Math-Net.Ru

Общероссийский математический портал

D. V. Pilshchikov, Оценка характеристик методов балансировки времени-памяти-данных с помощью производящих функций числа частиц и общего числа частиц в процессе Гальтона–Ватсона, *Матем. вопр. криптогр.*, 2014, том 5, выпуск 2, 103–108

DOI: <https://doi.org/10.4213/mvk122>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.198.55.26

26 апреля 2023 г., 16:56:09

Estimation of the characteristics of time-memory-data tradeoff methods via generating functions of the number of particles and the total number of particles in the Galton-Watson process

D. V. Pilshchikov

TVP Laboratory, Moscow

Received 25.09.2013

Time-memory-data tradeoff algorithms are tools for inverting one-way functions. This work provides some mathematical results for an accurate complexity analysis of the most famous of them. We consider a probabilistic model which allows us to estimate the mean values of some characteristics by studying the asymptotic behavior of the generating function of the joint distribution of the number of particles and the total number of particles in the subcritical and critical Galton-Watson processes.

Keywords: time-memory-data tradeoff.

Оценка характеристик методов балансировки времени-памяти-данных с помощью производящих функций числа частиц и общего числа частиц в процессе Гальтона–Ватсона

Д. В. Пильщиков

Лаборатория ТВП, Москва

Аннотация. Алгоритмы балансировки времени-памяти-данных используются для обращения однонаправленных функций. В работе приводятся математические результаты, позволяющие провести точный анализ сложности большинства известных алгоритмов такого типа. Для вероятностной модели получены оценки средних значений некоторых характеристик с помощью исследования предельного поведения производящих функций совместных распределений числа частиц и общего числа частиц в докритических и критических процессах Гальтона–Ватсона.

Ключевые слова: балансировка времени-памяти-данных.

In [3]–[12], [14], a problem of inverting an one-way function was considered. The results may be summarized as follows.

Let

$$G : X \rightarrow X,$$

be an one-way function defined on a set X , $|X| = N$, and $\mathcal{D}$ be a set of D elements of set X of the form

$$\mathcal{D} = \{y_i \in X | y_i = G(x_i), i \in 1, \dots, D\},$$

where

$$\{x_n \in X, n \in 1, \dots, D\}$$

is some unknown set $\bar{\mathcal{D}}$. The goal is to find at least 1 element of the set $\bar{\mathcal{D}}$ given the set $\mathcal{D}$.

Time-memory-data tradeoff algorithms are widely used to solve this problem. The most popular of these are the following three methods:

- classical Hellman tradeoffs ([7]) (the *HM*-method);
- distinguished points method ([5]) (the *DP*-method);
- the rainbow tables method ([12]) (the *RM*-method).

Any tradeoff method consists of two phases: pre-computation and online, in both phases chains of F -operations are calculated. Each chain is a sequential evaluations of the function (F -operations) of the form

$$F(x) = R(G(x)), x \in X,$$

where $R : X \rightarrow X$ a bijective function.

At the pre-computation phase, the tables consisting of start- and endpoints are constructed.

A solution to the problem is found at the online phase using tables constructed at the pre-computation phase. During the online phase, two types of chains are calculated: basic and additional. Basic chains start from elements of the set $\mathcal{D}$. If the end of the basic chain is found in the pre-computation table, an additional chain of F -operations is calculated to find the solution.

All of these methods and their numerous modifications (e.g. the modifications with perfect table [4]: the *DPP*-method and the *RMP*-method) may be concretized by such parameters as the size of the search space, the length of chains, the size of the tables used and their number. They are characterized by the probability of success, the (average) number of F -operations performed at the pre-computation and online phases (including basic and additional chains), and by the number of table lookups. In the papers referenced

above, some relations between these parameters and the characteristics of the methods are described. However, for some characteristics there are only upper or lower estimates, and for others their average values are calculated for the simplified probabilistic models.

In this work, a more accurate probabilistic model is considered. It allows us to solve the problem of estimating the average values of all the characteristics of the above methods by studying the asymptotic behavior of the generating function of the joint distribution of the number of particles and the total number of particles in the subcritical (*DP*, *DPP*-methods) and critical (*RM*-, *RMP*-, *HM*-methods) Galton-Watson processes.

Now we will describe our probabilistic model.

It is determined by parameters r, m , set $X, |X| = N$, and a function $G : X \rightarrow X$ with the characteristic

$$B = \frac{1}{N} \left(\sum_{x \in X} |G^{-1}(x)|^2 \right) - 1.$$

By X^G we denote the set of all functions of the form

$$X^G = \{R(G(x)) | R \in S(X)\},$$

where $S(X)$ is a permutation group on the set X .

For our probabilistic model we will use the following assumptions:

- all F -operations used in tradeoff algorithms are the result of sampling with replacement from the set X^G ;
- elements of the set $\bar{D}$ are the result of sampling with replacement from the set X ;
- each point of the set X may be the first point of a chain independently of the other points of X with the probability $\frac{m}{N}$; the sets of first points for different tables are chosen independently.

A theorem describing the asymptotic behavior of the generating function of the joint distribution of the number of particles and the total number of particles in the Galton-Watson process is formulated as follows (similar results may be found in [1, 2, 13]).

Let $a, b, c > 0, K = [0, a] \times [0, b] \times [0, c]$. Consider an increasing number sequence $t_k, k = 1, 2, 3, \dots$,

$$t_1 \geq \{a, \sqrt{c}, b + ac\}, t_k \rightarrow \infty,$$

and a sequence of the Galton-Watson processes $\mu_k(i), k = 1, 2, \dots$, with time parameter $i = 0, 1, \dots$. We assume that the first three factorial moments of random variable $\mu_k(1), k = 1, 2, \dots$ are denoted by

$$\mathbf{E}\mu_k(1) = 1 - \frac{A_k}{t_k}, A_k \geq 0,$$

$$\mathbf{E}\mu_k^{(2)}(1) = B_k, B_k > 0,$$

$$\mathbf{E}\mu_k^{(3)}(1) = R_k.$$

Let $v_k(i)$ be the total number of particles before time i

$$v_k(i) = \sum_{j=0}^{i-1} \mu_k(j),$$

$F_{k,i}(y, z)$ be the generating function of the vector $(\mu_k(i), v_k(i))$ distribution

$$F_{k,i}(y, z) = \mathbf{E} y^{\mu_k(i)} z^{v_k(i)} = \sum_{h=0}^{\infty} \sum_{n=0}^{\infty} \mathbf{P}\{\mu_k(i) = h, v_k(i) = n\} y^h z^n,$$

and $\tilde{F}_{k,i}(y, z)$ be its partial derivative

$$\tilde{F}_{k,i}(y, z) = \frac{\partial F_{k,i}(y, z)}{\partial y} = \sum_{h=1}^{\infty} \sum_{n=0}^{\infty} h \mathbf{P}\{\mu_k(i) = h, v_k(i) = n\} y^{h-1} z^n.$$

Consider two sequences of real-valued functions defined on K :

$$r_k(x, y, z) = t_k \left(1 - F_{k,[xt_k]} \left(1 - \frac{y}{t_k}, 1 - \frac{z}{t_k^2} \right) \right),$$

$$\tilde{r}_k(x, y, z) = \tilde{F}_{k,[xt_k]} \left(1 - \frac{y}{t_k}, 1 - \frac{z}{t_k^2} \right).$$

For $A \geq 0, B > 0$ and $(x, y, z) \in [0, \infty)^3$ we define functions

$$f_{A,B}(x, y, z) = \frac{1}{B/2} f_1 \left(x, y \cdot B/2 + A/2, z \cdot B/2 + \left(\frac{A}{2} \right)^2 \right) - (A/B),$$

$$\tilde{f}_{A,B}(x, y, z) = \tilde{f}_0 \left((y + (A/B)) x B/2, \left(z + \frac{A^2}{2B} \right) x^2 B/2 \right),$$

where

$$f_1(x, y, z) = \frac{1}{x} f_0(yx, zx^2), x > 0, f_1(0, y, z) = y,$$

$$f_0(y, z) = \frac{y + \sqrt{z} \cdot th(\sqrt{z})}{1 + y \cdot \frac{th\sqrt{z}}{\sqrt{z}}}, z > 0, f_0(y, 0) = \frac{y}{1 + y},$$

$$\tilde{f}_0(y, z) = \frac{1}{(ch\sqrt{z} + y \frac{sh\sqrt{z}}{\sqrt{z}})^2}, z > 0, \tilde{f}_0(y, 0) = \frac{1}{(1 + y)^2}.$$

Theorem 1. *Let the sequences A_k and $B_k, k = 1, 2, \dots$, converge to the limits A and B respectively, and the sequence $R_k, k \in 1, 2, \dots$, is bounded. Then the sequence of functions of three variables*

$$r_k(x, y, z) = t_k \left(1 - F_{k,[xt_k]} \left(1 - \frac{y}{t_k}, 1 - \frac{z}{t_k^2} \right) \right), k = 1, 2, \dots,$$

converges to the function $f_{A,B}(x, y, z)$ uniformly on K , and the sequence of functions of three variables

$$\tilde{r}_k(x, y, z) = \tilde{F}_{k, [xt_k]} \left(1 - \frac{y}{t_k}, 1 - \frac{z}{t_k^2} \right), k = 1, 2, \dots,$$

converges to the function $\tilde{f}_{A,B}(x, y, z)$ uniformly on K .

This theorem and the above probabilistic model allow us to describe a functional relationship of all characteristics of *HM*-, *DP*-, *DPP*-, *RMP*-, *RM*-methods and their parameters in terms of functions $f_{A,B}(x, y, z)$, $\tilde{f}_{A,B}(x, y, z)$.

References

- [1] *Vatutin V. A., Sagitov S. M.* A decomposable critical branching process with two types of particles // Proc. Steklov Inst. Math. — 1988. — V. 177. — P. 1–19
- [2] *Aliev S. A., Shurenkov V. M.* Transitional Phenomena and the Convergence of Galton-Watson Processes to Jirina Processes // Theory Probab. Appl. — 1983. — V. 27. №3. — P. 472–485.
- [3] *Avoine G., Junod P., Oechslin P.* Time-memory trade-offs: False alarm detection using checkpoints (extended version) // Tech. Rep. LASEC-REPORT 2005-002, Swiss Federal Institute of Technology (EPFL), Security and Cryptography Laboratory (LASAC), Lausanne, Switzerland, September 2005.
- [4] *Avoine G., Junod P., Oechslin P.* Characterization and improvement of Time-Memory Trade-Off based on perfect tables // Trans. Inf. Syst. Secur., 11:17:1–17:22, July 2008.
- [5] *Borst J., Preneel B., Vandewalle J.* On the time-memory tradeoff between exhaustive key search and table precomputation // Proc. 19th Symp. Inf. Theory in the Benelux, WIC. — 1998. — P. 111–118.
- [6] *Matsumoto T., Kim I., Hara T.* Methods to reduce time and memory in time-memory tradeoff // ISEC97-10, May 26, 1997.
- [7] *Hellman M. E.* A cryptanalytic time-memory trade off // IEEE Trans. Inf. Theory, IT-26. — 1980. — P. 401–406.
- [8] *Hong J.* The cost of false alarms in Hellman and rainbow tradeoffs // Des. Codes Cryptogr. — 2010. — V. 57. №3. — P. 293–327.
- [9] *Hong J., Jeong K. C., Kwon. E. Y., Lee I.-S., Ma D.* Variants of the distinguished point method for cryptanalytic time memory trade-off // ISPEC 2008, LNCS. — 2008. — V. 4991. — P. 131–145.

- [10] *Kim I.-J., Matsumoto T.* Achieving higher success probability in time-memory trade-off cryptanalysis without increasing memory size // IEICE Trans. Fundamentals, E82-A. — 1999. — P. 123–129.
- [11] *Ma D., Hong J.* Success probability of the Hellman trade-off // Inf. Process. Lett. — 2008. — V. 109. №7. — P. 347–351.
- [12] *Oechslin P.* Making a faster cryptanalytic time-memory trade-off // CRYPTO'03, LNCS. — 2003. — V. 2729. — P. 617–630.
- [13] *Pakes A. G.* Some limit theorems for the total progeny of a branching process // Adv. Appl. Probab. — 1971. — V. 3. №1. — P. 176–192.
- [14] *Standaert F. X., Rouvroy G., Quisquater J. J., Legat J. D.* A time-memory tradeoff using distinguished points: New analysis & FPGA results // Proc. CHES 2002, LNCS. — 2002. — P. 596–611.