Зачетные задачи

Зотов Алексей 497

May 24, 2017

Задача. ***1***. *Построить систему интерактивных доказательств для языка $\mathsf{GI\text{-}NO\text{-}EQUAL\text{-}CLASSES}$ $= \{(G_1, \dots G_m) \mid$ 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, что $G_i \ncong G_j$, причем вероятность ошибки $p_{ij} \leq \frac{1}{3m^2}$.
5. Повторяется с пункта (1), пропуская те индексы, для которых уже найден класс изоморфности.
6. V проверяет, что все классы получились разного размера.

Докажем, что алгоритм корректен:

- если $(G_1, \dots G_m) \in \mathsf{GI\text{-}NO\text{-}EQUAL\text{-}CLASSES}$, тогда каждый на каждой итерации прувер будет действовать наилучшим образом, положительная проверка на изоморфность и неизоморфность проходит без ошибок (с вероятностью 1).
- если $(G_1, \dots G_m) \notin \mathsf{GI\text{-}NO\text{-}EQUAL\text{-}CLASSES}$, тогда P не может неизоморфные графы отнести в один класс, но может попробовать изоморфные графы разбить по разным классам, воспользовавшись наличием ошибки при проверке $G_i \ncong G_j$. Таких проверок не больше m^2, значит $P_{err} \leq \sum p_{ij} \leq m^2 \cdot \frac{1}{3m^2} = \frac{1}{3}$.

Задача. ***5***. *Постройте систему интерактивных доказательств с общими случайными битами для языка $\mathsf{GROUP\text{-}NI} = \{G_0, G_1 \mid G_0,\ G_1$ — 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 $S = \{(H, \sigma) | H \cong G_i, i \in \{0, 1\}, \sigma \in \mathrm{Aut} H\}$. Тогда, если $G_0 \cong G_1$, то $|S| = n!$, иначе $|S| = 2 \cdot n!$. Воспользуемся семейством попарно независимых полиномиально вычислимых хеш-функций $H_{n,k} : 2^{\mathbf{N}} \to 2^{\mathbf{K}}$. А дальше как на лекции! TODO...

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

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

Какие из этих функций являются генераторами псведослучайных чисел и почему?

Ответ. Считаем $n = |s|$.

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

   $G'(s)$ - 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:

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

   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:

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

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

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

   $\frac{3^n}{2^{\frac{5n}{3}}} = e^{n(\ln 3 - \frac{5}{3}\ln 2)}$. 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.*

Черновик ответа. Идея: 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 и перестановку σ. V использует сколько нужжно случайных бит, выбирает строку, столбец или квадрат, и просит прувера открыть в T_1. Также выбирает случайную позицию (i, j) в исходной таблице такую, что $T_0[i, j] = x$ (т.е. в $T_0[i, j]$ записано некоторое известное число x) , и просит открыть $\sigma(x)$. Проверяет на корректность строку, столбец или квадрат соответственно, а также проверяет, что $T_1[i, j] = \sigma(x)$. Случайные биты, открытие-закрытие как на лекции. Вероятность найти ошибку за 1 шаг $p \geq \frac{1}{7} n^1 0$.