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

Random Number Generation Using Outputs from Multiple Beta Encoders

Koji Itaya† and Yutaka Jitsumatsu†

†Dept of Informatics
744 Motooka, Nishi-ku, Fukuoka 819-0395, Japan
Email: itaya@me.kyushu-u.ac.jp, jitumatu@inf.kyushu-u.ac.jp

Abstract—Beta encoder is an analog-to-digital converter which is robust to the fluctuation of the threshold voltage in a quantizer. Such a beta encoder is considered as a good candidate for random number generators (RNGs). In order to use a beta encoder as a RNG, strong correlation between consecutive bits must be eliminated. In this paper, the exclusive-or (EXOR) of outputs from multiple beta encoders is used as a random number. We investigated the statistical property of such a random number.

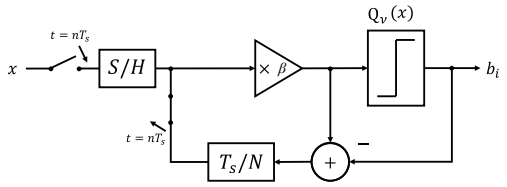


Figure 1: A block diagram of a cyclic-type β encoder

1. Introduction

Pseudo-random number generation is one of the most promising application of chaotic phenomenon observed in electronic circuits. There have been many researches on random number generator (RNG) using chaotic dynamics. Among them, RNGs using discrete-time chaotic dynamics with piecewise linear (PL) maps have attract much attention. Stojanovski and Kocarev [1] proposed to use a PL map with two slopes $1 < k_1 < 2$ and $1 < k_2 < 2$. Using the same PL map as in [1] but with $k_1 = k_2 (= k)$, Addabbo et al. presented an interesting approach in which the amplification factor k and a threshold are controlled by utilizing the observed statistics of the output binary codes [2]. Such a PL map with a slope $1 < k < 2$ is also used in β encoders that is a kind of analog-to-digital (A/D) converters, where the slope is denoted by β rather than k. In this paper, we consider a random number generation using exclusive or (EXOR) of multiple β encoders. The benefit of the proposed method over the existing ones [1][2] is that the proposed method is simple.

A β encoder is an A/D converter, proposed by Daubechies et al. in 2002 [3]. A β encoder aims to obtain β expansion coefficients of input value x, where β expansion of a real number $x \in (0, \frac{1}{\beta-1}]$ is defined by $x = a_1/\beta + a_2/\beta^2 + a_3/\beta^3 + \ldots$, where $a_i \in \{0, 1\}$ are the expansion coefficients and β is a fixed number in (1,2). A β expansion reduced to binary expansion if $\beta = 2$. The most important property of β encoder is its robustness to the fluctuation of the threshold voltage value in the quantizer. Such a property enables us to use coarse precision capacitances, and low gain operational amplifiers [3]. Then, we can design a β encoder extremely easily compared with other an A/D converter, and realize the miniaturization of a circuit area.

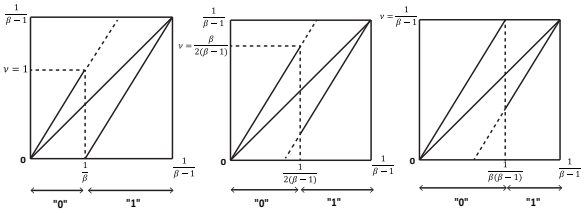
If we let a β encoder output a large number of bits, such as ten thousand bits for one sample, then its bit sequence is considered a random number sequence. We observed an attractor in the hardware circuit [5]. We consider this attractor as a replacement for random physical phenomenon in the physical RNG. Thus we treat the output of a β encoder as random number. However, a sequence of outputs of a β encoder has a strong correlation between adjacent outputs. Therefore we need to make it closer to i.i.d. sequence by performing some post-processing.

In this paper, we consider a sequence of EXORs of plural outputs from β encoders as random number sequence [6]. We performed a computer simulation, and evaluate the statistical properties of the generated random number sequences. A strong correlation between adjacent bits was highly suppressed by using multiple β encoders.

2. Pulse Code Modulation and β encoder

Pulse Code Modulation (PCM) is one of the standard analog-to-digital (A/D) conversion methods, which is based on binary expansion; the input analog value is converted into its binary expansion and then the binary expansion is expressed by a pulse train of its corresponding digital code. PCM consists of an amplifier that doubles the voltage accurately, a comparator that compares the voltage with the threshold value $1/2$, and a subtractor circuit that reduces the voltage by a reference voltage 1. However, if the threshold in the comparator fluctuates a little from the value $1/2$, then the output diverges. This observation suggests that we can not convert correctly.

A β encoder is an A/D converter based on β-expansion, consisting of an amplifier with an amplification factor β and a comparator with a threshold ν. A circuit diagram of cyclic β encoder is shown in Fig. 1. In a β encoder, an ana-



(a) greedy map (b) cautious map (c) lazy map

Figure 2: β-expansion map

log input value is converted into its corresponding β-ary expansion with finite precision. Let the output binary sequence obtained by a β encoder be $\{a_i\}_{i=1}^{\infty}$, and initial input value be $x = x_0 \in [0, \frac{1}{\beta-1})$, then we have

$$a_i = Q_{[\nu]}(\beta x_{i-1}), \quad i \geq 1, \tag{1}$$
$$x_i = \beta x_{i-1} - a_i, \quad i \geq 1, \quad x_0 = x, \tag{2}$$

where $Q_{[\nu]}(x)$ is a comparator, defined by

$$Q_{[\nu]}(x) = \begin{cases} 0 & 0 \leq x < \nu/\beta, \\ 1 & \nu/\beta \leq x < 1/(\beta-1). \end{cases}$$

The initial value x and $\{a_i\}_{i=1}^{\infty}$ satisfy the following relation:

$$x = \sum_{i=1}^{\infty} a_i \beta^{-i}, \tag{3}$$

where $1 < \beta < 2$ and $1 \leq \nu \leq \frac{1}{\beta-1}$. A β-expansion map is shown in Fig. 2. β-expansion map is called greedy, cautious, and lazy maps, if $\nu = 1$, $\nu = \frac{\beta}{2(\beta-1)}$, and $\nu = \frac{1}{\beta-1}$, respectively.

Daubechies et al.'s flaky quantizer: Daubechies et al. have proposed a model of quantizers having fluctuated threshold values, called a flaky quantizer [4]. A flaky quantizer is characterized by two threshold values, ν_0 and ν_1. If the voltage is less than ν_0, the quantizer outputs 0, if it is greater than ν_1, the quantizer outputs 1, and if it is between ν_0 and ν_1, we do not know the quantizer outputs 0 or 1. The output of a β encoder with flaky quantizer is given by

$$a_i = Q^{\mathrm{f}}_{[\nu_0,\nu_1]}(\beta x_{i-1}), \quad i \geq 1, \tag{4}$$
$$x_i = \beta x_{i-1} - a_i, \tag{5}$$

where $Q^{\mathrm{f}}_{[\nu_0,\nu_1]}(x)$ is flaky quantizer defined by

$$Q^{\mathrm{f}}_{[\nu_0,\nu_1]}(x) = \begin{cases} 0 & x < \nu_0, \\ 1 & x > \nu_1, \\ 0 \text{ or } 1 & \nu_0 \leq x \leq \nu_1. \end{cases}$$

This $Q^{\mathrm{f}}_{[\nu_0,\nu_1]}$ is a model of a quantizer that outputs on incorrect judgment near the threshold. In the computer simulation in Section 4, we let $Q^{\mathrm{f}}_{[\nu_0,\nu_1]}(x)$ to take 0 or 1 with equal probability if $\nu_0 \leq \nu \leq \nu_1$. We define the map from x_i to x_{i+1} as $C^{\mathrm{f}}_{\beta,[\nu_0,\nu_1]}(x)$. Namely, we define (See Fig. 3.)

$$C^{\mathrm{f}}_{\beta,[\nu_0,\nu_1]}(x) = \beta x - Q^{\mathrm{f}}_{[\nu_0,\nu_1]}(\beta x). \tag{6}$$

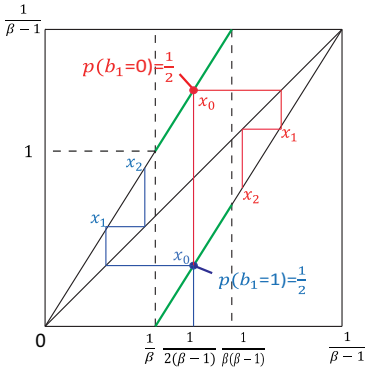


Figure 3: A β-expansion map with flaky quantizer

If the parameters ν_0, and ν_1 satisfy $1 \leq \nu_0 \leq \nu_1 \leq \frac{1}{\beta-1}$ and if the initial value satisfies $0 < x_0 < \frac{1}{\beta-1}$, then the orbit x_1, x_2, x_3, ... generated by $x_i = C^{\mathrm{f}}_{\beta,[\nu_0,\nu_1]}(x_{i-1})$ does not diverge.

3. The proposed method

A β encoders can be realized in a very small CMOS circuit, therefore it is possible to implement multiple β encoders into one chip. Based on this fact, Hirata et al. have proposed to use EXOR of the outputs from multiple β encoders to generate a sequence of random binary numbers [6]. In this paper, we evaluate the performance of Hirata et al.'s method by using Daubechies's flaky quantizers. We introduce the simulation method below.

Fixed threshold model: Firstly, we use quantizers with fixed thresholds to analyze Hirata et al.'s method. We assume that $K(\geq 1)$ β encoders with fixed thresholds are used. Once an analog signal is sampled, L bits of β expansion coefficients for this sample are obtained. Each of outputs of β encoders are distinguished by adding a superscript $^{(k)}$, such as $a_i^{(k)}$. An EXOR operation is performed among the outputs of β encoders of from 1 to K, which is defined as $b_i^{(K)}$, i.e.,

$$b_i^{(K)} = a_i^{(1)} \oplus a_i^{(2)} \oplus \cdots \oplus a_i^{(K)}, \quad i = 1, 2, \ldots L. \tag{7}$$

Parameters for β encoders are set as follows: The β value is chosen from 1.7, 1.8 and 1.9. The threshold is chosen from three-values, greedy, cautious, and lazy. Initial value is randomly selected from $[0, \frac{1}{\beta-1}]$ with uniform distribution. The number of bits is $L = 10,000$.

Flaky quantizer model: Secondly, we use Daubechies's flaky quantizers to analyze Hirata et al.'s method. Each of outputs of β encoders are denoted by $\overline{a}_i^{(k)}$. EXOR operation is performed among the outputs of β encoders from 1 to K, which is defined as $\overline{b}_i^{(K)}$, i.e.,

$$\overline{b}_i^{(K)} = \overline{a}_i^{(1)} \oplus \overline{a}_i^{(2)} \oplus \cdots \oplus \overline{a}_i^{(K)}, \quad i = 1, 2, \ldots, L. \tag{8}$$

The initial value $x_0^{(k)}$ is set to be $(\nu_0 + \nu_1)/2\beta$ for all $k = 1, \ldots, K$. The reason why we choose this number as the

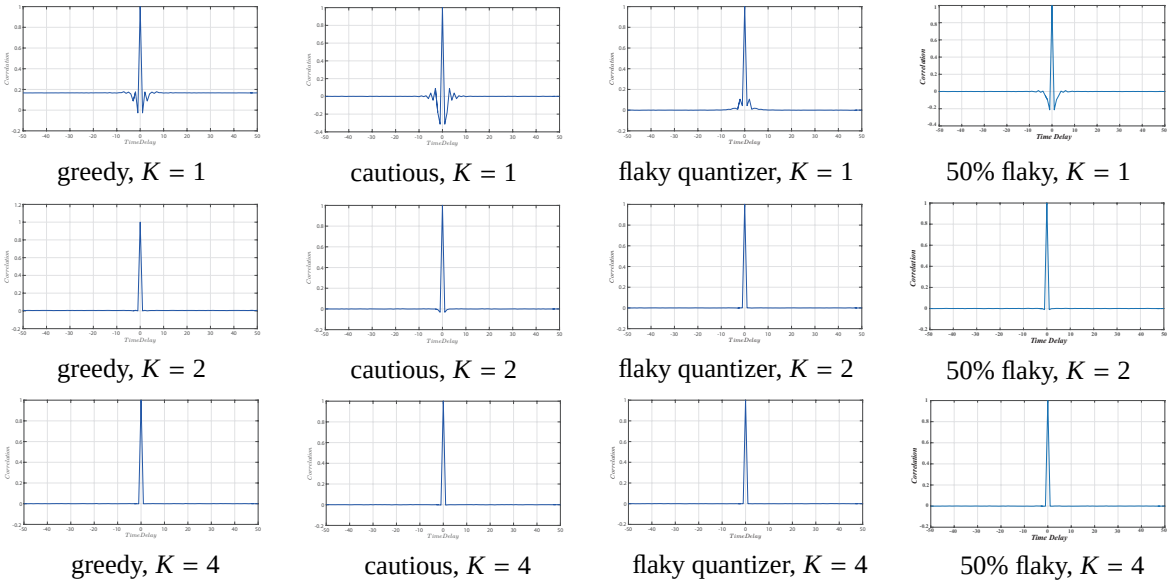


Figure 4: Autocorrelation function of $b_i^{(K)}$ for $\beta = 1.7$ and $L = 10,000$.

initial value is as follows: In a hardware β encoder, the common mode voltage is one of the easiest voltages to be employed, which is modeled as $(\nu_0 + \nu_1)/2\beta$. If the threshold of the quantizer in fixed, and if we start with the same initial value $x_0^{(k)}$, then the orbits $\{x_i^{(k)}\}$ should be the same for all of $k = 1, \ldots, K$. However, we employ the flaky quantizer here, so that the orbits $\{x_i^{(k)}\}$ for each k are different. Therefore, we assume the same initial value for all k.

4. Experiment

We consider the two analytical models i.e., fixed threshold and flaky quantizer models, on the random number generation method using EXOR of outputs of plural β encoders. The quality of the generated random number is evaluated by the following quantities: autocorrelation function, distribution of the sum of $b_i^{(K)}$, occurrence frequency of sequences of block length $N = 3, \ldots, 6$, and periodicity.

4.1. Autocorrelation function

Autocorrelation function of a random number sequence $b_i^{(K)}$, $i = 0, 1, \ldots, L-1$, is defined by

$$R^{(K)}(\ell) = \frac{1}{L} \sum_{i=0}^{L-\ell-1} b_i^{(K)} b_{i+\ell}^{(K)}. \tag{9}$$

Autocorrelation function of $\overline{b}_i^{(K)}$ is determined similarly and denoted by $\overline{R}^{(K)}(\ell)$. The number of β encoders is set to be $K = 1, 2, 4$ in both models. Furthermore, we performed 300 independent trials in each simulations. The autocorrelation function for $\beta = 1.7$ is shown in Fig. 4. In this figure, "greedy" and "cautious" correspond to the fixed threshold model and others correspond to the flaky quantizer model. The "50% flaky" means that the size of the range $[\nu_0, \nu_1]$ is 50% of the full range $[1, 1/(\beta - 1)]$, while "flaky quantizer" menas $[\nu_0, \nu_1] = [1, 1/(\beta - 1)]$. Autocorrelation functions for the lazy map are the almost the same as that of the greedy map and thus omitted here.

Fig. 4 shows that the autocorrelation values for $K = 1$ have strong correlations for the fixed threshold model. The autocorrelation function is close to the delta function if $K = 4$ for the fixed threshold model and if $K \geq 2$ for the flaky quantizer model.

Interestingly, we found that the autocorrelation function takes a positive value at $l = 1, -1$ for $\beta = 1.7$, but takes a negative value at $l = 1, -1$ for $\beta = 1.8$ and 1.9 $K = 1$ for the fixed threshold model. If we employ the fixed threshold model, the autocorrelation function at $l = \pm 1$ must take a negative value for any threshold value. However, the hardware experiment by Tanaka et al. [7] reported the autocorrelation value takes a positive value at $l = \pm 1$. Namely, the fixed threshold model does not match the result of experiment by Tanaka et al. Using the flaky quantizer model, we can make $\overline{R}^{(K)}(\ell)$ for $K = 1$ and $l = \pm 1$ to be negative. Hence, we consider the flaky quantizer model matches the hardware experiment more than the fixed threshold model.

4.2. Distribution of the sum of $b_i^{(K)} (i = 1, \ldots, L)$

The sum of $b_i^{(K)}$ from $i = 1$ to L is evaluated for both fixed and flaky quantizer models. For an i.i.d. binary sequence $c_1, c_2, \cdots$, the central-limit theorem states that $Z_L = L^{-1/2} \sum_{i=1}^{L} c_i$, approaches to a normal distribution as L goes to infinity. We expect the distribution of the sum of $b_i^{(K)}$ is close to the normal distribution. We use the variational distance as an approximate measure. Let two distributions on a finite set $\mathcal{X}$ be $P = (p_1, p_2, \ldots, p_{|\mathcal{X}|})$ and $Q = (q_1, q_2, \ldots, q_{|\mathcal{X}|})$. The variational distance between P and Q is defined by $d(P, Q) = \sum_{i=1}^{|\mathcal{X}|} |p_i - q_i|$. The variational

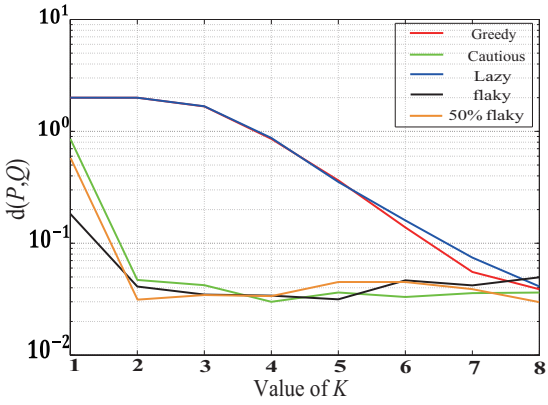


Figure 5: Variational distance between $\frac{1}{\sqrt{L}}\sum_{i=1}^{L} b_i^{(K)}$ and a normal distribution for $\beta = 1.7$ and $L = 120,000$.

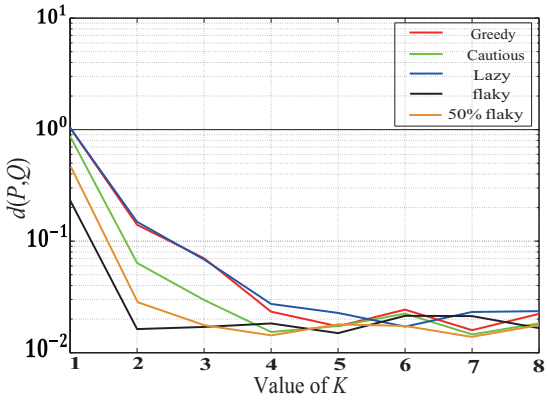


Figure 6: Variational distance between the empirical distribution of the bit pattern and the uniform distribution $\beta = 1.7$, $N = 6$, and $L = 10,000$

distance between the sum of $b_i^{(K)}$ and normal distribution is shown in Fig. 5. The variational distance was improved significantly at maximum value $K = 8$ in fixed threshold model, and $K = 2$ in flaky quantizer model. Fig. 5 shows that $K = 8$ is needed for greedy or lazy β expansions to achieve the same variational distance as flaky quantizers. The variational distance for cautious β expansions is as good as flaky quantizer model.

4.3. Occurrence frequency of bit patterns for short block length

We evaluate the number of occurrence of bit patterns such as $(0,0,\ldots,0)$, $(0,0,\ldots,1)$,...,$(1,1,\ldots,1)$ for block length of $N = 3,4,5$ and 6.The number of bits is $L = 120,000$. The variational distance between the empirical distribution of the bit patterns and uniform distribution for $N = 6$ and $\beta = 1.7$ is shown in Fig. 6. The variational was improved significantly at maximum value $K = 8$ in fixed threshold model, and $K = 2$ in flaky quantizer model. Fig. 6 shows that the quality of random numbers for cautious map is worse than the flaky quantizer. It is obversved that the performance of 50% flaky quantizer is between those of the fixed threshold with cautious map and the flaky quantizer.

4.4. Periodicity

We examined periodicity of the generated random numbers. We define $p \geq 1$ as the periodicity of an orbit $\{x_n\}_{n=0}^{\infty}$ if we find $x_n = x_{n+p}$ for some n. When we use multiple β encoders, we define p as the periodicity if we find $(x_n^{(1)}, x_n^{(2)}, \ldots, x_n^{(K)}) = (x_{n+p}^{(1)}, x_{n+p}^{(2)}, \ldots, x_{n+p}^{(K)})$ for some n. As far as we examined to length of sequence $L = 2^{20}$ we could not find such an example, and verified that the period of the generated bits is greater than 2^{20}.

5. Conclusion

In this paper, we have evaluated performance of Hirata et al.'s method by introducing Daubechies et al's flaky quantizer. In the fixed threshold model, eight β encoders are necessary to make the quality of generated sequence close to that of i.i.d. sequences. On the other hand, in the flaky quantizer model, two β encoders were enough. These results show that the number of β-encoders required to attain a sufficient quality of the random number after taking EXOR of the plural of β encoders is not so large as previously expected by Hirata et al.'s computer simulation employing the fixed threshold model.

References

[1] T. Addabbo et al., "Efficient Post-Processing Module for a Chaos-Based Random Bit Generator," *in Proc. IEEE Int. Conf. on Elec., Circ., and Syst. (ICECS)*, pp. 1224-1227, 2006.

[2] T. Stojanovski, P. Johnny, and L. Kocarev, "Chaos-Based Random Number Generators. Part II: Practical Realization," *IEEE Trans on Circ. and Syst.-I*, vol. 48, no. 3, pp. 382-385, 2001.

[3] I. Daubechies et al., "Beta Expansions: A New Approach to Digitally Corrected A/D Conversion," *Proc. IEEE Int. Symp. Circ. Syst. 2002 (ISCAS2002)*, vol. 2, pp. 784-787, 2002.

[4] I. Daubechies et al., "A/D Conversion With Imperfect Quantizers," *IEEE Trans. Inform. Theory,*, vol.52, no.3, pp.874–885, 2006.

[5] T. Kohda, Y. Horio, and K. Aihara, "β-Expansion Attractors Observed in A/D Converters," *Chaos: An Interdisciplinary J. of Nonlinear Science*, vol. 22, 047512, 2012.

[6] Y. Hirata et al., "Pseudo-Random number generator using β-expansion in A/D converters," *The 30th Symp. on Crypto. and Inform. Security 2013 (SCIS 2013)*, Jan. 2013.

[7] S. Tanaka, A. Hyogo, and T. Matsuura, "Physical Random Number Generator using A/D Converter based on Beta-exapansion," *IEEJ Tech. Meeting on Electronic Circ., ECT-15-036*, pp. 29-34, Mar. 2015.