Упражнения к лекции по *коммуникационной сложности*.

Андрей Ромащенко, andrei.romashchenko@gmail.com

25 апреля 2013 года. Школа 444.

1. На лекции мы доказали, что для вычисления предиката равенства

$$\mathrm{EQ}(a,b) = \begin{cases} 1, & \text{если } a = b, \\ 0, & \text{если } a \neq b \end{cases}$$

существуют (а) детерминированный коммуникационный протокол с коммуникационной сложностью $n+1$ и (б) вероятностный коммуникационный протокол с коммуникационной сложностью не более $2\lceil \log \frac{2n}{\varepsilon} \rceil + 1$.

Пусть $\varepsilon = 1/10000$ (допустимая вероятность ошибки равна одной сотой доле процента). Начиная с какого n коммуникационная сложность вероятностного протокола для данной задачи становится меньше сложности детерминированного протокола? Начиная с какого n коммуникационная сложность вероятностного протокола становится меньше сложности детерминированного протокола в 100 раз? В 10^6 раз?

2. У Алисы имеется целое число a из интервала $1, \ldots, 2^n$ а у Боба целое число b из того же интервала. Алиса и Боб хотят узнать, какое из двух чисел больше; говоря формально, они хотят вычислить значение функции

$$\mathrm{GT}(a,b) = \begin{cases} 1, & \text{если } a \geq b, \\ 0, & \text{если } a < b. \end{cases}$$

Докажите, что детерминированная коммуникационная сложность этой задачи равна $n+1$ (постройте детерминированный протокол с коммуникационной сложностью $n+1$ и покажите, что протоколов с меньшей коммуникационной сложностью для задачи GT не существует).

3. У Алисы имеется некоторое подмножество $A \subset \{1, \ldots, n\}$, а у Боба подмножество $B \subset \{1, \ldots, n\}$. Алиса и Боб хотят узнать, пересекаются ли эти два множества; говоря формально, они хотят вычислить значение функции

$$\mathrm{DISJ}(A,B) = \begin{cases} 1, & \text{если } A \cap B = \emptyset, \\ 0, & \text{иначе.} \end{cases}$$

Докажите, что детерминированная коммуникационная сложность этой задачи равна $n+1$

Указание: Рассмотрите такие пары множеств (A, B), где $B = \{1, \ldots, n\} \setminus A$. Докажите, что каждому листу в дереве коммуникационного протокола может соответствовать не более одной такой пары.

4. У Алисы имеется некоторое подмножество $A \subset \{1, \ldots, 2^n\}$, а у Боба подмножество $B \subset \{1, \ldots, n\}$. Алиса и Боб хотят узнать максимальный элемент в объединении этих множеств $A \cup B$.

(а) Постройте для этой задачи детерминированный коммуникационный протокол с коммуникационной сложностью не более $2n$.

(б) Постройте для этой задачи детерминированный коммуникационный протокол с коммуникационной сложностью не более $\frac{3}{2}n + c$ для некоторого c, которое не зависит от n.

(в)* Постройте для этой задачи детерминированный коммуникационный протокол с ещё меньшей коммуникационной сложностью. Какой сложности вам удалось достичь?

5. Для функции GT из задачи 2 постройте вероятностный коммуникационный протокол с коммуникационной сложностью $O(\log^2 n)$, который для каждой пары входов (a, b) приводит к правильному ответу с вероятностью не менее 0,99.

6. Рассмотрим вероятностные коммуникационные протоколы, в которых Алиса и Боб имеют доступ к *общему* источнику случайных битов.

"Игрушечное" описание данной модели: Представим себе, что Останкинская башня каждую секунду посылает в эфир один случайный бит (каждый раз ноль или единица выбираются с равными вероятностями и независимо от предыдущих сигналов). Живущие в Москве Алиса и Боб слушают эту радиопередачу и таким образом получают доступ к общей случайной последовательности нулей и единиц.

Постройте в данной модели коммуникационный протокол для вычисления функции $\mathrm{EQ}(a, b)$ из задачи 1 с коммуникационной сложностью не больше 8 и вероятностью ошибки для каждой пары (a, b) не больше $1/100$.

Замечание: Это не опечатка! Коммуникационная сложность в этой задаче действительно не зависит от n.

7. (а) В коммуникационной модели с общим источником случайности постройте для функции GT из задачи 2 протокол с коммуникационной сложностью $O(\log n \cdot \log\log n)$, который для каждой пары входов (a, b) приводит к правильному ответу с вероятностью не менее 0,99.

(б)* Улучшите оценку коммуникационной сложности в этой задаче до $O(\log n)$.

8. Доказательство постулата Бертрана в задачах.

(а) Докажите, что $\frac{4^n}{2n+1} \le C_{2n}^n \le 4^n$.

Указание: Раскройте скобки в выражении $(1+1)^{2n}$*; покажите, что* C_{2n}^n *является максимальным среди всех биномиальных коэффициентов* C_{2n}^m.

(б) Докажите, что $C_{2n}^n = \frac{(n+1)\cdot(n+2)\cdot\ldots\cdot(2n)}{1\cdot 2\cdot\ldots\cdot n}$.

(в) Докажите, что все простые числа p из интервала от $n+1$ до $2n$ (если таковые существуют) делят число C_{2n}^n.

(г) Докажите, что произведение всех простых чисел из интервала от 1 до k не превосходит 4^k. *Указание: воспользуйтесь пунктом (в), а затем примените верхнюю оценку из пункта (а) для* $n = \frac{k}{2}, \frac{k}{4}, \frac{k}{8}, \ldots$

(д) Докажите, что все простые числа p из интервала от $2n/3$ до n (если таковые существуют) делят числитель и знаменатель $\frac{(n+1)\cdot(n+2)\cdot\ldots\cdot(2n)}{1\cdot 2\cdot\ldots\cdot n}$ ровно по одному разу (это значит, что такие простые числа *не* делят C_{2n}^n).

(е) Докажите, что простые числа p из интервала от $\sqrt{2n}$ до $2n/3$ (если таковые существуют) входят в произведение $\frac{(n+1)\cdot(n+2)\cdot\ldots\cdot(2n)}{1\cdot 2\cdot\ldots\cdot n}$ в степени не выше 1. *Указание: сосчитайте, сколько чисел кратных* p *встречается в числителе и в знаменателе данной дроби; сравните эти два числа между собой. Покажите, что чисел кратных* p^2 *в чис-*

лителе и знаменателе этой дроби нет.

(ж) Докажите, что каждое простое число p из интервала от 1 до $\sqrt{2n}$ входит в $C_{2n}^n = \frac{(n+1)\cdot(n+2)\cdot\ldots\cdot(2n)}{1\cdot 2\cdot\ldots\cdot n}$ в степени не выше $\log_p(2n)$. *Указание: сосчитайте, сколько в числителе и в знаменателе этой дроби встрчается чисел кратных p, затем сколько там встречается чисел кратных p^2, чисел кратных p^3, и т.д. Оцените разницу между кратностями, с которыми p входит в числитель и в знаменатель.*

(з) Предположим, что в интервале от $n+1$ до $2n$ нет простых чисел. Докажите с помощью (е-ж) и (г), что при данном предположении должно быть выполнено неравенство

$$C_{2n}^n \leq 4^{\frac{2}{3}n} \cdot (2n)^{\sqrt{2n}}.$$

Покажите, что это неравенство противоречит пункту (а) при всех достаточно больших n (скажем, при всех $n > 10000$).

(и) Докажите, что для всех целых положительных n найдется такое простое число p, что $n < p \leq 2n$. *Указание: после доказательства пункта (з) остается лишь перебором проверить данное утверждение для $n \leq 10000$.*

Список литературы.

1. Литература по теории коммуникационной сложности.

[1] Александр Александрович Разборов. Коммуникационная сложность. Серия Летняя школа “Современная математика”. МЦНМО, 2012.

[2] Eyal Kushilevitz and Noam Nisan. Communication Complexity. Cambridge University Press. 1998.

[3] Sanjeev Arora and Boaz Barak. Computational Complexity: A Modern Approach. Cambridge University Press. 2009. (Черновой вариант книги легально распространяется в сети, см. `http://www.cs.princeton.edu/theory/complexity/`)

2. Дополнительная литература: теория сложности вычислений.

[4] Michael Sipser. Introduction to the theory of computation. Course Technology, 2005.

[5] Владимир Николаевич Крупский. Введение в сложность вычислений. Москва, Факториал Пресс, 2006

3. Дополнительная литература: построение и анализ алгоритмов.

[6] Т. Кормен, Ч. Лейзерсон, Р. Ривест. Алгоритмы: построение и анализ. 1-е издание, МЦНМО, 2000.

[7] Thomas Cormen, Charles Leiserson, Ronald Rivest, Clifford Stein. Introduction to Algorithms. 3rd edition. MIT Press, 2009.

[8] Александр Шень. Программирование: теоремы и задачи. 2-е издание, М.: МЦНМО, 2004. (Свободно распространяемое издание, см. `http://www.mccme.ru/free-books/`)

4. Элементарное доказательство постулата Бертрана.

[9] В. Уфнаровский. Прогулка до теоремы Чебышёва. Журнал *Квант*, номер 6, 1992.

[10] В. Тихомиров. Теорема Чебышёва о распределении простых чисел. Журнал *Квант*, номер 6, 1994.

[11] А. Коробов. Простые числа и постулат Бертрана. Журнал *Квант*, номер 4, 1998.

[12] М. Айгнер и Г. Циглер. Доказательства из книги. М.: Мир, 2006.