (V_2, E_2)$.

1. • V: выбирает случайную перестановку π и случайный номер $i \in \{1,2\}$; отправляет P граф $\widetilde{G}_i = (\widetilde{V}_i, \widetilde{E}_i)$, изоморфный графу G_i:

$$\forall u, v \in V_i \;\; e(u,v) \in E_i \Leftrightarrow e(\pi(u), \pi(v)) \in \widetilde{E}_i.$$

   • P: вычисляет номер i', такой что граф $G_{i'}$ изоморфен графу $\widetilde{G}_i$ и отправляет этот номер V.

2. • V: если $i = i'$, отправляет 1, иначе отправляет 0.

   • P: завершает протокол, отправив $\emptyset$.

3. • V: если нечестный решатель P^* не прислал пустое сообщение, завершает протокол, отправив $\emptyset$.

   • P^*: нет ограничений.

Пример 6.2. Рассмотрим язык `GI`, состоящий из пар изоморфных простых конечных графов. Интерактивное доказательство с нулевым разглашением для `GI` будет немного сложнее:

- Общий вход решателя P и верификатора V: два простых конечных графа $G_1 = (V_1, E_1)$ и $G_2 = (V_2, E_2)$. Для номера $i \in \{1,2\}$ обозначим через σ_i некоторый изоморфизм между графами G_i и G_{3-i}, если графы изоморфны, иначе это тождественное отображение. И пусть $\sigma_{3-i} = \sigma_i^{-1}$.

1. • V: пропускает свою очередь, посылая сообщение 0.

   • P: выбирает случайную перестановку π и случайный номер $i \in \{1,2\}$, отправляет V граф $\widetilde{G}_i = (\widetilde{V}_i, \widetilde{E}_i)$, изоморфмный графу G_i:

$$\forall u, v \in V_i \;\; e(u,v) \in E_i \Leftrightarrow e(\pi(u), \pi(v)) \in \widetilde{E}_i.$$

2. • V: выбирает случайный номер $i' \in \{1,2\}$ и отправляет граф $G_{i'}$, чтобы P прислал изоморфизм $G_{i'}$ с $\widetilde{G}_i$.

   • P: если $i' = i$, тогда отправляет перестановку $\psi = \pi$, иначе отправляет перестановку $\psi = \pi \circ \sigma_{i'}$.

3. • V: если ψ – изоморфизм $G_{i'}$ с $\widetilde{G}_i$, тогда отправляет 1, иначе отправляет 0.

   • P: завершает протокол, отправив $\emptyset$.

4. • V: если нечестный решатель P^* не прислал пустое сообщение, завершает протокол, отправив $\emptyset$.

   • P^*: нет ограничений.

6.2 Формальное определение

Дадим теперь формальное определение понятие интерактивной системы доказательств с нулевым разглашением и покажем, что приведённые выше примеры систем доказательств для задач `GI` и `NGI` ему удовлетворяют.

6.2.1 Совершенно нулевое разглашение

Суть нулевого разглашения заключается в том, что любой нечестный верификатор V^*, который попытается получить от решателя P дополнительные знания, притворившись верификатором V, ничего не узнает. Запишем это формально.

Определение 6.2. Будем называть интерактивную систему доказательств (V, P) для языка L системой доказательств с *совершенным неразглашением*, если для любого полиномиального вероятностного вероятностного верификатора V^* существует полиномиальный вероятностный *симулятор* M^*, такой что

$$\forall x \in L \, \forall s \in \{0,1\}^* \quad \Pr\left[M^*(x) = s\right] = \Pr\left[\langle V^*, P\rangle(x) = s\right].$$

Замечание 6.1. Условия совершенного неразглашения оказываются слишком строгим: не удаётся привести пример ни одного языка L и интерактивной системы доказательств для него с совершенным неразглашением, чтобы $L \notin \mathbf{BPP}$. А вот следующее определение систем доказательств с совершенно нулевым разглашением лишено такого недостатко, потому что для задачи `GI` известна такая интерактивная система доказательств, и неизвестно $\texttt{GI} \in^? \mathbf{BPP}$.

Определение 6.3. Будем называть интерактивную систему доказательств (V, P) для языка L системой доказательств с *совершенно нулевым разглашением*, если для любого полиномиального вероятностного верификатора V^* существует полиномиальный вероятностный *совершенный симулятор* M^*, такой что для любой строчки $x \in L$ выполняются условия:

1. $\Pr[M^*(x) = \perp] \leq \frac{1}{2}$.
2. $\forall s \in \{0,1\}^* \quad \Pr\left[M^*(x) = s \;\middle|\; M^*(x) \neq \perp\right] = \Pr\left[\langle V^*, P\rangle(x) = s\right]$.

Класс языков, для которых существуют системы доказательств с совершенно нулевым разглашением, будем обозначать **PZK**.

Замечание 6.2. Если в определении системы доказательств с нулевым разглашением вместо случайной величины $\langle V^*, P\rangle(x)$ взять случайную величину $view(c(V^*(x), P(x)))$, то ничего не изменится.

6.2.2 Вычислительно нулевое разглашение

Ещё более широким классом языков являются языки, для которых есть интерактивные системы доказательств с вычислительно нулевым разглашением. На следующей лекции будет доказано, что этот класс содержит **NP**-полную задачу, а значит и весь класс **NP**.

Определение 6.4. Будем называть интерактивную систему доказательств (V, P) для языка L системой доказательств с *вычислительно нулевым разглашением*, если для любого полиномиального вероятностного верификатора V^* существует полиномиальный вероятностный *симулятор* M^*, такой что $\forall x \in L$ случайные величины $\langle V^*, P\rangle(x)$ и $M^*(x)$ вычислительно неразличимы.

Класс языков, для которых существует системы доказательств с вычислительно нулевым разглашением, будем обозначать **CZK**.

Упражнение 6.1. Доказать, что **PZK** $\subseteq$ **CZK**.

Теорема 6.1. *Язык всех пар изоморфных графов* GI $\in$ **PZK**.

Доказательство. Пара алгоритмов (V, P), описанных в примере 6.2, образует интерактивную систему доказательств с совершенно нулевым разглашением. Пусть время работы нечестного верификатора V^* ограничено некоторым полиномом q от длины входа $n = |x|$. Рассмотрим следующий симулятор M^*, состоящий из двух подпрограмм M_1 и M_2:

- Вход симулятора M^*: два графа $G_1 = (V_1, E_1)$ и $G_2 = (V_2, E_2)$.

1. - M_1: выбирает случайную строку $r \leftarrow U_{\{0,1\}^{q(n)}}$ и моделирует V^* со случайными битами r, пока тот не запросит первое сообщение решателя P, отправив сообщение 0.
   - M_2: выбирает случайную перестановку π и случайный номер $i \in \{1, 2\}$, отправляет M_1 граф $\widetilde{G}_i = (\widetilde{V}_i, \widetilde{E}_i)$, изоморфмный графу G_i:
   $$\forall u, v \in V_i \;\; e(u, v) \in E_i \Leftrightarrow e(\pi(u), \pi(v)) \in \widetilde{E}_i.$$
2. - M_1: продолжает моделировать верификатор V^* до отправки $G_{i'}$.
   - M_2: если $i' = i$, тогда отправляет перестановку $\psi = \pi$,
     иначе выдаёт $\perp$ и останавливается.
3. - M_1: продолжает моделировать верификатор V^* до отправки 1 или 0.
   - M_2: завершает протокол, отправив $\emptyset$. Выдаёт $view(c(M_1(x), M_2(x)))$ и останавливается.

Так как при $x \in$ GI графы G_1 и G_2 изоморфны, то $\Pr[M^*(x) = \perp] = \frac{1}{2}$.

Докажем, что для любого $s \in \{0, 1\}^*$

$$\Pr\left[M^*(x) = s \;\middle|\; M^*(x) \neq \perp\right] = \Pr\left[view(c(V^*(x), P(x))) = s\right].$$

НУО будем считать, что $s = (0, \widetilde{G}_i, G_{i'}, \psi, b)$, где $b \in \{0, 1\}$, так как иначе M_2 останавливает M^* и выдаёт $\perp$. Требуемое утверждение следует из того, что существует биекция между событиями вероятностных пространств, заданных программами V^* и M^*. $\square$