XIII Летняя онлайн-школа «Комбинаторика и алгоритмы»
Даниил Мусатов, «Модели делегирования вычислений»
Список упражнений №2: интерактивные доказательства

1. Пусть есть генератор битов, распределённых равномерно и независимо друг от друга. Как сгенерировать число, равномерно распределённое от 0 до m? А как сгенерировать число, равномерно распределённое среди тех чисел, которые взаимно просты с m? А перестановку чисел от 1 до n, равномерно распределённую среди всех таких перестановок?

2. Пусть $G_0 = (V_0, E_0)$ и $G_1 = (V_1, E_1)$ — два графа, т.ч. $|V_0| = |V_1| = n$. Можно считать, что $V_0 = V_1 = \{1, \dots, n\}$. Тогда $\varphi\colon \{1, \dots, n\} \to \{1, \dots, n\}$ называется *изоморфизмом* G_0 и G_1, если для всех u и v выполнено $(u, v) \in E_0$ тогда и только тогда, когда $(\varphi(u), \varphi(v)) \in E_1$. Если существует изоморфизм, то графы G_0 и G_1 называются *изоморфными*, обозначение $G_0 \simeq G_1$. Изоморфизм графа в себя называется *автоморфизмом*.

а) Докажите, что изоморфность графа — отношение эквивалентности, т.е. $G \simeq G$, из $G \simeq H$ следует $H \simeq G$, из $G \simeq H$ и $H \simeq K$ следует $G \simeq K$.

б) Докажите, что автоморфизмы графа образуют группу, т.е. композиция автоморфизмов есть автоморфизм, существует единичный автоморфизм и у любого автоморфизма есть обратный. Такая группа для графа G обозначается через $\operatorname{Aut} G$.

в) Докажите, что если $G \simeq H$, то $|\operatorname{Aut} G| = |\operatorname{Aut} H|$ (группы автоморфизмов изоморфных графов содержат одинаковое число элементов). Чему равняется произведение $|\operatorname{Aut} G|$ на размер класса изоморфизма G?

3. Пусть имеется чёрный ящик, который по двум графам честно говорит, изоморфны ли они. Предложите алгоритм поиска изоморфизма, если он существует.

4. Рассматривается следующий интерактивный протокол:

1. На вход стороны получают графы G_0 и G_1 на n вершинах. Прувер должен доказать, что графы неизоморфны.
2. Верификатор выбирает случайный бит $b \in \{0, 1\}$ и случайную перестановку $\psi \in S_n$. Верификатор отправляет пруверу $H = \psi(G_b)$.
3. Прувер присылает в ответ бит $c \in \{0, 1\}$.
4. Верификатор одобряет ответ, если $c = b$, и отвергает в противном случае.

Докажите, что если графы действительно неизоморфны, то прувер будет успешен с вероятностью 1, а если изоморфны — то с вероятностью $\frac{1}{2}$.

5. Постройте систему интерактивных доказательств для такой задачи. На вход подаются графы $G_1, \dots, G_m$ и число k. Требуется проверить, что среди них найдётся ровно k попарно неизоморфных друг другу, такие что любой из оставшихся изоморфен одному из выбранных.

6. Пусть заданы числа m и $a \in [1, m-1]$, такое что $\text{НОД}(a, m) = 1$. Тогда a называется *квадратичным вычетом*, если $\exists x\ a \equiv x^2 (\mod m)$, и невычетом, иначе. Докажите, что произведение двух вычетов есть вычет, а произведение вычета и невычета есть невычет. Докажите, что если x есть фиксированный вычет, а y принимает все возможные значения среди вычетов, то xy тоже принимает все возможные значения среди вычетов.

7. Рассматривается следующий интерактивный протокол:

1. На вход стороны получают число m и $a \in [1, m-1]$, такой что $\text{НОД}(a, m) = 1$. Прувер должен доказать, что a — квадратичный невычет.

2. Верификатор выбирает случайный бит $b \in \{0, 1\}$ и случайное z, такое что НОД$(z, m) = 1$. Верификатор отправляет пруверу $y = a^b \cdot z^2 (\mod m)$.

3. Прувер присылает в ответ бит $c \in \{0, 1\}$.

4. Верификатор одобряет ответ, если $c = b$, и отвергает в противном случае.

Докажите, что если a действительно квадратичный невычет, то прувер будет успешен с вероятностью 1, а если вычет — то с вероятностью $\frac{1}{2}$.