# Зачетные задачи

Зотов Алексей 497

May 21, 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, 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 $(G_1, \dots G_m) \in$ GI-NO-EQUAL-CLASSES, тогда каждый на каждой итерации прувер будет действовать наилучшим образом, положительная проверка на изоморфность и неизоморфность проходит без ошибок (с вероятностью 1).
- если $(G_1, \dots G_m) \notin$ GI-NO-EQUAL-CLASSES, тогда $P$ не может неизоморфные графы отнести в один класс, но может попробовать изоморфные графы разбить по разным классам, воспользовавшись наличем ошибки при проверке $G_i \ncong G_j$. Таких проверок не больше $m^2$, значит $P_{err} \leq \sum p_{ij} \leq m^2 \cdot \frac{1}{3m^2} = \frac{1}{3}$.