Нулевое разглашение для языков из NP

Ю. Лифшиц[*]

7 ноября 2005 г.

План лекции

1. Нулевое разглашение для NISO
2. Нулевое раазглашение для языков из NP
3. Нулевое разглашение для задачи 3-раскрашиваемости
4. Формулировка теоремы

1 Нулевое разглашение для NISO

На предыдущей лекции был приведен протокол интерактивного доказательства неизоморфности графов G_1 и G_2

1. V выбирает случайное $b \in [1, 2]$ и случайную перестановку π
2. V посылает P $\pi(G_b)$
3. P угадывает b и посылает V
4. шаги 1-3 повторяются достаточно большое число раз

Свойства полноты и корректности для данного протокола очевидны. Но он не обладает свойством нулевого разглашения, так как для любого графа G_0 V может определить, какому из графов G_1 , G_2 он не изоморфен. Тем не менее существует протокол доказательства NISO с нулевым разглашением.

2 Нулевое разглашение для языков из NP

2.1 Напоминания

1. Язык L принадлежит классу языков NP, если $\exists$ полиномиальный P, такой что $(x \in L) \Leftrightarrow \exists y (P(x, y) = 1)$.

[*] Законспектировал В. Столбов .

2. Язык L является NP-полным, если $\forall L_1 \in NP \exists poly f x \in L_1 \Leftrightarrow f(x) \in L$

3. Язык 3-раскрашиваемых графов является NP-полным.

Уточнение 1 - f из свойства 2 является инъекцией.

2.2 Доказательства с нулевым разглашением для языков из NP

Допустим, что мы знаем протокол, доказывающий с нулевым разглашением задачу 3-раскрашиваемости. Пусть L - некий язык из NP (например, язык составных чисел), а f - отображение, сопоставляющее каждому натуральному числу некий граф, являющийся 3-раскрашиваемым тогда и только тогда, когда это число составное.

Тогда рассмотрим протокол:

1. V и P вычисляют $G(x)$

2. P (в нашей модели он вычислительно неограничен) находит 3- раскраску G

3. Осуществляется протокол интерактивного доказательства 3-раскрашиваемости графа G

Полнота и корректность данного протокола очевидны. Доказательство свойства нулевого разглашения тоже очевидно - $VIEW[V, P]$ и $VIEW[V_1, P_1]$ совпадают (V_1 и P_1 - участники протокола доказательства 3-раскрашиваемости графа.) Таким образом, из нулевого разглашения для протокола 3-раскрашиваемости по определению следует нулевое разглашение для предыдущего протокола.

3 Нулевое разглашение для задачи 3- раскрашиваемости

3.1 Уточнение определения

Знак изоморфизма в определении

$\forall V_1 \exists S_{PPT} \forall x \in L VIEW[V_1, P] \cong S(x)$

означает, что распределения ответов у вероятностных алгоритмов совпадают.

3.2 Нулевое разглашение в слабом смысле

S_{PPT} и R_{PPT} называются вычислительно неразличимыми, если не существует полиномиального P, способного по результату работы одного из этих алгоритмов определить, какой именно алгоритм был запущен.

Протокол интерактивного доказательства называется протоколом с ненулевым разглашением в слабом смысле, если условие совпадения распределений заменено на условие вычислительной неразличимости.

3.3 Протокол доказательства 3-раскрашиваемости

1. P случайным образом переставляет цвета.
2. P шифрует цвета, используя привязку к биту и посылает зашифрованную раскраску V
3. V выбирает 2 вершины, соединенные ребром, и посылает P их номера.
4. P расшифровывает цвета указанных вершин.
5. V проверяет, что цвета вершин не совпадают.
6. Шаги 1-5 повторяются много раз (рекомендуется порядка числа ребер).

Полнота и корректность достаточно очевидны. Осталось доказать, что данный протокол обладает свойством нулевого разглашения в слабом смысле.

3.4 Построение S_{PPT}

1. S выбирает 2 соединенные ребром вершины V_1 , V_2, красит их в различные цвета, а все остальные - в красный.
2. S шифрует цвета, используя привязку к биту и посылает зашифрованную раскраску V
3. V выбирает 2 вершины, соединенные ребром, и посылает S их номера.
4. Если V выбрал V_1 и V_2, S расшифровывает цвета, иначе стирает V память.

3.5 Доказательство свойства ненулевого разглашения в слабом смысле.

Доказательство будет проводиться методом black-box reduction. Точнее, докажем, что если кто-то сумеет за полиномиальное время отличить симулятор от настоящего диалога, то шифрование является нестойким.

Предположим противное. Пусть $\exists V$, который умеет отличать сообщения от S и сообщения от P.

Тогда рассмотрим набор алгоритмов I_i, где i изменяется от 0 до n- 2. I_i выбирает i+2 вершины, раскрашивает их правильной 3- раскраской, а все остальные красит в красный, шифрует цвета, используя привязку к биту и посылает все это V. Заметим что сообщения от I_0 совпадают с сообщениями от S, а сообщения от I_{n-2} совпадают с сообщениями от P. Значит, найдется k, такой что V различит сообщения от I_k и от I_{k+1}. но эти сообщения отличаются шифром цвета одной вершины. Таким образом, с вероятностью n^{-1} шифрограмму можно сломать. Таким образом, шифрование нестойкое.

4 Формулировка теоремы

1. $\forall L \in NP \exists$ протокол интерактивного доказательства теорем вида $x \in L$ с нулевым разглашением.
2. Стойкость протокола основана на стойкости шифрования.

5 Использованные материалы

1. Бумажный конспект лекции.
2. WinEdit 5.3