Statistical mechanical formulation and simulation of prime factorization of integers

Chihiro H Nakajima
Department of Physics, Kyushu University

We are proposing a formulation of the problem prime factorization of integers as a ground state searching problem. The purpose of this study is to estimate computational complexity of the prime factorization problem with stochastic algorithms on classical computers.

When an integer N_o is located in $2^{n-1} < N_o \leq 2^n$, the maximum number of prime divisors is bounded by n. We performed replica exchange Monte Carlo simulations of the system which is constructed by n degree of freedom $\{d_i\}$, $(i = 1, \cdots, n)$. Each d_i takes the value $d_i \in \{1, \cdots, 2^n\}$. The detail of the cost function $H(\{d_i\})$ is shown as,

$$H(\{d_i\}) = H_1 + H_2 \tag{1}$$

$$H_1 = \sum_{i=1}^{n} \epsilon_i \ , \ \ \epsilon_i = \min\left(\mathrm{mod}(N_o, d_i) \ , \ d_i - \mathrm{mod}(N_o, d_i) \right) \tag{2}$$

$$H_2 = \left(\log N_o - \sum_{i=1}^{n} \log(d_i) \right)^2 - \gamma M \tag{3}$$

$$d_i(\{\sigma_{i,j}\}) = 1 + \sum_{j=1}^{n-1} \sigma_{i,j} 2^{j-1}, \qquad \sigma_{i,j} \in \{1, -1\} \qquad , \tag{4}$$

where M is the number of divisors $\{d_i\}$ which are larger than 1. H_1 is the cost to prefer the case when N_o is divisible by each $\{d_i\}$. As temperature in simulation T goes lower, indivisible combinations of $\{d_i\}$ are thus excluded (see Fig. 1). H_2 is the cost to prefer the case when the production $\prod_{i=1}^{n} d_i$ is quivalent to N_o. And by the term $-\gamma M$, the combination of $\{d_i\}$ which includes the largest number of non-trivial divisors becomes the most prefered.

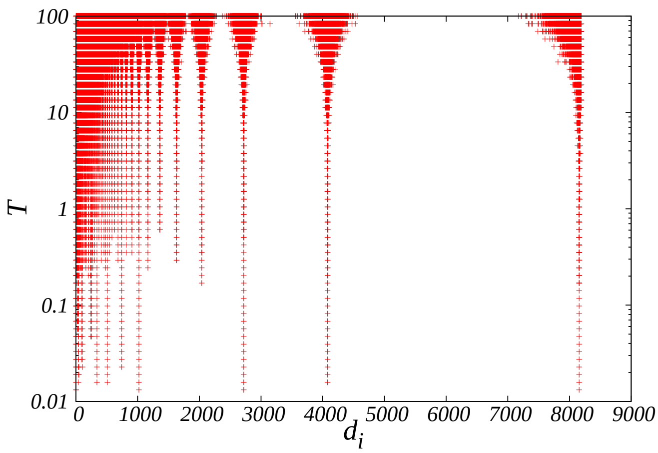

Figure 1: The example of simulated histogram of each d_i in each temperature with $N_o = 8157$. This picture is projected onto $d_i - T$ plane, and the state which is hit more than one time is plotted.

The objective of this study is to obtain the probability of finding correct factorization as a function of Monte Carlo step τ_{MC}, and its asymptotic behavior with increasing of τ_{MC} and n.