ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 23 МАТЕМАТИКИ Выпуск 5
2016

Д. В. Пильщиков (Москва, Лаб. ТВП). **О связях между моделями случайных деревьев, возникающих в задачах обоснования сложности методов балансировки время-память.**

Ряд задач прикладной математики связан с задачей обращения однонаправленной функции

$$G : X \to X, \quad |X| = N,$$

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

Для решения этой задачи широкое распространение получили методы балансировки время–память–данные [1, 2, 3]. В одном из подходов к оценке сложности этих методов возникает проблема оценки средних значений характеристик случайного дерева $T_{x,F}$, являющегося максимальным поддеревом графа случайного отображения $F : X \to X$ с корнем в $x \in X$. Для ее решения в [4] предлагается использовать значение аналогичных характеристик случайного дерева, моделирующего реализации подходящего процесса Гальтона–Ватсона [5]. Изложенные далее результаты связаны с обоснованием данного подхода.

Пусть имеется упорядоченное множество $X = \{x_1, \ldots, x_N\}$. Каждое отображение $F : X \to X$ задает ориентированный граф. Его вершинами являются элементы множества X, а дуга из вершины x' ведет в вершину x'' тогда и только тогда, когда $F(x'') = x'$. С элементом $x \in X$ свяжем ориентированное дерево $T_{x,F}$, являющееся максимальным поддеревом графа отображения F с корнем x и некорневыми вершинами из множества $X \backslash \{x\}$. Обозначим множество всех таких деревьев через $\mathcal{P}(X, x)$.

Пусть $\mathcal{G}$ — множество всех генеалогических деревьев [5]. Каждому дереву $T \in \mathcal{P}(X, x)$ поставим в соответствие генеалогическое дерево $\varphi(T) \in \mathcal{G}$. Для этого вершине x дерева T поставим в соответствие вершину (0) генеалогического дерева.

Далее, если $x_{i_1}, \ldots, x_{i_{m(0)}}$, $i_1 < \cdots < i_{m(0)}$ — полный набор вершин дерева T первого уровня, то поставим им в соответствие вершины $(01), \ldots, (0m_{(0)})$ генеалогического дерева. Проводя аналогичные действия уровень за уровнем построим генеалогическое дерево $\varphi(T)$, соответствующее дереву T.

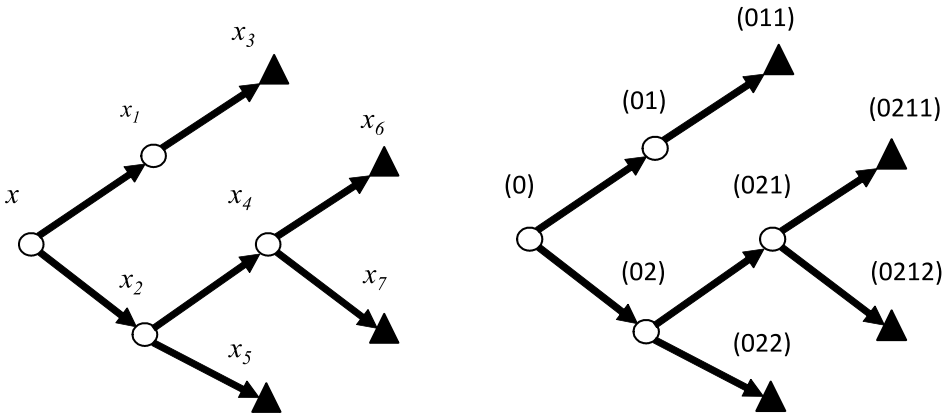

Рис. Дерево $T \in \mathcal{P}(X, x)$ и соответствующее ему дерево $\varphi(T) \in \mathcal{G}$.

Пусть теперь на множестве всех отображений множества X в себя задана вероятностная мера $\mathbf{P}_0$. Она естественным образом индуцирует вероятностную меру $\mathbf{P}_1$ на множестве генеалогических деревьев

$$\mathbf{P}_1(G) = \mathbf{P}_0(\varphi(T_{x,F}) = G), \quad G \in \mathcal{G}.$$

По мере $\mathbf{P}_1$ на $\mathcal{G}$ построим меру $\mathbf{P}_2$, определяющую процесс Гальтона–Ватсона. Для этого положим

$$\mathbf{P}_2(\mu_0(G) = k) = \mathbf{P}_1(\mu_0(G) = k), \quad k = 0, 1, \ldots,$$

где $\mu_0(G)$ — кратность корня дерева G. Случайные генеалогические деревья, заданные на вероятностных пространствах $\{\mathcal{G}, \mathbf{P}_1\}$ и $\{\mathcal{G}, \mathbf{P}_2\}$, обозначим $\mathcal{T}_1$ и $\mathcal{T}_2$.

Приводимые далее результаты описывают условия при которых средние значения случайных величин $\zeta(\mathcal{T}_1)$ и $\zeta(\mathcal{T}_2)$ асимптотически сближаются для широкого круга числовых характеристик $\zeta(G) : \mathcal{G} \to \mathbb{R}^+$ и вероятностных мер $\mathbf{P}_0$.

Пусть $F_0 : X \to X$ — фиксированное отображение и $\mathcal{H} : X \to X$ — случайная подстановка, принимающая каждое из $N!$ значений с одинаковой вероятностью. Меру $\mathbf{P}_0$ зададим по формуле

$$\mathbf{P}_0(F) = \mathbf{P}(\mathcal{H}(F_0) = F), \quad F \in X^X.$$

Через $v_r(t, T)$ обозначим число вершин кратности r, $r \in 0, \ldots, N$, находящихся в первых t слоях дерева $T \in \mathcal{G}$.

Теорема 1. *Верно следующее соотношение между распределениями случайных деревьев $\mathcal{T}_1$ и $\mathcal{T}_2$*

$$\mathbf{P}(v_0(t, \mathcal{T}_1) = k_0, \ldots, v_N(t, \mathcal{T}_1) = k_N) = \gamma(k_0, \ldots, k_N) \cdot \mathbf{P}(v_0(t, \mathcal{T}_2) = k_0, \ldots, v_N(t, \mathcal{T}_2) = k_N),$$

где $(k_0, \ldots, k_N)$ — произвольный набор неотрицательных целых чисел,

$$\gamma(k_0, \ldots, k_N) = \frac{\prod_{r=0}^{N} \prod_{i=0}^{k_r - 1} (1 - \frac{i}{N_r})}{\prod_{i=0}^{\sum_{r=0}^{N} k_r - 1} (1 - \frac{i}{N})},$$

$$N_r = \Big| \big\{ x' \in X \,|\, |F_0^{-1}(x') \backslash \{x\}| = r \big\} \Big|, \quad r \in 0, \ldots, N.$$

Рассмотрим последовательности множеств X_s ($|X_s| = N_s$), отображений $F_{0,s} : X_s \to X_s$ и числовых характеристик $\zeta_s : \mathcal{G} \to \mathbb{R}^+$, $s \in 1, 2, \ldots$. Для каждого s

описанным выше образом построим на $\mathcal{G}$ меры $P_{1,s}$ и $P_{2,s}$ (при произвольном выборе элемента $x_s \in X_s$), случайные деревья $\mathcal{T}_{1,s}$, $\mathcal{T}_{2,s}$ и случайные величины $\zeta_s(\mathcal{T}_{1,s})$, $\zeta_s(\mathcal{T}_{2,s})$. Для отображений $F_{0,s}$ определим величины $N_{r,s} = |\{x' \in X || F_{0,s}^{-1}(x') \backslash \{x_s\}| = r\}|, r \in 0, \ldots, N_s$.

Следующая теорема описывает условия, при которых из сходимости ряда $\mathbf{E}\zeta_s(\mathcal{T}_{2,s})$, $s = 1, 2, \ldots$, следует сходимость к тому же пределу ряда $\mathbf{E}\zeta_s(\mathcal{T}_{1,s})$, $s = 1, 2, \ldots$.

Теорема 2. *Пусть при* $s \to \infty$ *выполняются соотношения*
1) $\mathbf{E}\zeta_s(\mathcal{T}_{2,s}) \to A \leqslant \infty$,
2) $N_s \to \infty$,
3) $\max \zeta_s = O(N_s^{1/3})$,
4) $\sum_{r=0}^{N_s} \frac{N_{r,s}}{N_s} r^3 = o(N_s^{1/3})$.
Тогда при $s \to \infty$ *существует предел* $\mathbf{E}\zeta_s(\mathcal{T}_{1,s}) \to A$.

СПИСОК ЛИТЕРАТУРЫ

1. *Hellman M. E.* A cryptanalytic time-memory trade off. — IEEE Transactions on Information Theory, 1980, IT-26, p. 401–406.
2. *Borst J.*, *Preneel B.*, *Vandewalle J.* A Time-Memory Tradeoffs using Distinguished Points. — Technical report ESAT-COSIC Report 98-1 / Departement of Electrical Engineering, Katholieke Universiteit Leuven, 1998.
3. *Oechslin P.* Making a faster cryptanalytic time-memory trade-off. — Advances in Cryptology–CRYPTO'03, Santa Barbara, California, USA, August 2003. Springer-Verlag, 2003. (Lecture Notes in Computer Science); v. 2729, p. 617–630.
4. *Pilshchikov D. V.* Estimation of the characteristics of time-memory-data tradeoff methods via generating functions of the number particles and the total number of particles in the Galton-Watson process. — Математические вопросы криптографии, 2014, т. 5, в. 2, с. 103–108.
5. *Ватутин В. А.* Распределение расстояния до корня минимального поддерева, содержащего все вершины данной высоты. — Теория вероятн. и ее примен., 1993, т. 38, в. 2, с. 273–287.