Д.В.Мусатов

Задачи к курсу «Интерактивные системы доказательств»

Задача 1. Покажите, что только интерактивность, без использования случайности, не расширяет класс верифицируемых доказательств. А именно, рассмотрим такой тип интерактивных систем: сначала прувер и верификатор узнают некоторое утверждение x. Прувер присылает некоторый текст y_1, затем верификатор, зная x и y_1, вычисляет (за полиномиальное время) запрос z_1, на который прувер отвечает сообщением y_2, затем верификатор вычисляет новый запрос z_2, получает y_3, и так далее. После какого-то (полиномиального) числа раундов верификатор отвечает «да» или «нет». Требуется, чтобы для истинного утверждения x у прувера была такая стратегия, что верификатор ответит «да», а для ложного утверждения x любая стратегия прувера приведёт к ответу «нет». Докажите, что в таком случае есть и система с одним раундом: прувер присылает y, а верификатор сразу даёт ответ.

Задача 2. Напоминание: остаток x, взаимно простой с модулем m, называется квадратичным вычетом по модулю m, если $x \equiv a^2 \mod m$ для некоторого a, и квадратичным невычетом в противном случае.

а) Докажите, что произведение двух вычетов есть вычет, а произведение вычета и невычета есть невычет.

б) Докажите, что если x есть фиксированный вычет, а y принимает все возможные значения среди вычетов, то xy тоже принимает все возможные значения среди вычетов.

в) Постройте систему интерактивных доказательств для утверждения вида «a — квадратичный невычет». (Указание: можно использовать ту же общую идею, что в примерах с Зевсом и Афиной и с неизоморфизмом графов).

Задача 3. А теперь придумайте систему интерактивных доказательств с совершенно нулевым разглашением для утверждений вида «x — квадратичный вычет». (Указание: можно использовать ту же идею, что в примерах с Али-Бабой и с изоморфизмом графов).

Задача 4. Обобщённым судоку называется такая задача: в некоторых клетках квадрата $n^2 \times n^2$ записаны числа от 1 до n^2. Требуется установить, можно ли заполнить все оставшиеся клетки, так чтобы в каждом столбце, каждой строке и каждом «выровненном» квадрате $n \times n$ все числа от 1 до n^2 встречались по одному разу. (В обычном судоку $n = 3$). Придумайте систему интерактивных доказательств с вычислительно нулевым разглашением для этой задачи. Решение можно излагать в терминах «запертых сундучков»/«шторок»/«запечатанных конвертов».

Задача 5. И снова о квадратичных вычетах. На этот раз придумайте, как построить вероятностно проверяемое доказательство того, что x есть невычет. Верификатор должен делать константное число запросов к тексту доказательства. (Указание: и вновь подойдёт та же идея, что в задаче о неизоморфизме графов).

Задача 6. Покажите, как переделать PCP-верификатор, совершающий q адаптиных запросов к доказательству, в PCP-верификатор, совершающий 2^q неадаптивных запросов.