2015 International Symposium on Nonlinear Theory and its Applications
NOLTA2015, Kowloon, Hong Kong, China, December 1-4, 2015

Performance Evaluation of a Random Number Generation Using a Beta Encoder

Yeelai Shu, Yutaka Jitsumatsu, and Kohei Oda

Department of Informatics, Kyushu University
744 Motooka, Nishi-ku, Fukuoka, 819-0395, Japan
Email: shu@me.inf.kyushu-u.ac.jp, jitumatu@inf.kyushu-u.ac.jp, oda@me.inf.kyushu-u.ac.jp

Abstract—A β encoder is an analog-to-digital (A/D) converter, that outputs a truncated sequence of β expansion of an input value x. We recently proposed a method for generating sequences of random numbers using a hardware β encoder followed by a β-ary to binary converter. This paper gives the performance analysis of the random number generation in terms of the variational distance between the target distribution and the distribution of the output sequence and the expected length of the input sequence per one output symbol.

1. Introduction

There are two major schemes for Analog-to-Digital (A/D) converters: pulse code modulation (PCM) and $\Delta\Sigma$ modulation. In case of PCM, the continuous-time signal is sampled at a rate higher than Nyquist rate. The samples are, then, quantized to the truncated binary expansions of the samples. The quantization error is upper bounded by $C \cdot 2^{-N}$ with some constant C, where N is the length of the binary expansion. However, this upper-bound cannot be guaranteed if N becomes very large. One of the reasons is that the PCM method is sensitive to the variation in the comparator voltage offset. Once a comparator makes an erroneous decision at some bit, the error cannot be recovered by the following bits. On the other hand, $\Delta\Sigma$ modulations are robust to fluctuations of threshold values in their quantizers. However, they require a very high oversampling rate. This implies that $\Sigma\Delta$ modulation can only be used in narrow-bandwidth applications. Moreover, the quantization error of $\Sigma\Delta$ modulation decreases in inverse proportion to the number of bits in contrast to the exponential accuracy of the PCM.

Daubechies et.al [1] proposed a new A/D converter that is based on the β expansion of a real number and, therefore, is called the β encoder. The β expansion of a real number $x \in [0, 1/(\beta-1)]$ with $\beta \in (1, 2)$ is defined by

$$x = \sum_{i=1}^{\infty} a_i \beta^{-i}, \quad a_i \in \{0, 1\}. \tag{1}$$

This research was supported in part by the Aihara Project, the FIRST program from JSPS, initiated by CSTP and JSPS KAKENHI Grant Number 25820162.

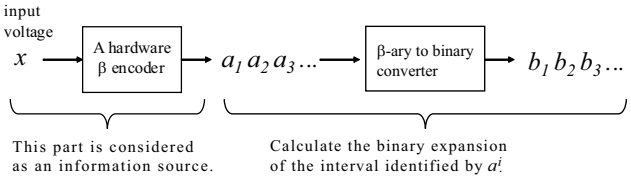

Figure 1: A block diagram of the proposed method.

For a fixed x, $a_1 a_2 \cdots$ are not unique. In fact, there are infinitely many ways to expand x. This implies that digital codes produced by a β encoder are redundant. Unlike PCM, an erroneous decision made by a β encoder can be recovered by the following bits. Thus, a β encoder is robust to fluctuation of threshold value of a quantizer. Such a β encoder does not need high-precision circuit elements and is implemented by an electronic circuit that achieves very small area consumption as well as low power consumption [2].

We observe chaos attractors in β converters [3]. This fact motivated Hirata et.al [4] to use a β encoder as a random number generator. However, outputs from a β encoder have strong correlations between successive bits. Such strong correlations should be eliminated. Then, Matsumura et.al [5] proposed another method for generating a sequence of random numbers using a β encoder. This method employs a β-ary to binary converter (See Fig. 1).

This paper provides performance analysis of the proposed method in terms of variational distance as well as the expected length of input sequence per an output symbol.

2. β encoder

The β expansion of a real number $x \in [0, 1/(\beta-1)]$ with $\beta \in (1, 2)$ is defined by (1). The set of coefficients $\{a_i\}$ in (1) are called cautious expansion if a_i is determined as follows:

Definition 1 *Cautious expansion with a threshold* $\nu \in (1, \frac{1}{\beta-1})$ *of a real number* $x \in [0, \frac{1}{\beta-1})$ *is defined recursively by*

$$a_{i+1} = Q_\nu(\beta x_i), \quad i = 0, 1, \ldots, \tag{2}$$

$$x_{i+1} = C_{\beta,\nu}(x_i), \tag{3}$$

where $C_{\beta,\nu}$ *is the cautious* β *map, defined by*

$$C_{\beta,\nu}(x) = \beta x - Q_\nu(\beta x). \tag{4}$$

The map $C_{\beta,\nu}(x)$ is called greedy if $\nu = 1$ and lazy if $\nu = 1/(\beta - 1)$.

Definition 2 *The (β, α)-transformation $T_{\beta,\alpha} : [0,1) \mapsto [0,1)$ is defined by [6]*

$$T_{\beta,\alpha}(x) = \beta x + \alpha \bmod 1,\ \beta \geq 1,\ 0 \leq \alpha \leq 1. \tag{5}$$

It can be known that we have $\varphi(C_{\beta,\nu}(\varphi^{-1}(x))) = T_{\beta,\alpha}(x)$, where $\varphi^{-1}(x) = x + \alpha/(\beta - 1)$. The most important property of the β map is that there is a unique absolutely continuous invariant probability measure [6].

Theorem 1 (Parry [6]) *An unnormalized invariant measure for $T_{\beta,\alpha}(x)$ is given as*

$$h(x) = \sum_{x < T^n_{\beta,\alpha}(1)} \beta^{-n} - \sum_{x < T^n_{\beta,\alpha}(0)} \beta^{-n}. \tag{6}$$

Remark 1 *Suppose that we ignore the first a^n and consider $a_{n+1}a_{n+2}a_{n+3}\cdots$. It should be noted that from this sequence we obtain $x_n = \sum_{i=n+1}^{\infty} a_i\beta^{-i}$. Theorem 1 implies that $\{x_n - \alpha/(\beta - 1)\}$ tends to follow Parry's absolutely continuous invariant density $h(x)$ for almost all initial values $x = x_0$.*

Daubechies et.al [1] pointed out that the value ν may differ from one application to the next and introduced a flaky version of an imperfect quantizer, defined by

$$Q^{\mathrm{f}}_{[\nu_0,\nu_1]}(x) = \begin{cases} 0, & \text{if } x \leq \nu_0, \\ 1, & \text{if } x \geq \nu_1, \\ 0 \text{ or } 1, & \text{if } x \in (\nu_0, \nu_1). \end{cases} \tag{7}$$

This notation means that for $x \in (\nu_0, \nu_1)$ we do not know which value in $\{0, 1\}$ the flaky quantizer will assign.

Daubechies et. al [1] gave the following theorem that guarantees the exponential accuracy of the quantization error made by a β encoder with a flaky quantizer.

Theorem 2 (Daubechies et.al [1]) *For $\beta \in (1,2)$, $x \in [0,1)$, $1 < \nu_0 < \nu_1 < 1/(\beta - 1)$, define*

$$b^{\mathrm{f}}_{i+1} = Q^{\mathrm{f}}_{[\nu_0,\nu_1]}(\beta x^{\mathrm{f}}_i), \quad i = 0, 1, 2, \cdots, \tag{8}$$

$$x^{\mathrm{f}}_{i+1} = \beta x^{\mathrm{f}}_{i+1} - Q^{\mathrm{f}}_{[\nu_0,\nu_1]}(\beta x^{\mathrm{f}}_i), \quad x^{\mathrm{f}}_0 = x \tag{9}$$

Then for all $N \in \mathbb{N}$,

$$0 \leq x - \sum_{i=1}^{N} b^{\mathrm{f}}_i \beta^{-i} \leq \nu_1 \beta^{-N}. \tag{10}$$

In what follows, we consider a scale-adjusted β expansion of $\tilde{x} = s(\beta - 1)x \in [0, s]$, where s is a scale parameter and $\beta \in (1,2)$. For simplicity, assume $s = 1$.

Definition 3 *The scale-adjusted β map of scale one, $S_{\beta,\nu} : [0,1) \mapsto [0,1)$ for $\nu \in [(\beta - 1), 1]$ is defined by*

$$S_{\beta,\nu}(x) = \beta x - (\beta - 1)Q_\nu(\beta x). \tag{11}$$

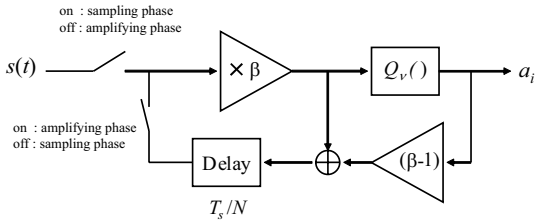

Figure 2: Scale-adjusted β-encoder with $s = 1$.

Let $\tilde{x} \in [0,1)$ be an input for the scale-adjusted β encoder. The output sequence for $\tilde{x}$ is (See Fig. 2)

$$a_{i+1} = Q_\nu(\beta x_i), \quad i = 0, 1, \ldots \tag{12}$$

$$x_{i+1} = S_{\beta,\nu}(x_i) \quad x_0 = \tilde{x}, . \tag{13}$$

Then, we have $\tilde{x} = (\beta - 1)\sum_{i=1}^{\infty} a_i\beta^{-i}$. As shown in Fig. 3, $x_n = S^n_{\beta,\nu}(x_0)$ does not diverge if the threshold value ν satisfies $\nu \in [\beta - 1, 1]$. Since the exact value ν in a circuit is not known, ν can be considered a random variable distributed in a range $[\nu_0, \nu_1]$. In this case, x_n does not diverge if $\nu_0 \geq \beta - 1$ and $\nu_1 \leq 1$. This property makes the β encoders robust to the fluctuations of the threshold.

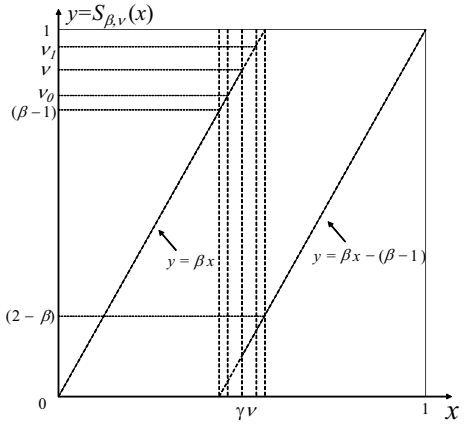

Figure 3: A map of the scale-adjusted β map with $s = 1$.

For almost all initial values $x_0 \in [0,1)$, x_n generated by Eq. (13) does not fall into periodic points but stays within a range. Attractors are observed in the dynamics of β encoders and are referred to as β expansion attractors [3]. Such an attractor can be considered as an information source. The connection between information sources and the chaotic dynamics is discussed in [7].

2.1. The proposed method

We recently proposed a method for converting a binary sequence generated from a β encoder to another binary sequence that is approximately regarded as independent and identically distributed (i.i.d.) random variables [5]. The proposed β-ary to binary converter should be implemented in a digital circuit. Therefore, we have developed a fixed-point arithmetic with limited precision for the interval al-

gorithm, which is similar to the methods discussed by Uyematsu and Li [8]. A real number $x \in [0,1)$ with unlimitted precision is rounded down to a fixed point number $\ell/2^w$, $\ell \in \{0,1,\ldots,2^w-1\}$, where w is called a word length.

[The β-ary to binary conversion algorithm [5]]

1. Let n be the number of output symbols we shall generate. Let $i = j = 1$, $k = 0$, $l' = 0$, $u' = 2^w - 1$, and $\gamma = \lfloor \frac{2^w}{\beta} \rfloor$, and $\lfloor x \rfloor$ denotes the smallest integer greater than or equal to x.

2. Read a_i. If $a_i = 0$, then update
$$u' = l' + \left\lfloor \frac{(u'-l')\cdot\gamma}{2^w} + \frac{1}{2} \right\rfloor \tag{14}$$
If $a_i = 1$, then update
$$l' = u' - \left\lfloor \frac{(u'-l')\cdot\gamma}{2^w} + \frac{1}{2} \right\rfloor \tag{15}$$

3. (a) If $\frac{1}{4} \le \frac{\ell'}{2^w} < \frac{1}{2}$ and $\frac{1}{2} \le \frac{u'}{2^w} < \frac{3}{4}$, then update $\ell' = 2\ell' - 2^{w-1}, u' = 2u' - 2^{w-1}$, and $k = k+1$.
   (b) If $\frac{u'}{2^w} < \frac{1}{2}$, then output $b_j b_{j+1} \cdots b_{j+k} = 01\cdots1$ and update $k = 0$, $\ell' = 2\ell'$, $u' = 2u'$, and $j = j+k+1$.
   (c) If $\frac{\ell'}{2^w} \ge \frac{1}{2}$, then output $b_j b_{j+1} \cdots b_{j+k} = 10\cdots0$ and update $k = 0$, $l' = 2l' - 2^w$, $u' = 2u' - 2^w$, and $j = j+k+1$.

4. If $j \ge n$, then let $m = i$ and quit. Otherwise, update $i = i+1$ and go back to Step 2.

Note that m is the number of input symbols required to generate n output symbols and that m depends on $\{a_i\}$. Because of the truncation operations in Eqs. (14) and (15), the distribution of the generated sequence is deviated from the target distribution. The effect of the word length w is left to be analyzed.

3. The Random Number Generation Problem in Information Theory

By the β-ary to binary converter, shown in Fig. 1, we try to generate a sequence of $b_1 b_2 \cdots$ which is regarded as an i.i.d. random process from an input sequence $a_1 a_2$ which is not an i.i.d. process. The problem of simulating a prescribed target distribution by repeating tosses of a coin with a given probability is known as *a random number generation problem* in information theory [10]. Knuth and Yao [9] have investigated the problem of random number generation for simulating an arbitrary target distribution by successive tosses of an unbiased coin.

Han and Hoshi [11] proposed a deterministic algorithm, called the interval algorithm, that generates target random sequences of fixed length from a prescribed information source by use of random coin sequences of variable length from a given information source. The interval algorithm is based on the successive refinement of partitions of the unit interval $[0,1)$. They gave a tight upper bound on the expected number of tosses:

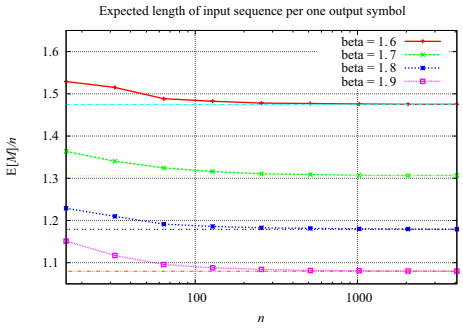

Figure 4: The expected length of the input sequence per one output symbol.

Theorem 3 (Han and Hoshi [11]) *Let $\mathcal{A}$ and $\mathcal{B}$ be finite sets. Let $\boldsymbol{p} = \{p(a)\}$ and $\boldsymbol{q} = \{q(b)\}$ be probability distributions on $\mathcal{A}$ and $\mathcal{B}$. Let $\mathrm{E}[M]$ be the expected number of tosses required to simulate an i.i.d. random sequence of length n subject to the distribution $\boldsymbol{q}$. Then, we have*
$$\frac{nH(\boldsymbol{q})}{H(\boldsymbol{p})} \le \mathrm{E}(M) \le \frac{nH(\boldsymbol{q})}{H(\boldsymbol{p})} + \frac{\log_2(2(|\mathcal{A}|-1))}{H(\boldsymbol{p})} + \frac{h(p_{\max})}{(1-p_{\max})H(\boldsymbol{p})}, \tag{16}$$
where $p_{\max} = \max_{a\in\mathcal{A}} p(a)$, $H(\boldsymbol{p}) = -\sum_{a\in\mathcal{A}} p(a)\log_2 p(a)$ is the entropy, and $h(p) = -p\log_2 p - (1-p)\log_2(1-p)$ is the binary entropy.

In the β-ary to binary conversion algorithm, the target distribution is $q(0) = q(1) = 1/2$ so that we have $H(\boldsymbol{q}) = 1$.

See [10] for a theoretical framework of random number generation in information theory, where asymptotic approximation problems are considered in which the target random numbers are generated approximately within an arbitrarily small torelance in terms of variational distance.

Definition 4 (Variational Distance) *Let $\boldsymbol{q} = \{q(b)\}$ and $\tilde{\boldsymbol{q}} = \{\tilde{q}(b)\}$ be probability distributions on a finite set $\mathcal{B}$. The variational distance between $\boldsymbol{q}$ and $\tilde{\boldsymbol{q}}$ is defined by*
$$d(\boldsymbol{q},\tilde{\boldsymbol{q}}) = \sum_{b\in\mathcal{B}} |q(b) - \tilde{q}(b)| \tag{17}$$

4. Numerical Results

The performance of the random number generation using β encoder and β-ary/binary converter is evaluated. In the proposed method, a hardware β encoder is used. However, in this study, β encoder is simulated by a computer program. Fig. 4 shows the expected length of input symbols per one output symbol. Simulation results shows that $E[M]/n$ approaches to the value $\frac{1}{\log_2\beta}$ from above. This result shows that the proposed method is efficient in terms of the conversion rate.

Fig. 5 shows the histograms of the generated output sequence $b_1 \cdots b_5$. In this simulation, $K = 32{,}000$ input signals, defined by $\tilde{x}^{(k)} = k/K$, $k = 0,1,\ldots,K-1$, are

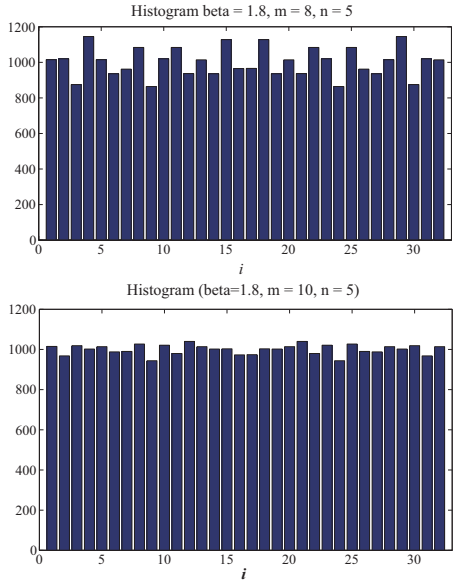

Figure 5: Histogram of the generated binary sequence $b_1 b_2 \cdots b_5$. The horizontal axis shows $i = \sum_{j=1}^{5} b_j 2^{5-j}$

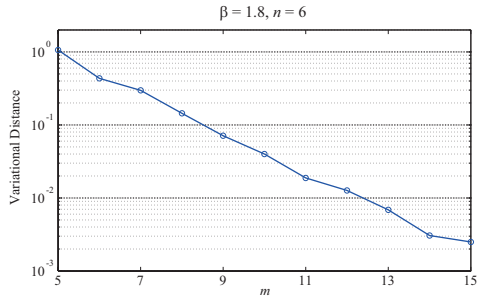

Figure 6: Variational distance between the uniform distribution and the distribution of the output sequence. Horizontal axis shows the length of the input sequence $a_1 \ldots a_m$.

used to generate $\boldsymbol{a}^{(k)} = a_1^{(k)} \cdots a_m^{(k)}$. Then, for each $\boldsymbol{a}^{(k)}$, β-ary/binary converter gives $b_1^{(k)} \cdots b_5^{(k)}$, where the length of output signals is fixed to $n = 5$. The lower graph is much closer to uniform distribution than the upper one. Figure 6 shows that the variational distance between the uniform distribution and the empirical distribution for $b_1^{(k)} \cdots b_n^{(k)}$ decreases exponentially as m increases.

We have so far assumed that the β value in a hardware β encoder is known to the β-ary/binary converter. However, it is one of the important properties of β encoders that the β value can fluctuate. It should be reasonable to assume that there is a mismatch between β used in a β-ary/binary converter, denoted by $\hat{\beta}$ and the true β. In Fig. 7 shows that the variational distance does not approaches to zero if $\beta \neq \hat{\beta}$ as m increases.

5. Conclusion

The performance of a recently proposed random number generation method using β encoder with β-ary/binary converter [5] is evaluated in term of the conversion rate and

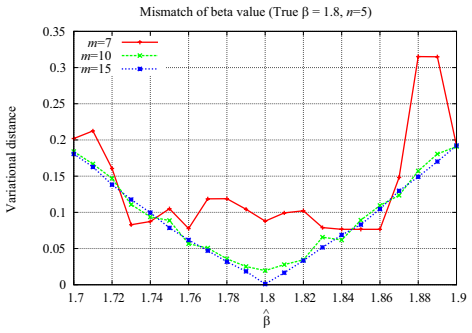

Figure 7: The effect of mismatch between β values used in β encoder and β-ary/binary converter

variational distance between uniform distribution and the distribution obtained by the proposed method. The conversion rate, i.e., the expected length of input sequence per one output symbol approaches to the value $1/\log_2 \beta$. We have verified that the variational distance decreases exponentially. Such results show the efficiency of the method [5]. The effect of short word length w is left to be analyzed.

References

[1] I. Daubechies, R.A. DeVore, C.S. Güntürk, and V. A. Vaishampayan, "A/D Conversion With Imperfect Quantizers," *IEEE Trans. Inform. Theory*, vol.52, no.3, March 2006.

[2] H. San et. al, "Non-binary Pipeline Analog-to-Digital Converters Based on β-Expansion," *IEICE Trans. Fundamentals*, vol.E96-A, no.2, pp. 415-421, Feb. 2013.

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

[4] Y. Hirata, Y. Jitsumatsu, T. Kohda, and K. Aihara, "Pseudo-Random Number Generator Using β-Expansion Attractors in A/D Converters," *Proc. of the 30th Sympo. on Cryptography and Information Security* , Jan. 2013 (in Japanese).

[5] K. Matsumura, T. Teraji, K. Oda, and Y. Jitsumatsu, "Random Number Generation Using β Encoder," *Proc. of the 32nd Sympo. on Cryptography and Information Security* , Jan. 2015 (in Japanese).

[6] W. Parry, "Representations for real numbers, " *Acta Math. Acad. Sci. Hung.* 15, 95-105, 1964.

[7] T. Kohda, "Information Sources Using Chaotic Dynamics," *Proc. IEEE*, vol.90, no.5, pp.641-661, 2002.

[8] T. Uyematsu and Y. Li, "Two Algorithms for Random Number Generation Implemented by Using Arithmetic of Limited Precision," *IEICE Trans. Fundam.*, vol.E86-A, no.10, pp.2542-2551, 2003.

[9] 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.

[10] T. S. Han, *Information-Spectrum Methods in Information Theory*, Springer, 2003.

[11] T. S. Han and M. Hoshi, "Interval Algorithm for Random Number Generation," *IEEE Trans. on Inform. Theory*, 43, pp.599-611, 1997.