2016 International Symposium on Nonlinear Theory and Its Applications,
NOLTA2016, Yugawara, Japan, November 27th-30th, 2016

Performance Analysis of the Interval Algorithm for Random Number Generation in the Case of Markov Coin Tossings

Yasutada Oohama[†]

†University of Electro-Communications,
1-5-1 Chofugaoka, Chofu-shi, Tokyo 182-8585, Japan
Email: oohama@uec.ac.jp

Abstract—In this paper we analyze the interval algorithm for random number generation proposed by Han and Hoshi in the case of Markov coin tossings. Using the expression of real numbers on the interval [0,1), we first establish an explicit representation of the interval algorithm with the representation of real numbers on the interval [0,1) based one number systems. Next, using the expression of the interval algorithm, we give a rigorous analysis of the interval algorithm. We discuss the difference between the expected number of the coin tosses in the interval algorithm and their upper bound derived by Han and Hoshi and show that it can be characterized explicitly with the established expression of the interval algorithm.

1. Introduction

Simulation problems of generating random sequences from a prescribed information source by using a random sequence from a given information source are called the random number generation. In the random number generation random sequences from a prescribed information sources are called the *target* random sequences which we wish to *produce* and the random sequence from given information sources are called the *coin* random sequences that the target random sequences are *made from*.

There have been several works on the random number generation in the field of computer science and information theory. Some interesting relations between random number generation and information theory have been found in the papers of Elias [1] and Knuth and Yao [2].

Han and Hoshi [3] studied a variable-to-fixed random number generation problem. They studied the method of generating target random sequences of *fixed length* from a prescribed information source by using coin random sequences of *variable length* from a given information source. They proposed a simple algorithm called the interval algorithm and obtained results for its performance analysis. They established an upper bound of the average length of coin random sequences necessary to create target random sequences. The derived bound is characterized with a fraction of two entropies of given and prescribed sources and is shown to be asymptotically optimal for large length of output sequences.

In our previous work [4], we studied the performance analysis of the interval algorithm for random number generation proposed by Han and Hoshi [3]. In this work we treated the case where we wish generate a target random variable by using a *coin* random sequence from a stationary memoryless sources. In this paper we study the performance analysis of the interval algorithm in an extended case where coin random sequences are from the stationary Markov information sources.

In [4], we derived explicit results on the performance analysis of the interval algorithm for random number generation using an expression of real numbers in the unit interval [0,1). On the expression of real numbers in the unit interval, we used a kind of generalized number system based on the stochastic structure of the coin random process. Using the above representation of real numbers on the interval, we established an explicit expression of the interval algorithm. In this paper we show that the same result also holds for the case where the coin random process is a Markov chain. Using this expression of the algorithm, we give a rigorous analysis of the interval algorithm. We discuss the difference between the expected number of the coin tosses in the interval algorithm and their upper bound derived by Han and Hoshi and show that it can be characterized explicitly with the established expression of the interval algorithm.

2. Interval Algorithm for Random Number Generation

Let X be random variables taking values in a finite set $\mathcal{X} \triangleq \{0,1,\cdots,N-1\}$. Let $p_X \triangleq \{p_X(x)\}_{x\in\mathcal{X}}$ be a probability distribution of X. Let $\{Y_t\}_{t=1}^{\infty}$ be a stationary Markov source. For each $t = 1,2,\cdots$, Y_t takes values in a finite set $\mathcal{Y} \triangleq \{0,1,\ \cdots,M-1\}$. The stationary Markov source $\{Y_t\}_{t=1}^{\infty}$ is specified with the $M \times M$ stochastic matrix denoted by $P = [P_{ij}]$, where

$$P_{ij} = \Pr\{Y_{t+1} = j|Y_t = i\},\ \text{for } t = 1,2,\cdots.$$

We also write $P_{ij}, (i,j)\times\mathcal{Y}^2$ as $P_{ij} = p_Y(j|i)$. Let $\mathcal{Y}^*$ denote the set of all finite sequence emitted from the above information source. We write a string from information source as $y_l^m \triangleq y_l\, y_{l+1} \cdots y_m \in \mathcal{Y}^*$. If $l > m$, the string y_l^m means *null* string denoted by λ. When $l = 1$, we frequently omit the suffix 1 of y_1^m and write $y^m = y_1 y_2 \cdots y_m$. Let $p_Y(y_l^m)$ denote the probability of y_l^m. Since the information source is a stationary Markov source, we have

$$p_Y(y_l^m) = p_Y(y_l) P_{y_l y_{l+1}} \cdots P_{y_{m-1} y_m}.$$

Here $\{p_Y(a)\}_{a \in \mathcal{Y}}$ is a stationary distribution computed from P. The probability of the null string λ assumes to be one.

In this paper we deal with the variable to fixed random number generation problem of generating target random variable X by using the coin random sequence Y_1 $Y_2 \cdots Y_i \cdots$ from a stationary Markov information sources $\{Y_t\}_{t=1}^{\infty}$. A formal definition of the variable to fixed random number generation problem is the following. Repeated tosses of the coin random variable Y produces random sequence $Y_1, Y_2, \cdots$ from a discrete memoryless source. The coin toss terminates at some finite time L to generate a random variable X with a prescribed distribution p_X. L is a random variable specified in terms of a deterministic two valued function such that $f(Y^i)$ ='Continue' for $1 \le i \le L-1$ and $f(Z^L)$ ='Stop'. The output X is expressed as $X = \psi(Y^L)$ with some deterministic function ψ.

In the above random number generation problem Han and Hoshi [3] proposed a simple algorithm called interval algorithm and evaluated its performance. Let $I = [0, 1)$. Define the cumulative probabilities for p_Y by

$$c_Y(0) \triangleq 0, c_Y(y) \triangleq \sum_{i<y} p_Y(i), 1 \le y \le M-1.$$

Using these probabilities, define the decomposition of I by

$$I_Y(y) \triangleq [c_Y(y), c_Y(y) + p_Y(y)).$$

For p_X, we use the same notations and definitions as those for p_Y. For given $y_1 \in \mathcal{Y}$, define the cumulative probabilities for $p_Y(\cdot|y_1) = \{p_Y(y_2|y_1)\}_{y_2 \in \mathcal{Y}}$ by

$$c_Y(0|y_1) \triangleq 0, c_Y(y_2|y_1) \triangleq \sum_{i<y_2} p_Y(i|y_1), 1 \le y_2 \le M-1.$$

For $k = 1, 2, \cdots$, and any string $y^k = y_1 y_2 \cdots y_k \in \mathcal{Y}^k$, define the semi-open interval $I_Y(y^k) \triangleq [L_Y(y^k), U_Y(y^k))$ by the following recursions:

$$\left.\begin{aligned} &L_Y(y_1) = c_Y(y_1), \\ &U_Y(y_1) = c_Y(y_1) + p_Y(y_1) \\ &L_Y(y^i) = L_Y(y^{i-1}) + p_Y(y^{i-1}) c_Y(y_i|y_{i-1}), \\ &U_Y(y^i) = L_Y(y^i) + p_Y(y^i), \text{ for } 2 \le i \le k. \end{aligned}\right\} \quad (1)$$

The procedure of computing upper and lower end points of the interval corresponding to a given sequence is equivalent to the encoding algorithm in the arithmetic coding.

Interval algorithm by Han and Hoshi [3] can be stated in the following.

Interval Algorithm (Han and Hoshi [3]):

1) Set $i = k = 1, y_0 = \lambda$.
2) Given y_{i-1}, generate a letter $y_i \in \mathcal{Y}$ according to the transition provability $P_{y_{i-1} y_i}$ of the coin random variable.
3) Compute $I_Y(y^i) = [L_Y(y^i), U_Y(y^i))$ according to the recursion (1).
4) If $I_Y(y^i) \subseteq I_X(x)$ for some $x \in \mathcal{X}$, then output x as the value of target random variable X and stop the algorithm.
5) Set $i = k + 1$ and go to 2).

In the above interval algorithm the target random variable X can exactly be produced.

3. An Explicit Representation of the Interval Algorithm

In this section we give two expressions of real numbers in the interval $I = [0, 1)$ on the number system. There is some complementary relation between the above two expressions. Using those expressions we give an explicit form of the interval algorithm.

3.1. Representation of real numbers

For $z \in [0, 1)$, define the sequence $\{a_i\}_{i=1}^{\infty} \in \mathcal{Y}^*$ such that

$$z \in I_Y(a^i), i = 1, 2, \cdots.$$

It can easily be verified that using $a_1, a_2, \cdots$, z can be expressed in the following manner:

$$z = \sum_{k \ge 1} p_Y(a^{k-1}) \sum_{a < a_k} p_Y(a|a_{k-1}) = \sum_{k \ge 1} p_Y(a^{k-1}) c_Y(a_k|a_{k-1}).$$

We call the above expression *the p_Y-ary representation of the real number z* and write as

$$z = 0.a_1 a_2 a_3 \cdots . \quad (2)$$

In the above expression, if we wish to express z with the sum of the number having the expression

$$0.a_1 a_2 a_3 \cdots a_t 00 \cdots$$

and the other remaining term, we write

$$z = 0.a_1 a_2 \cdots a_t \ + \ 0.0_{a_1} 0_{a_2} \cdots 0_{a_t} a_{t+1} \cdots , \quad (3)$$

where the second term is defined by

$$0.0_{a_1} 0_{a_2} \cdots 0_{a_t} a_{t+1} \cdots \triangleq \sum_{k \ge t+1} p_Y(a^{k-1}) c_Y(a_k|a_{k-1}).$$

Next, for $z \in [0, 1)$, set $\bar{z} = 1 - z$. Using the sequence $\{a_i\}_{i \ge 1}$ appearing in the p_Y-ary representation of the real number z, $\bar{z}$ has an expression

$$\bar{z} = \sum_{k \ge 1} p_Y(a^{k-1}) \sum_{a > a_k} p_Y(a|a_{k-1}).$$

Then, adopting the notation

$$c_Y(\bar{a}|a_{k-1}) \triangleq \sum_{i>a} p_Y(i|a_{k-1}),$$

we obtain the following expression

$$\bar{z} = \sum_{k\geq 1} p_Y(a^{k-1}) c_Y(\bar{a}_k|a_{k-1}).$$

We call the above expression *the p_Y-ary co-representation of the real number z* and write as

$$\bar{z} = 0.\bar{a}_1\bar{a}_2\bar{a}_3\cdots. \tag{4}$$

Let $z^{(n)}$ denote the real number which is obtained by rounding off z to n-digits in the p_Y-ary representation, that is,

$$z^{(n)} \triangleq 0.a_1a_2\cdots a_n.$$

Similarly, let $\bar{z}^{(n)}$ denote the real number which is obtained by rounding off $\bar{z}$ to n-digits in the p_Y-ary co-representation, that is,

$$\bar{z}^{(n)} \triangleq 0.\bar{a}_1\bar{a}_2\cdots\bar{a}_n.$$

It can easily be verified that the p_Y-ary representation and the p_Y-ary co-representation of the real number z satisfy the following.

Property 1

a) *For any i, $z \in I_Y(a^i)$.*

b) $c_Y(a_i|a_{i-1}) + c_Y(\bar{a}_i|a_{i-1}) = 1 - p_Y(a_i|a_{i-1})$.

c) *For $z = 0.a_1a_2\cdots a_n\cdots \in [0,1)$, we have*

$$z^{(n)} + \bar{z}^{(n)} = 1 - p_Y(a^n).$$

3.2. An explicit representation of the interval algorithm

In this subsection, we give an explicit form of the interval algorithm by using the p_Y-ary representation and p_Y-ary co-representation of the real number in the interval $I = [0,1)$. It can easily be seen from the definition of the interval algorithm the interval $I_X(x) = [L_X(x), U_X(x))$ corresponding to the target random number $x \in \mathcal{X}$ has a form of a disjoint sum of the intervals $I_Y(\cdot)$. In our previous work we obtained an explicit form of the disjoint sum in the case where the source $\{Y_t\}_{t=1}^{\infty}$ representing coin tossings is a discrete memoryless source. In the present case where $\{Y_t\}_{t=1}^{\infty}$ is a stationary Markov source the same result holds. This result is as follows.

Theorem 1 *For $x \in \mathcal{X}$, let $I_X(x) = [L_X(x), U_X(x))$ be an interval corresponding to the target random variable X taking values in $\mathcal{X}$. Suppose that lower and upper endpoints $L_X(x)$ and $U_X(x)$ have the following p_Y-ary representation and p_Y-ary co-representations:*

$$L_X(x) = 0.a_1a_2\cdots, \quad \overline{L_X(x)} = 0.\bar{a}_1\bar{a}_2\cdots,$$
$$U_X(x) = 0.b_1b_2\cdots.$$

For each $x \in \mathcal{X}$, there exists an integer $t = t(x)$ such that representations of $L_X(x)$ and $U_X(x)$ have first different values at the t-th place at their p_Y-ary representations. Then, we have

$$p_X(x) = p_Y(a^{t-1})\Bigg[d_Y(a_t, b_t|a_{t-1}) + \sum_{k\geq t+1}\left\{p_Y(a_t^{k-1})c_Y(\bar{a}_k|a_{k-1}) + p_Y(b_t^{k-1})c_Y(b_k|b_{k-1})\right\}\Bigg], \tag{5}$$

where

$$d_Y(a_t, b_t|a_{t-1}) \triangleq \sum_{a_t<a<b_t} p_Y(a|a_{t-1})$$

and $d_Y(a_t, b_t|a_{t-1}) = 0$ when $b_t = a_t + 1$. The above expression leads to the following description of $I_X(x)$ with the disjoint sum of intervals corresponding to the target random sequences in the interval algorithm:

$$I_X(x) = \sum_{a_t<y<b_t} I_Y(a^{t-1}y) + \sum_{k\geq t+1}\left\{\sum_{y>a_k} I_Y(a^{k-1}y) + \sum_{y<b_k} I_Y(b^{k-1}y)\right\}. \tag{6}$$

It can be seen from the above presentation that the interval $\sum_{a_t<y<b_t} I_Y(a^{t-1}y)$ is in the middle of the interval $I_X(x)$ and that the sequence of intervals $\{\ \sum_{y>a_{k+1}} I_Y(a^ky)\}_{k\geq t}$ entirely covers the lower part of the interval $I_X(x)$. Those intervals are called *downward sequences* in Han and Hoshi [3]. We also know that the sequence of intervals $\{\sum_{y<b_k} I_Y(b^{k-1}y)\ \}_{k\geq t+1}$ in the third term in the right member of the above equation entirely covers the upper part of $I_X(x)$. This sequence of the intervals are called *upward sequence* in Han and Hoshi [3]. The result of Theorem can be regarded as giving an explicit form of upward/downward sequences of intervals in the interval algorithm. Those sequences of intervals is shown in Fig. 1.

As a corollary of this theorem we can obtain a result, which is quite useful for the performance algorithm of the interval algorithm. To describe this result we define some quantities: For each $a \in \{1, 2, \cdots, M-1\}$, let $\{l_{k,a}\}_{k\geq 1}$ be a sequence of positive integers satisfying

$$t - 1 \leq l_{1,a} < l_{2,a} < \cdots < l_{i,a} < l_{i+1,a} < \cdots.$$

Similarly, for each $b \in \{0, 1, \cdots, M-2\}$, let $\left\{\tilde{l}_{k,b}\right\}_{k\geq 1}$ be a sequence of positive integers satisfying

$$t \leq \tilde{l}_{1,b} < \tilde{l}_{2,b} < \cdots < \tilde{l}_{i,b} < \tilde{l}_{i+1,b} < \cdots.$$

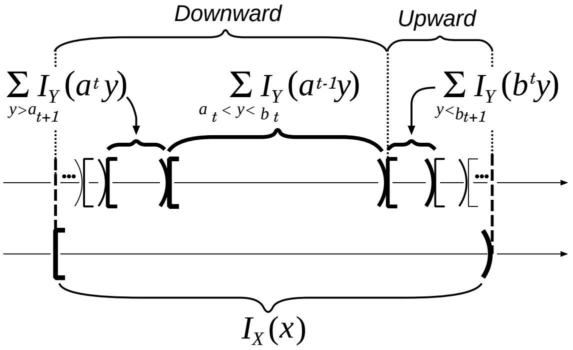
Downward
Upward
$\sum_{y>a_{t+1}} I_Y(a^t y)$
$\sum_{a_t<y<b_t} I_Y(a^{t-1}y)$
$\sum_{y<b_{t+1}} I_Y(b^t y)$
$I_X(x)$

Figure 1: Upward and downward sequences of intervals.

The two families of sequences

$$\{l_{k,a}\}_{k\geq 1, 1\leq a\leq M-1} \text{ and } \left\{\tilde{l}_{k,b}\right\}_{k\geq 1, 0\leq b\leq M-2}$$

are uniquely determined by the representation (5) of interval algorithm in Theorem 1. Details are found in [4]. The following is a corollary of Theorem 1.

Corollary 1 *For each $x \in \mathcal{X}$, we have*

$$p_X(x) = p_Y(a^{t(x)-1})$$
$$\times \sum_{k\geq 1}\left[\sum_{a=1}^{M-1} p_Y\left(a_t^{l_{k,a}+1}\middle| a_{t-1}\right) + \sum_{b=0}^{M-2} p_Y\left(b_t^{\tilde{l}_{k,b}+1}\middle| a_{t-1}\right)\right],$$

where if $l_{1,a} = t-1$, then $p_Y\left(a_t^{l_{1,a}+1}\middle| a_{t-1}\right) = p_Y(a|a_{t-1})$.

4. Performance Analysis of the Interval Algorithm

In this section we present a rigorous performance analysis of the interval algorithm using the expression of the interval algorithm we gave in the previous section. Set

$$\eta_0(a, x|a_{t-1}) \overset{\triangle}{=} \sum_{k\geq 1} p_Y\left(a_t^{l_{k,a}+1}\middle| a_{t-1}\right), \tag{7}$$

$$\eta_1(b, x|a_{t-1}) \overset{\triangle}{=} \sum_{k\geq 1} p_Y\left(b_t^{\tilde{l}_{k,b}+1}\middle| a_{t-1}\right). \tag{8}$$

Define two probability distributions on positive integers by

$$p_Y^{(0)}(\cdot|a, x, a_{t-1}) \overset{\triangle}{=} \left\{\frac{p_Y\left(a_t^{l_{k,a}+1}\middle| a_{t-1}\right)}{\eta_0(a, x|a_{t-1})}\right\}_{k=1,2,\cdots},$$

$$p_Y^{(1)}(\cdot|b, x, a_{t-1}) \overset{\triangle}{=} \left\{\frac{p_Y\left(b_t^{\tilde{l}_{k,b}+1}\middle| a_{t-1}\right)}{\eta_1(b, x|a_{t-1})}\right\}_{k=1,2,\cdots}.$$

Let $p_{\max} \overset{\triangle}{=} \max_{(i,j)\in\mathcal{Y}^2} P_{ij}$. Define the geometrical distribution p^* with parameter $p_{\max}$ by

$$p^* \overset{\triangle}{=} \left\{{p_{\max}}^{k-1}(1-p_{\max})\right\}_{k=1,2,\cdots}.$$

For each $a \in \mathcal{Y}$, let $Y_2(a)$ be a random variable having the distribution $\{\Pr\{Y_2 = y|Y_1 = a\}\}_{y\in\mathcal{Y}}$. The entropy rate of $\{Y_t\}_{t=1}^{\infty}$ is given by

$$H(Y_2|Y_1) = \sum_{a=0}^{M-1} p_Y(a)H(Y_2(a)).$$

We set

$$H_{\max}(Y_2(\cdot)) \overset{\triangle}{=} \max_{a\in\mathcal{Y}} H(Y_2(a)),$$
$$H_{\min}(Y_2(\cdot)) \overset{\triangle}{=} \min_{a\in\mathcal{Y}} H(Y_2(a)).$$

The following is our main result.

Theorem 2

$$\frac{H(X)}{H_{\max}(Y_2(\cdot))} \leq \bar{L} \leq \frac{H(X)}{H_{\min}(Y_2(\cdot))} + \frac{\log 2(M-1)}{H_{\min}(Y_2(\cdot))}$$
$$+\frac{h(p_{\max})}{H_{\min}(Y_2(\cdot))(1-p_{\max})} - \frac{\Delta}{H_{\min}(Y_2(\cdot))}, \tag{9}$$

where Δ is a nonnegative number defined by

$$\Delta \overset{\triangle}{=} \sum_{x=0}^{N-1} p_Y(a^{t(x)-1})$$
$$\times\left\{\sum_{a=1}^{M-1} \eta_0(a, x|a_{t-1}) D(p_Y^{(0)}(\cdot|a, x, a_{t-1}) \parallel p^*)\right.$$
$$\left.+\sum_{b=0}^{M-2} \eta_1(b, x|a_{t-1}) D(p_Y^{(1)}(\cdot|b, x, a_{t-1}) \parallel p^*)\right\}.$$

By letting $\Delta = 0$ in (9), we obtain the upper bound of $\bar{L}$ derived by Han and Hoshi [3]. Hence our upper bound improves their one. The quantity Δ indicates a lower bound of the deviation of the upper bound of $\bar{L}$ obtained by Han and Hoshi [3] from the true value of $\bar{L}$. This quantity is characterized with the p_Y-ary representation and the p_Y-ary co-representation of the endpoints of the intervals corresponding to the target random numbers.

References

[1] P. Elias, "The efficient construction of an unbiased random sequences," *Ann. Math. Statist.*, vol. 43, pp. 865-870, 1972.

[2] D. Knuth and A. Yao, "The complexity of nonuniform random number generation," *Algorithm and Complexity, New Directions and Results,* pp. 357-428, ed. by J. F. Traub, Academic Press, New York, 1976.

[3] T. S. Han and M. Hoshi, "Interval algorithm for random number generation," *IEEE Trans. Inform. Theory*, vol. 43, pp. 599-611, March 1997.

[4] Y. Oohama, "Performance analysis of the interval algorithm for random number generation based on number systems," *IEEE Trans. Inform. Theory*, vol. 57, pp. 1177-1185, March 2011.