Зачетные задачи

Зотов Алексей 497

May 25, 2017

Задача. ***1****. Построить систему интерактивных доказательств для языка* GI-NO-EQUAL-CLASSES $= \{(G_1, \dots G_m) \mid$ *в разбиении этого набора графов на классы эквивалентности по отношению изоморфизма нет двух классов одинакового размера*$\}$

Ответ. Мы уже знаем, что $\mathsf{GNI} \in \mathbf{IP}$ и будем это использовать. Также $\mathsf{GI} \in \mathbf{NP}$. $M = \{1, \dots, m\}$

Рассмотрим такой протокол :

1. $\forall i \in 1, \dots, m$ верификатор V посылает пруверу P индекс i соответствующий G_i.
2. P возвращает $X_i = \{(k, S_{ki}) | G_k \cong G_i\}$ - множество индексов графов, изоморфных G_i и соответствующие сертификаты изоморфности. $X_i = (K_i, S_i)$ - обозначение.
3. V проверяет полученные сертификаты.
4. $\forall j : j \notin K_i$ верификатор V инициирует протокол проверки $(G_i, G_j) \in \mathbf{GNI}$), с вероятностью ошибки $p_{ij} \leq \frac{1}{3}$.
5. Алгорим повторяется с пункта (1), игнорируя те индексы, для которых уже найден класс изоморфности.
6. V проверяет, что все классы получились разного размера. Возвращает True, если на каждый шаг протокола корректный (проверка сертификатов, проверка на $G_i \ncong G_j$), и полученные классы разного размера. Иначе False.

Докажем, что алгоритм корректен:

- если $X = (G_1, \dots G_m) \in$ GI-NO-EQUAL-CLASSES, тогда каждый на каждой итерации прувер будет действовать корректно, положительная проверка на изоморфность и неизоморфность проходит без ошибок (с вероятностью 1).
- если $X = (G_1, \dots G_m) \notin$ GI-NO-EQUAL-CLASSES, тогда P не может неизоморфные графы отнести в один класс(т.к. проверка сертификатов детерминированная), но может попробовать изоморфные графы разбить по разным классам, воспользовавшись наличем ошибки при проверке $G_i \ncong G_j$. На каждой такой проверке вероятность обмануть верификатор $p_{ij} \leq \frac{1}{3}$. Значит вероятность ошибочно принять X: $P_{\text{err}} \leq \frac{1}{3}$.

Задача. ***4****. Постройте систему интерактивных доказательств с общими случайными битами для языка* GROUP-NI $= \{G_0, G_1 \mid G_0,\ G_1 -$ *табилцы умножения двух неизоморфных конечных групп*$\}$

Ответ. Проверить, что данные таблицы это таблицы умножения групп, верификатор может без прувера за $O(n^2)$. Достаточно проверить *ассоциативность, наличие единицы и обратимость всех элементов.* Нужно проверить их неизоморфность.
Рассмотрим $S = \{(H, \sigma) | H \cong G_i, i \in \{0, 1\}, \sigma \in \text{Aut}H\}$. Тогда, если $G_0 \cong G_1$, то $|S| = n!$, иначе $|S| = 2 \cdot n!$. Каждую группу порядка n можно записать двоичным числом длины m, где $m = p(n)$. Обозначим $K = 2n!$, имеем $S \subset \{0, 1\}^m$. Выберем k таким, что $2^{k-2} \leq K \leq 2^{k-1}$. Рассмотрим такой протокол:

- V выбирает случайную хэш-функцию h из семейства попарно независимых полиномиально вычислимых(от m, k) хеш-функций $H_{m,k} : 2^{\mathbf{m}} \to 2^{\mathbf{k}}$. Также выбирает случайный $y \in 0, 1^k$. Отправляет пруверу P пару (h, y) (значит можно считать,что случайные биты - общие).

- P выбирает $x \in S : h(x) = y$. Возвращает верификатору пару (x, s), где s - сертификат $x \in S$.
- V проверяет сертификат s и $h(x) = y$. Принимает доказательство если проверки корректные.

Покажем корректность протокола. Пусть $p = \frac{|S|}{2^k}$.

- $P_{h,y}\{\exists x \in S : h(x) = y\} \leq p$ - так как $|h(S)| \leq |S|$.
- Рассмотрим E_x - событие $\{h(x) = y\}$. $Pr\{\cup_{x \in S} E_x\} \geq \sum_{x \in S} Pr\{E_x\} - \sum_{x < x' \in S} Pr\{E_x \cap E_{x'}\} = \frac{|S|}{2^k} - \frac{|S|(|S|-1)}{2} \frac{1}{2^{2k}} > p(1 - \frac{p}{2}) \geq\geq \frac{3}{4}p$ (так как $p \leq \frac{1}{2}$ из-за выбора p и ограничения сверху на размер S).

Получили $\frac{3}{4}p \leq P_{h,y}\{\exists x \in S : h(x) = y\} \leq p$, значит :

- Если $|S| \geq K$, то $\frac{3}{4}p_0 \leq P_{h,y}\{\exists x \in S : h(x) = y\}$
- Если $|S| \leq \frac{K}{2}$, то $P_{h,y}\{\exists x \in S : h(x) = y\} \leq p \leq \frac{p_0}{2} < \frac{3}{4}p_0$

  Для разных случаев получили некоторый вероятностый зазор, который можно увеличить полиномильным числом повторений протокола.

Задача. ***2.*** *Пусть есть $m = n(n-1)/2$ булевых схем полиномиального размера $\phi_1, \ldots, \phi_m$ со входом длины k и одним выходом. Для каждого $x \in \{0,1\}^k$ рассмотрим граф G_x на n вершинах, матрица смежности которого задана результатами работы схем ϕ_j на входе x. Рассмотрим множество графов $\mathcal{G} = \{G_x | x \in \{0,1\}^k\}$. Пусть мы хотим отделить наборы $\phi_1, \ldots, \phi_m$, когда в множестве $\mathcal{G}$ менее C различных попарно неизоморфных графов от наборов, когда их хотя бы D ($D \geq C$). Существует ли интерактивная система доказательств, которая делает это при $C = D$? Можете ли вы её построить? Если не можете, то попробуйте её построить для случая $C = D/2$.*

Ответ. Да, такой протокол существует. $\mathbf{L} = \{\{(\phi_1 \ldots \phi_m)\} : \text{в } \mathcal{G} \text{ содержится менее } D \text{ попарно неизоморфных графов}\}$. $\mathbf{L} \in \mathbf{PSAPCE}$. Можно посчитать количество классов изоморфности графов на полиномиальной памяти, для этого храним текущее число классов, для каждого не рассмотренного графа G_i, перебираем все уже рассмотренные G_j (перебор графов, или наборов булевых формул это одно и то же), если $\forall j \leq i : G_j \ncong G_i$, то увеличиваем число классов эквивалентности. Полученное число классов эквивалентности и будет ответом. Дальше сравним его с D. Значит $\mathbf{L} \in \mathbf{PSAPCE}$. Знаем $\mathbf{IP} = \mathbf{PSAPCE}$. Значит нужный протокол из $\mathbf{IP}$ существует.

Для $C = D/2$ подойдет протокол подробно описанный выше, в задаче (4).

Задача. ***3.*** *Пусть $S \in \mathbf{NP}$. Обозначим через S_n множество $S \cap \{0,1\}^n$. Постройте систему интерактивных доказательств, получающую на вход число K, такую что если $|S_n| > K$, то прувер убеждает верификатора с вероятностью 1 (а не 2/3, как на лекции), а если $|S_n| < K/2$, то прувер убеждает с вероятностью не больше 1/3. Можно ли заменить $K/2$ на $0.99K$? (Аргумент полинома во времени работы верификатора - это n).*

Ответ. Используем протокол, подробно описанный в задаче (4).

Для $0.99K$ достаточно проверять не размер множества S, а размер множества $(S \times S \times \ldots \times S) = S^l$, которое очевидно лежит в $\mathbf{NP}$, l выбираем так, что $0.99^l \leq \frac{1}{2}$. Получаем сравнение для размеров M и K, где $\frac{1}{2}K^l \leq M \leq K^l$.

Ошибку первого рода можно до 0, так как мы получили протокол из IP, для которого в одном из эквивалентных определений соответствующая ошибка равна 0.

Задача. ***5.*** *Определим класс $\mathbf{AMA}'$ и $\mathbf{AMA}''$ так: $B \in \mathbf{AMA}'(\mathbf{AMA}'')$, если существует полиномиальный алгоритм $V(x, r, s, q)$, такой что:*

- *Если $x \in B$, то $\mathbf{Pr}_r[\exists\ s \mathbf{Pr}_q[V(x, r, s, q) = 1] \geq \frac{2}{3}] \geq \frac{2}{3}$*
- *(для $\mathbf{AMA}'$) Если $x \notin B$, то $\mathbf{Pr}_r[\exists\ s \mathbf{Pr}_q[V(x, r, s, q) = 1] \geq \frac{2}{3}] \leq \frac{1}{3}$*
- *(для $\mathbf{AMA}''$) Если $x \notin B$, то $\mathbf{Pr}_r[\forall\ s \mathbf{Pr}_q[V(x, r, s, q) = 1] \leq \frac{1}{3}] \geq \frac{2}{3}$*

(а) (1 балл) Поясните, в чём отличие трёх определений. А именно, почему один и тот же V может удовлетворить одному и не удовлетворить другому.
(б) (4 балла) Докажите, что $\mathbf{PP} \subset \mathbf{AMA}'$.
(в) (5 баллов) Докажите, что $\mathbf{AMA}'' = AMA$.

Ответ. 1.

2. Пусть $\mathsf{L} \in \mathbf{PP}$, значит $\exists M$:

   - $x \in L \implies P_q[M(x,q)=1] > \frac{1}{2}$
   - $x \notin L \implies P_q[M(x,q)=1] \leq \frac{1}{2}$

   Положим тогда $V(x,s,r,q) = M(x,q) \quad \forall r,s$. Тогда :

   - $x \in L \implies P_r[\exists s : P_q[V(x,s,r,q) = M(x,q) = 1] > \frac{1}{2}] = 1 \geq \frac{2}{3}$
   - $x \notin L \implies P_r[\exists s : P_q[V(x,s,r,q) = M(x,q) = 1] > \frac{2}{3} > \frac{1}{2}] = 0 \leq \frac{1}{3}$

   Заметим, что если в AMA' заменить $\frac{2}{3}$ на $\frac{1}{2}$, то ничего не изменится, так ка $\frac{1}{2}$ и $\frac{1}{3}$ остались отделимыми. Значит $L \in AMA'$.

3.

Задача. ***6***. *Пусть G является генератором псевдослучайных чисел. Рассмотрим следующие модификации:*

- $G'(s) = \begin{cases} 0^{|G(s)|}, & \textit{если } s \textit{ содержит ровно } \frac{|s|}{2} \textit{ единиц} \\ G(s), & \textit{иначе} \end{cases}$
- $G'(s) = \begin{cases} 0^{|G(s)|}, & \textit{если } s \textit{ содержит ровно } \frac{|s|}{3} \textit{ единиц} \\ G(s), & \textit{иначе} \end{cases}$

Какие из этих функций являются генераторами псведослучайных чисел и почему?

Ответ. Считаем $n = |s|$. В обоих случая полиномиальная вычислимость $G'(s)$ очевидна. Нужно проверить пункт (2) определения.

1.
$$G'(s) = \begin{cases} 0^{|G(s)|}, & \text{если s содержит ровно } \frac{|s|}{2} \text{ единиц} \\ G(s), & \text{иначе} \end{cases} \tag{1}$$

   $G'(s)$ - не является ГПСЧ.
   В s ровно $\frac{|s|}{2}$ единиц в $C_n^{\frac{n}{2}}$ различных s. Считая, что $s \sim U_n$ и воспользовавшись тем, что для достаточно больших n выполнено $C_n^{\frac{n}{2}} > \frac{2^n}{n+1}$, получим:

$$P(G(s) = 0^{p(n)}) \geq \frac{C_n^{\frac{n}{2}}}{2^n} \geq \frac{1}{n+1} \quad n \geq N_0 \tag{2}$$

   Воспользуемся определением вычислительной неотличимости, $y_n \sim U_{p(n)}$, пусть $\{D_n\}$ - такое симейство схем, что $D_n(x) = 1 \iff x = 0^n$. Получим :
   $|P\{D_n(G'(s)) = 1\} - P\{D_n(y_n)) = 1\}| \geq \frac{1}{n+1} - \frac{1}{2^n} \geq \frac{1}{2(n+1)}$. при $n \geq 10$. Также $\frac{1}{2(n+1)} \geq \frac{1}{2(p(n)+1)}$ при $n > N_p$. То есть мы получили, что $\exists\{D_n\}$, $\exists q(p(n)) = \frac{1}{2(p(n)+1)}$ $\forall N \exists n > N : |P\{D_n(G'(s)) = 1\} - P\{D_n(y_n)) = 1\}| \geq \frac{1}{q(p(n))}$. Значит y_n и $G'(s)$ - не являются вычислительно неотличимыми. Значит $G'(s)$ - не является ГПСЧ.

2. $G'(s) = \begin{cases} 0^{|G(s)|}, & \text{если s содержит ровно } \frac{|s|}{3} \text{ единиц} \\ G(s), & \text{иначе} \end{cases}$ $G'(s)$ - не является ГПСЧ.
   В s ровно $\frac{|s|}{3}$ единиц в $C_n^{\frac{n}{3}}$ различных s. Воспользуемся формулой Стирлинга:

$$C_n^{\frac{n}{3}} = \frac{n!}{\frac{n}{3}!\frac{2n}{3}!} \sim \frac{3}{\sqrt{4\pi n}} \frac{3^n}{2^{\frac{2n}{3}}} \tag{3}$$

   Обозначим событие $X = \{$ в s ровно $\frac{|s|}{3}$ единиц$\}$. Тогда, считая $s \sim U_n$, получим :

$$P\{G'(s) \neq G(s)\} \leq P\{X\} \sim \frac{3}{\sqrt{4\pi n}} \frac{3^n}{2^{\frac{5n}{3}}} \tag{4}$$

$\frac{3^n}{2^{\frac{5n}{3}}} = e^{n(\ln 3 - \frac{5}{3}\ln 2)}$. Заметим, что $\ln 3 - \frac{5}{3}\ln 2 = c < 0$. Т.е. $P\{G'(s) \neq G(s)\} \sim \frac{3}{2\sqrt{\pi n}} e^{cn}$. Значит $\exists N \forall n > N : P\{G'(s) \neq G(s)\} \leq \frac{3}{\sqrt{\pi n}} e^{c_0 n} \leq e^{cn}, \quad c_0, c < 0.$

Так как $G(s)$ - ГПСЧ, то $y_n \sim U_{p(n)}, \forall\{D_n\}\forall q_1(x)$ - полином $\exists N \forall n > N$: $|P\{D_n(G(s)) = 1\} - P\{D_n(y_n) = 1\}| < \frac{1}{q_1(p(n))}$.

Воспользуемся определением вычислительной неотличимости :
$y_n \sim U_{p(n)}, \forall\{D_n\}\forall q(x)$ - полином $\exists q_1(x) = \frac{q(x)}{2}, \exists N \forall n > N : |P\{D_n(G'(s)) = 1\} - P\{D_n(y_n) = 1\}| \leq |P\{D_n(G'(s)) = 1\} - P\{D_n(G(s)) = 1\}| + |P\{D_n(G(s)) = 1\} - P\{D_n(y_n) = 1\}| < e^{cn} + \frac{1}{q_1(p(n))} < \frac{1}{q(p(n))}$

Получили, что $G'(s)$ и y_n вычислительно неотличимы. Значит $G'(s)$ - ГПСЧ.

Задача. 7. *Обобщённым судоку называется такая задача: в квадрате $n^2 \times n^2$ в некоторых клетках расставлены числа от 1 до n^2. Вопрос: можно ли заполнить оставшиеся клетки числами от 1 до n^2, так чтобы в каждой строке, в каждом столбце, а также в каждом из n^2 "выровненных" квадратов $n \times n$ каждое число встречалось по одному разу. В стандартном судоку $n = 3$. Известно, что эта задача* **NP***-полна. Предложите протокол доказательства существования решения с вычислительно нулевым разглашением, не использующий сводимость к какой-либо другой задаче.*

Ответ. Будем использовать "Протокол привязки к биту", описанный на лекции, для выполнения операций "Загораживание" и "Открытие".

- S - "загораживание", $S(b) = (c, k)$
- R - "открытие", $R(c, k) = \{b, \mathsf{ERROR}\}$
- Требования :
  1. Корректность : $R(S(b)) = b$
  2. Секретность : привязка к 0 и 1 вычислительно неотличимы.
  3. Неподменяемость : невозможность $R(c, k_0) = 0$ и $R(c, k_1) = 1$

Протокол:

Исходная таблица T_0.

- P выбирает случайную перестановку $\sigma \in S_{n^2}$, записывает решение в таблицу T_1, применяет σ к числам $\{1, \dots n^2\}$ из таблицы T_1. "Закрывает" таблицу T_1 и перестановку σ и отправляет верификатору.
- V выбирает случайным образом строку, столбец или квадрат, и просит прувера "открыть" выбранный элемент в T_1. Также V выбирает случайную позицию (i, j) в исходной таблице такую, что $T_0[i, j] = x$ (т.е. в $T_0[i, j]$ уже записано некоторое известное число x , и просит прувера "открыть" $\sigma(x)$. Проверяет на корректность строку, столбец или квадрат соответственно, а также проверяет, что $T_1[i, j] = \sigma(x)$.
- Повторяем протокол с начала нужное количество раз(полином).
- Принимает доказательство, если все проверки пройдены на каждом шаге.

Корректность:

- Если решение существует, то P будет дйствовать оптиматьно, ошибка второго рода может возникнуть только в протоколе привязки к биту, но ее можно сделать очень маленькой. Во всех остальных частях протокола ошибки не возникнет.
- Если решения нет, то либо есть некорректный элемент(строка,столбец, квадрат), либо прувер применил замену индексов не соответствующим перестановке σ образом. В первом случае вероятность не заметить ошибку $P_1 \leq \frac{3n^2-1}{3n^2} = 1 - \frac{1}{3n^2}$, во втором, $P_2 \leq \frac{n^2-1}{n^2} = 1 - \frac{1}{n^2}$. В любом случае $P \leq 1 - \frac{1}{3n^2}$. $P^{3n^2} \leq (1 - \frac{1}{3n^2})^{3n^2} \sim \frac{1}{e}, n \to \inf$. Значит повторив полиномиальное количество раз сможем получить достаточно малую ошибку.

Задача. *9.* *Расширим определение* **PCP**, *введённое на лекции. Назовём классом* $\mathbf{PCP}_{c,s}(r,q)_\Sigma$ *класс языков* L, *для которых существует полиномиальный вероятностный верификатор* V *с произвольным доступом к строке* $\pi \in \Sigma^*$ *длины не более* $q2^{O(R)}$, *со следующими условиями:*

- V *использует не больше* r *случайных битов и делает не больше* q *неадаптивных запросов к* π *(обратите внимание, что здесь мы отказываемся от* $O(\dot{})$*-обозначений);*
- *Если* $x \in L$, *то* $\mathbf{Pr}\{V^\pi(x) = 1\} \geq c$;
- *Если* $x \notin L$, *то* $\mathbf{Pr}\{V^\pi(x) = 1\} \leq s$.

Соответственно, класс, введённый на лекции, является классом $\mathbf{PCP}_{1,\frac{1}{2}}(r,q)_{\{0,1\}}$ *Будем считать, что размер алфавита* $|\Sigma|$ *может зависеть от длины входа* $|x|$. *Докажите, что:*
(а) (1 балл) Для алфавитов Σ *полиномиального размера выполнено* $\mathbf{PCP}_{c,s}(O(\log n), 0)_\Sigma \subset \mathbf{P}$
(б) (4 балла) Для алфавитов Σ *полиномиального размера выполнено* $\mathbf{PCP}_{c,s}(O(\log n), 1)_\Sigma \subset \mathbf{P}$ *(для любых параметров* $c > s$*)*
(в) (5 баллов) Для алфавитов Σ *и параметров* q, *таких что* $|\Sigma|^q$ *не больше полинома, выполнено* $\mathbf{PCP}_{1,\frac{1}{|Sigma|q}}(O(\log n), q)_\Sigma \subset P$

Ответ. 1. $q = 0 \implies$ алгоритм проверки детерменированный, к сертификату не обращается, работает полином. Это есть **P**