ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 23 МАТЕМАТИКИ Выпуск 3
2016

Д. В. Пильщиков (Москва, Лаб. ТВП)**. О некоторых свойствах моментов числа прообразов случайно выбранной точки.**

Ряд задач прикладной дискретной математики (особенно прикладной криптографии (см. [1, 2, 3]) связан с задачей обращения однонаправленной функции

$$G : X'' \to X'$$

в одной из точек набора $\{a_1, \ldots, a_D\}$, $a_i \in X'$, $i \in \overline{1, D}$.

В переборных алгоритмах типа «балансировка время–память–данные» эта задача сводится к многократному поиску решения уравнения вида $F(x) = a$ в подготовленных специальным образом таблицах значений некоторой функции $F : X \to X$, связанной определенным образом с функцией G.

В ряде подходов к оценке временной сложности балансировок время-память-данные (см. [4, 5]) в качестве математической модели числа прообразов точки $x \in X$ относительно t-кратной композиции функции F используется ветвящийся процесс Гальтона–Ватсона $\mu(t)$, $t = 0, 1, \ldots$. Получаемые в этом случае асимптотические оценки сложности решения задачи обращения однонаправленной функции G, как правило, зависят от асимптотического поведения трех первых факториальных моментов числа непосредственных потомков одной частицы процесса μ.

Распределение данной случайной величины полагается равным распределению мощности ξ_F полного прообраза случайно и равновероятно выбранной точки $x \in X$ относительно функции F

$$\mathbf{P}\{\mu(1) = d\} = \mathbf{P}\{\xi_F = d\}.$$

В связи с этим возникает задача оценки первых трех факториальных моментов ξ_F через подходящие характеристики отображения G. Изложенные далее результаты связаны с ее решением.

Для произвольной функции $G : X'' \to X'$ обозначим

$$p_G(d) = \frac{\left|\left\{ x \in X' \middle| \left|F^{-1}(x)\right| = d \right\}\right|}{|X'|},$$

$$\mu_G^{(1)} = \sum_{d=0}^{N'} p_G(d)d, \quad \mu_G^{(2)} = \sum_{d=0}^{N} p_G(d)d^{[2]}, \quad \mu_G^{(3)} = \sum_{d=0}^{N} p_G(d)d^{[3]}, \quad \mu_G^{\langle 3\rangle} = \sum_{d=0}^{N} p_G(d)d^3.$$

Пусть функция G выбирается случайно и равновероятно среди всех функций, отображающих множество $X'', |X''| = N''$, в множество $X', |X'| = N'$, а моменты $\mu_G^{(1)}$, $\mu_G^{(2)}$, $\mu_G^{(3)}$ рассматриваются как случайные величины.

Теорема 1. *Выполняются следующие равенства*:

$$\mu_G^{(1)} = \frac{N''}{N'},$$

$$\mathbf{E}\mu_G^{(2)} = \frac{(N'')^{[2]}}{(N')^2}, \quad \mathbf{E}\mu_G^{(3)} = \frac{(N'')^{[3]}}{(N')^3},$$

а при любом $C > 0$ *выполняются следующие неравенства*

$$\mathbf{P}\left\{\left|\mu_G^{(2)} - \frac{(N'')^{[2]}}{(N')^2}\right| > \sqrt{\frac{C}{N'}}\right\} < \frac{2}{C}\left(\frac{N''}{N'}\right)^2,$$

$$\mathbf{P}\left\{\left|\mu_G^{(3)} - \frac{(N'')^{[3]}}{(N')^3}\right| > \sqrt{\frac{C}{N'}}\right\} < \frac{6}{C}\left(1 + 3\cdot\frac{N''}{N'}\right)\left(\frac{N''}{N'}\right)^3.$$

Пусть теперь функция $G : X' \to X$ является ограничением функции $F : X \to X$, $|X| = N$, на множество $X' = X\backslash\Theta$, $\Theta \subset X$, $|\Theta| = \frac{N}{t}$.

Теорема 2. *При любом выборе множества* Θ *верны следующие соотношения*

$$\mu_F^{(1)} = 1, \quad \mu_G^{(1)} = 1 - 1/t,$$
$$\mu_G^{(2)} = \mu_F^{(2)} - \varepsilon, \quad |\varepsilon| \leqslant 2\sqrt{\frac{1}{t}\mu_F^{\langle 3\rangle}},$$
$$\mu_G^{\langle 3\rangle} \leqslant \mu_F^{\langle 3\rangle}.$$

Рассмотрим два фиксированных отображения $G' : X'' \to X'$, $G : X' \to X$ и подстановку $\pi : X' \to X'$. Построим композицию $G'' : X'' \to X$ этих отображений

$$G''(x) = G \circ \pi \circ G'(x).$$

Пусть подстановка π выбирается случайно и равновероятно среди всех подстановок, отображающих множество X' в себя, а момент $\mu_{G''}^{(2)}$ рассматривается как случайная величина.

Теорема 3. *Верна формула*

$$\mathbf{E}\mu_{G''}^{(2)} = \mu_G^{(2)}\frac{(N'')^{[2]}}{(N')^{[2]}} + \frac{N'}{N}\mu_{G'}^{(2)} - \mu_G^{(2)}\mu_{G'}^{(2)}\frac{1}{N'-1}.$$

Рассмотрим теперь два фиксированных отображения $F' : X' \to X'$, $G : X' \to X$, подстановку $\pi : X' \to X'$ и инъективное отображение $\varphi : X \to X'$. Построим композицию $F : X \to X$ этих отображений

$$F(x) = G \circ \pi \circ F' \circ \varphi(x).$$

Пусть подстановка π выбирается случайно и равновероятно среди всех подстановок, отображающих множество X' в себя, отображение φ выбирается случайно и равновероятно среди всех инъективных отображений множества X в множество X', а момент $\mu_F^{(2)}$ рассматривается как случайная величина.

Следствие. *Верна формула*

$$\mathbf{E}\mu_F^{(2)} = \mu_G^{(2)}\frac{(N)^{[2]}}{(N')^{[2]}} + \mu_{F'}^{(2)}\frac{N-1}{N'-1} - \mu_G^{(2)}\frac{(N)^{[2]}}{(N')^{[2]}}\frac{\mu_{F'}^{(2)}}{N'-1}.$$

СПИСОК ЛИТЕРАТУРЫ

1. *Hellman M. E.* A cryptanalytic time-memory trade-off. — IEEE Trans. Inform. Theory, 1980, v. IT-26, is. 4, p. 401–406.
2. *Standaert F.-X., Rouvroy G., Quisquater J.-J., Legat J.-D.* A time-memory tradeoff using distinguished points: New analysis & FPGA results. — In: Cryptographic Hardware and Embedded Systems–CHES 2002. 4th International Workshop (Redwood Shores, CA, August 13–15, 2002). Revised Papers. Ed. by B. S. Kaliski, Jr., C. K. Koc, C. Paar. Heidelberg etc.: Springer, 2002, p. 593–610. (Ser. Lect. Notes Comput. Sci. V. 2523.)

3. *Oechslin P.* Making a faster cryptanalytic time-memory trade-off. — In: Advances in Cryptology–CRYPTO 2003. 23rd Annual International Cryptology Conference (Santa Barbara, CA, August 17–21, 2003). Proceedings. Ed. by D. Boneh. Heidelberg etc.: Springer, 2003, p. 617–630. (Ser. Lect. Notes Comput. Sci. V. 2729.)
4. *Pilshchikov D. V.* Estimation of the characteristics of time-memory-data trade-off methods via generating functions of the number particles and the total number of particles in the Galton–Watson process. — Матем. вопросы криптографии, 2014, т. 5, в. 2, с. 103–108.
5. *Пильщиков Д. В.* Анализ сложности алгоритма параллельного поиска «золотой» коллизии. — Матем. вопросы криптографии, 2015, т. 6, в. 4, с. 77–98.