Задачи для экзамена по курсу «Математическая криптография» (весенний семестр 2019/2020 уч. г.)

1. Пусть $\mathcal{D}$ и $\mathcal{E}$ — распределения вероятностей на некотором конечном или счетном множестве X. Доказать, что статистическое расстояние между этими распределениями, определенное как $(1/2)\sum_{x\in X}|\Pr_{\mathcal{D}}\{x\}-\Pr_{\mathcal{E}}\{x\}|$, совпадает с $\max_{S\subseteq X}|\Pr_{\mathcal{D}}S-\Pr_{\mathcal{E}}S|$. Указать множество, на котором этот максимум достигается. (*Указание:* рассмотреть множества $X_+=\{x\in X\mid \Pr_{\mathcal{D}}\{x\}\geqslant\Pr_{\mathcal{E}}\{x\}\}$ и $X_-=X\setminus X_+=\{x\in X\mid \Pr_{\mathcal{D}}\{x\}<\Pr_{\mathcal{E}}\{x\}\}$.)

2. Пусть m и n — целые положительные числа и $r=n \bmod m$ (т. е. r — остаток от деления n на m). Найти явную формулу (в терминах m, n и r) для статистического расстояния между $\mathcal{U}(\{0,\ldots,m-1\})$ и распределением случайной величины $\widetilde{x} \bmod m$, где $\widetilde{x}\leftarrow\mathcal{U}(\{0,\ldots,n-1\})$. Используя эту формулу, получить верхнюю оценку $m/4n$ для этого статистического расстояния.

3. Пусть $\mathcal{D}_i$ и $\mathcal{E}_i$ — распределения вероятностей на конечном или счетном множестве X_i для каждого $i\in\{1,\ldots,n\}$. Доказать, что $\Delta(\mathcal{D}_1\times\ldots\times\mathcal{D}_n,\mathcal{E}_1\times\ldots\times\mathcal{E}_n)\leqslant\sum_{i=1}^n\Delta(\mathcal{D}_i,\mathcal{E}_i)$, где Δ — статистическое расстояние, $\mathcal{D}_1\times\ldots\times\mathcal{D}_n$ — распределение случайной величины $(\widetilde{d}_1,\ldots,\widetilde{d}_n)$ при $\widetilde{d}_i\leftarrow\mathcal{D}_i$ для всех $i\in\{1,\ldots,n\}$ (что подразумевает независимость $\widetilde{d}_1,\ldots,\widetilde{d}_n$), а $\mathcal{E}_1\times\ldots\times\mathcal{E}_n$ определяется аналогично. (*Указание:* использовать гибридный метод.)

4. Пусть N — бесконечное подмножество $\mathbb{N}$. Функция $\xi\colon N\to\mathbb{R}_+=\{r\in\mathbb{R}\mid r\geqslant 0\}$ называется существенной (noticeable, см. [Gol, Volume 1, Subsection 2.2.1]), если существует полином p такой, что неравенство $\xi(n)\geqslant 1/p(n)$ выполняется при всех достаточно больших $n\in N$. Очевидно, что всякая существенная функция не является пренебрежимо малой. Верно ли обратное (для функций из N в $\mathbb{R}_+$)?

5. Пусть $f\colon\{0,1\}^*\to\{0,1\}^*$ — полиномиально вычислимая функция такая, что существует полиномиальный вероятностный алгоритм A, удовлетворяющий условию $\Pr[A(1^n,\widetilde{i},f(\widetilde{x}))=\widetilde{x}_{[\widetilde{i}]}]\geqslant 1-\varepsilon/n$ для всех $n\in N$, где $\widetilde{x}\leftarrow\mathcal{U}(\{0,1\}^n)$, $\widetilde{i}\leftarrow\mathcal{U}(\{1,\ldots,n\})$, $0<\varepsilon<1$ и N — бесконечное подмножество $\mathbb{N}$. Доказать, что функция f не является односторонней. См. также [Lub, Exercise 20].

6. Пусть $f\colon\{0,1\}^*\to\{0,1\}^*$ — односторонняя функция. Доказать, что для любого полинома p неравенство $|f(\{0,1\}^n)|>p(n)$ выполняется для всех достаточно больших $n\in\mathbb{N}$. Другими словами, $|f(\{0,1\}^n)|$ растет быстрее любого полинома. См. также [Gol, Volume 1, Subsection 2.7.4, Exercise 10]. (*Указание:* использовать неравенство $\sum_{i=1}^n x_i^2\geqslant 1/n$, верное для всех $x_1,\ldots,x_n\in\mathbb{R}$ таких, что $\sum_{i=1}^n x_i=1$. Это неравенство легко доказать, рассмотрев неотрицательную сумму $\sum_{i=1}^n(x_i-1/n)^2$.)

7. Пусть $f\colon\{0,1\}^*\to\{0,1\}^*$ — слабо односторонняя перестановка. Для произвольного $n\in\mathbb{N}$ рассмотрим разложение $f|_{\{0,1\}^n}$ в произведение независимых циклов. Обозначим через $\mathrm{lc}_f(x)$ длину цикла, содержащего $x\in\{0,1\}^n$, т. е. $\mathrm{lc}_f(x)=\min\{i\geqslant 1\mid f^i(x)=x\}$, где f^i — i-кратная композиция f с самой собой. Доказать, что для любого полинома p неравенство $\mathsf{E}\,\mathrm{lc}_f(\widetilde{u}_n)>p(n)$ выполняется для всех достаточно больших $n\in\mathbb{N}$, где $\widetilde{x}\leftarrow\mathcal{U}(\{0,1\}^n)$, а E — среднее значение (математическое ожидание). Другими словами, $\mathsf{E}\,\mathrm{lc}_f(\widetilde{u}_n)$ растет быстрее любого полинома. См. также [Gol, Volume 1, Subsection 2.7.4, Exercise 11]. (*Указание:* использовать неравенство Маркова.)

8. Пусть $f\colon\{0,1\}^* \to \{0,1\}^*$ — односторонняя перестановка такая, что $\Pr[A(f(\widetilde{u}_n)) = \widetilde{u}_n] \leqslant 2^{-n} + \mathrm{negl}(n)$ для любого полиномиального вероятностного алгоритма A, где $\widetilde{u}_n \leftarrow \mathcal{U}(\{0,1\}^n)$. Привести пример функции, которая трудно аппроксимируема по f, но не трудна для f.

9. Предположим, что односторонние функции существуют. Построить одностороннюю функцию и трудный для нее предикат b такой, что $\Pr[b(\widetilde{u}_n) = 1] = 1/2$ для всех n, где $\widetilde{u}_n \leftarrow \mathcal{U}(\{0,1\}^n)$. (Функция и предикат могут быть определены на $\bigcup_{n\in N}\{0,1\}^n$ для некоторого полиномиально перечислимого множества $N \subseteq \mathbb{N}$.) См. также [Gol, Volume 1, Subsection 2.7.4, Exercise 26].

10. Привести пример полиномиально вычислимой и сохраняющей длину функции $f\colon\{0,1\}^* \to \{0,1\}^*$, которая не является односторонней, но для которой верно заключение теоремы Гольдрайха—Левина, т. е. предикат $xy \mapsto \bigoplus_{i=1}^{n}(x_{[i]} \odot y_{[i]})$ является трудным для функции $xy \mapsto (f(x), y)$, где $x, y \in \{0,1\}^n$, $n \in \mathbb{N}$. См. также [Lub, Exercise 21].

11. Пусть g — псевдослучайный генератор, отображающий $\{0,1\}^n$ в $\{0,1\}^{m(n)}$ для всех $n \in \mathbb{N}$. Пусть также $(a_n \mid n \in \mathbb{N})$ — такое семейство строк, что $a_n \in \{0,1\}^{m(n)}$ для любого $n \in \mathbb{N}$ и функция $1^n \mapsto a_n$ полиномиально вычислима. Доказать, что $\Pr[g(\widetilde{u}_n) = a_n] = \mathrm{negl}(n)$, где $\widetilde{u}_n \leftarrow \mathcal{U}(\{0,1\}^n)$. См. также [Gol, Volume 1, Subsection 3.8.4, Exercise 12].

12. Пусть для каждого $j \in \{1,\ldots,n\}$ определена система секретной связи $((e_{i_j}^{(j)}\colon M_j \to C_j \mid i_j \in K_j), \mathcal{K}_j)$ в смысле теории Шеннона, совершенная относительно априорного распределения вероятностей $\mathcal{M}_j$. Доказать, что

$$(((e_{i_1}^{(1)},\ldots,e_{i_n}^{(n)}) \mid (i_1,\ldots,i_n) \in K_1 \times \ldots \times K_n), \mathcal{K}_1 \times \ldots \times \mathcal{K}_n),$$

где функция $(e_{i_1}^{(1)},\ldots,e_{i_n}^{(n)})\colon M_1 \times \ldots \times M_n \to C_1 \times \ldots \times C_n$ для каждого $(i_1,\ldots,i_n) \in K_1 \times \ldots \times K_n$ определяется формулой

$$(e_{i_1}^{(1)},\ldots,e_{i_n}^{(n)})(m_1,\ldots,m_n) = (e_{i_1}^{(1)}(m_1),\ldots,e_{i_n}^{(n)}(m_n)),$$

является совершенной системой секретной связи относительно $\mathcal{M}_1 \times \ldots \times \mathcal{M}_n$.

13. С каким известным классом сложностей совпадает класс всех языков, для которых существует протокол интерактивного доказательства (с границей полноты 1 и границей корректности 0) с детерминированными доказывающим и проверяющим?

14. Доказать, что если в определении вычислительно (а также статистически или абсолютно) нулевого разглашения заменить $\mathrm{view}_{V'}^{P}(x)$ на $\langle P, V'\rangle(x)$, то получится эквивалентное определение. (Обозначения см. в конспекте лекций.) Говоря неформально, если можно эффективно симулировать $\mathrm{view}_{V'}^{P}(x)$ для любого полиномиального V' и любого $x \in L$, то можно эффективно симулировать $\langle P, V'\rangle(x)$ для любого полиномиального V' и любого $x \in L$, и наоборот. См. также [Gol, Volume 1, Subsection 4.12.4, Exercise 10].

Литература

[Gol] O. Goldreich. Foundations of cryptography. Volume 1 (Basic tools). Volume 2 (Basic applications). Cambridge University Press, 2001 (v. 1), 2004 (v. 2).

[Lub] M. Luby. Pseudorandomness and cryptographic applications. Princeton University Press, 1996.