Задачи для слушателей вводного курса по теоретической информатике

Computer Science Club, ПОМИ РАН

8 декабря 2018

1. «Лемма Шварца – Зиппеля». (Она нужна для анализа вероятностностного алгоритма проверки равенства многочленов, который много где используется)

Пусть $P(x_1, \ldots, x_n)$ многочлен с коэффициентами в некотором конечном поле F степени (суммарной по всем переменным) d, причём не все коэффициенты нулевые. Тогда доля всех точек $(x_1, \ldots, x_n)$, где многочлен обращается в нуль, среди всего F^n, не превосходит d/n.

2. Мы видели, что коммуникационная сложность проверки равенства двух слов длины n равна $\Theta(n)$ для детерминированных алгоритмов и не больше $O(\log n)$ для вероятностных (на самом деле эта оценка точная, но этого мы пока не знаем). Покажите, что если считать слова двоичными записями чисел, то коммуникационная сложность вычисление предиката $x \le y$ есть $\Theta(n)$ в детерминированном случае и $O(\log^2 n)$ в вероятностном. (Это можно улучшить до $O(\log n)$, но сильно сложнее.)

3. Предположим, что в задаче о коммуникационной сложности Алиса и Боб имеют доступ к общим случайным битам (кто-то бросает монету и сообщает им результаты бесплатно). Как это использовать для уменьшения коммуникационной сложности проверки равенства?

4. Покажите, что для любых трёх слов длины не больше n выполняется неравенство для колмогоровских сложностей

$$2K(x, y, z) \le K(x, y) + K(x, z) + K(y, z) + O(\log n);$$

Это можно сделать, несколько раз используя формулу для сложности пары

$$K(u, v) = K(u) + K(v|u) + O(\log n)$$

5. Комбинаторная версия этого утверждения: если в трёхмерном пространстве есть конечное множество из V точек, и его проекции на три координатные плоскости содержат S_{xy}, S_{yz} и S_{xz} точек, то

$$V^2 \le S_{xy} S_{xz} S_{yz}$$

Попробуйте доказать это утверждение непосредственно или вывести его из неравенства для колмогоровской сложности (предыдущая задача). Попробуйте вывести неравенство предыдущей задачи из комбинаторного утверждения.

6. Докажите, что колмогоровская сложность числа n стремится к бесконечности, когда $n \to \infty$. Пусть $B(n)$ — максимальное число, колмогоровская сложность которого не больше n. Покажите, что $B(n)$ не имеет вычислимой верхней оценки.

7. Запишем принцип Дирихле для трёх голубей и двух клеток. Введём переменные $f_{11}, f_{12}, f_{21}, f_{22}, f_{31}, f_{32}$, при этом f_{ij} означает, что голубь i летит в клетку j. Как записать в виде конъюнктивной нормальной формы запрещения в принципе Дирихле (каждый голубь куда-то летит, должен лететь только в одну клетку и в каждой клетке не должно быть двух голубей)? Эти условия противоречивы — можете вывести пустую клаузу по правилу резолюций?

8. Есть некоторое обобщение обсуждавшейся двойственности, касающееся не вывода противоречия, а следования. Соответствующее утверждение из линейной алгебры: известно, что любого решение системы уравнений

$$\begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = 0 \\ \dots \\ a_{m1}x_1 + \dots + a_{mn}x_n = 0 \end{cases}$$

является решением уравнения $b_1x_1 + \dots + b_nx_n = 0$. Покажите, что это уравнение можно получить сложением уравнений системы с некоторыми коэффициентами.

Как могло бы выглядеть аналогичное утверждение для линейных неравенств и для исчисления резолюций? Может быть, что-то из этого удастся и доказать.

9. Пусть p — простое число. Остаток $x \neq 0$ по модулю p называется квадратичным вычетом, если квадрат какого-то целого числа даёт остаток x при делении на p. Сколько всего есть квадратичных вычетов? Покажите, что произведение квадратичных вычета и невычета — невычет. Покажите, что произведение двух невычетов — вычет. Предложите способ интерактивного доказательства того, что данный остаток x является невычетом, и того, что x является вычетом. (Знатоки теории чисел знают, что для простого p в этом нет надобности, есть алгоритм, которые проверяет, вычет это или нет — но аналогичные доказательства имеют смысл для непростых модулей.)

10. Что можно сказать о схемной сложности предиката $x > y$, где x и y — n-битовые числа? (Входом являются $2n$ битов, по n для каждого числа, выход — один бит.)

`sasha.shen@gmail.com`, `skype:alexander-shen`

(Не предполагается, что для получения зачёта надо решить все или большинство задач, так что напишите, кто что решил, и мы обсудим)