Оценки коммуникационной сложности линейных PIR-протоколов

Г. А. Майлыбаева

Протоколы извлечения информации без раскрытия запроса, PIR-протоколы, позволяют пользователю получить один бит из базы данных, копия которой хранится на k несообщающихся серверах таким образом, что администраторы базы данных не узнают номер запрашиваемого бита. Предполагаем, что пользователь может генерировать случайные числа для вычисления запросов к серверам. Для любого натурального l обозначим $[l] = \{0, \ldots, l-1\}$. Тогда если k — это количество серверов, n — количество бит в базе данных x, s — максимальное значение генератора случайных чисел, m — количество бит в запросе пользователя, $p_j, j \in [k]$ — количество бит в ответе j-го сервера, $p = p_0 + \ldots + p_{k-1}$ — суммарное количество бит в ответах серверов, то (k, n, s, m, p)-*PIR-протоколом* называется набор из $k+2$ функций $I = \langle Q, A^0, \ldots, A^{k-1}, R\rangle$, где Q — функция, которую использует пользователь для построения запросов, $A^j, j \in [k]$ — функция, которую использует сервер S_j для построения ответов, R — реконструирующая функция, которую использует пользователь для вычисления значения искомого бита. В этих терминах, коммуникационная сложность протокола определена как число $C(I) = km + p$.

Получена точная по порядку оценка коммуникационной сложности для класса PIR-протоколов при $k = 2$, при ограничениях, наложенных на класс возможных функций ответов и реконструирующих функций.

Пусть для $\forall a = (a_0, \ldots, a_{n-1})$, $b = (b_0, \ldots, b_{n-1}) \in \{0,1\}^n$: $\pi_b(a_0, \ldots, a_{n-1}) = (c_0, \ldots, c_{m-1})$, где $m = \|b\|$ — проекция вектора a на те координаты, где в векторе b стоят единицы. Определим сложность реконструирующей функции R как минимальное число $e(R)$

такое, что существуют такие функции $b^j : [n] \times [s] \to B_{p_j}^{e_j}, j \in [k]$ и функция $f : \{0,1\}^e \to \{0,1\}$, что $e_0 + \ldots + e_{k-1} = e$ и для $\forall i \in [n]$ и $\forall r \in [s]$ функция

$$R(i, r, A^0(Q(0, i, r), x), \ldots, A^{k-1}(Q(k-1, i, r), x)) =$$
$$= f(\pi_{b^0(i,r)}(A^0(Q(0, i, r), x)), \ldots, \pi_{b^{k-1}(i,r)}(A^{k-1}(Q(k-1, i, r), x))).$$

Линейными PIR-протоколами назовем такие протоколы, что для любого $j \in [k]$ любой бит ответа A^j есть линейная функция от базы данных x. Класс всех линейных PIR-протоколов обозначим через $\mathcal{L}$.

Положим $\mathcal{L}_2 = \{I \in \mathcal{L} : e(I) \leqslant 2\}$. Обозначим $\mathcal{I}(k, n, s)$ класс всех (k, n, s, m, p)-PIR-протоколов, где $m \geqslant 0, p > 0$. Пусть $\mathcal{A} \subseteq \mathcal{I}(k, n, s)$. Тогда обозначим $C(k, n, s, \mathcal{A}) = \min\{C(I) : I \in \mathcal{A}\}$.

Теорема 1. *Для любых натуральных s, n верно*

$$C(2, n, s, \mathcal{L}_2) \asymp \sqrt{n}.$$

Автор выражает благодарность Э. Э. Гасанову за постановку задачи.

Список литературы

[1] Chor B., Goldreich O., Kushilevitz E., Sudan M. Private information retrieval // Proc. of the 36th Annu. IEEE Symp. on Foundations of Computer Science. P 41–51. 1995. Journal version: J. of the ACM. 45: 965–981. 1998.

[2] Гасанов Э. Э., Майлыбаева Г. А. Доступ к базам данных без раскрытия запроса // Материалы конференции «Математика и безопасные информационные технологии». Москва, 23–24 октября 2003 г. С. 393–395.

[3] Майлыбаева Г. А. Оценки коммуникационной сложности PIR-протоколов с малыми случайными числами // Тезисы докладов XIV Международной конференции «Проблемы теоретической кибернетики». Пенза, 23–25 мая 2005 г. М., 2005. С. 93.