Intermittency and number expansions for random interval maps

Zeegers, B.P.

CHAPTER 6

A Lochs Theorem for pseudo-random number generation with β-encoders

This chapter is joint work with Charlene Kalle and Evgeny Verbitskiy.

Abstract

The β-encoder is an analog circuit that converts an input signal $x \in [0, 1)$ into a finite bitstream $b_1, \ldots, b_m$ that corresponds to a representation of x in non-integer base $\beta \in (1, 2)$. In this chapter we study a question posed by Jitsumatsu and Matsumura on the number of output digits from the β-encoder that are necessary to correctly determine the first n base 2 digits of the original input x. We confirm the lower bound established by Jitsumatsu and Matsumura, we provide an upper bound and give two different limit results for this value, the last one of which is reminiscent of Lochs' Theorem.

§6.1 Introduction

Since the work [DDGV02] from 2002 by Daubechies et al. the advantages and disadvantages of the β-encoder as a replacement for the commonly used Pulse Code Modulation (PCM) in analog-to-digital (A/D) conversion have been considered. Given a real number $\beta \in (1,2)$, the scale-adjusted β-encoder converts an analog input signal $x = x_0 \in [0,1)$ into a bitstream $b_1, \ldots, b_k$ of specified length k by using a circuit consisting of an *amplifier* with amplification factor β, a *scale adjuster* with scaling factor $\beta - 1$, and a *quantiser*

$$Q_u(y) = \begin{cases} 0, & \text{if } y < u, \\ 1, & \text{if } y \geq u, \end{cases}$$

with threshold value $u \in [\beta - 1, 1]$. The bits b_n are produced iteratively by setting $x_n = \beta x_{n-1} - (\beta - 1)b_n$ and $b_n = Q_u(\beta x_{n-1})$. This algorithm is depicted in Figure 6.1 and is set up in such a way that it provides a *β-expansion* of the number $\frac{x}{\beta - 1}$, i.e. x can be represented as

$$x = (\beta - 1) \sum_{n=1}^{\infty} \frac{b_n}{\beta^n},$$

and thus finite truncations $b_1, \ldots, b_k$ of the sequence $(b_n)_{n \geq 1}$ give bitstreams that approximate x well. The PCM works similarly but with multiplication factor 2 and threshold value 1 (and no scale adjuster).

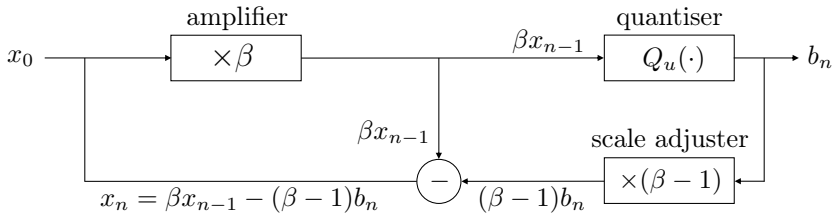

Figure 6.1: Iteration process of the scale-adjusted β-encoder.

Due to noise in the circuit the value of u fluctuates while running the iteration process. Since each number x has an essentially unique base 2 representation, PCM is not robust against these quantisation errors, see e.g. [DDGV06, G12]. It was proven in [EJK90, S03] that, contrary to binary expansions, for each $\beta \in (1,2)$ Lebesgue almost every x has uncountably many different β-expansions. The advantage of using a β-encoder over PCM for A/D-conversion thus lies in the fact that if the quantisation threshold u is chosen well inside the interval $[\beta - 1, 1]$, then the β-encoder can recover from a quantisation error and still produce good approximations of the original input signal x by shifting from one β-expansion of x to another. The robustness of the β-encoder in the A/D-conversion process has been studied in e.g. [DDGV06, JW09, KHTA12, KHA12, SKM+13, MIS+15].

In recent years the β-encoder was considered as a source for random number generation, see [JMKA13, SJO15, JM16, KJ16]. An issue with this application was that the successive bits in the output of a β-encoder are strongly correlated. Jitsumatsu and Matsumura proposed in [JM16] to remove this dependence between bits by adding an algorithm to the process that converts the output bits from the β-encoder into the base 2 digits of the number it represents. A natural question asked in [JM16] is the following: If we use $\boldsymbol{u} = (u_n)_{n\geq 1}$ to denote the consecutive threshold values u_n used at each time step of the approximation algorithm, what is the number $k(m, \boldsymbol{u}, x)$ of bits from the β-encoder that are necessary to obtain m base 2 digits of the number x via this process? In [JM16] the lower bound $k(m, \boldsymbol{u}, x) \geq \frac{m \log 2}{\log \beta}$ was found. The authors of [JM16] remarked that a theoretical analysis of the expected value of $k(m, \boldsymbol{u}, x)$ is relevant as an indication of the efficiency of the proposed pseudo-random number generator.

It is the purpose of this chapter to address the question posed in [JM16], which is reminiscent of the considerations of Lochs in [L64] and related settings from [BDK99, DF01] discussed in Subsection 5.1.1. Unfortunately these results as well as the results obtained in Chapter 5 do not immediately apply to the question from [JM16] due to the uncertainty in the threshold value u, even though as we will see below the iteration process of the β-encoder can be described with a random dynamical system. In particular, the results of Chapter 5, which are in the context of random dynamical systems, do not apply because fluctuations in u are assumed to be unknown. (This is discussed at the end of Subsection 5.1.2.) Indeed, in reality we do not know, given some output $b_1, \ldots, b_k$ of the β-encoder, which $u_1, \ldots, u_k$ resulted in this output. Nevertheless, in our first main result of this chapter we recover the lower bound from [JM16] and we obtain a statement on an upper bound for $k(m, \boldsymbol{u}, x)$. More precisely, we obtain the following results. Again λ denotes the one-dimensional Lebesgue measure.

Theorem 6.1.1. *Let $\beta \in (1, 2)$ and $\boldsymbol{u} = (u_n)_{n\geq 1} \in [\beta - 1, 1]^{\mathbb{N}}$. For all $x \in [0, 1)$ and all $m \in \mathbb{N}$ it holds that*

$$k(m, \boldsymbol{u}, x) \geq \frac{m \log 2}{\log \beta}. \tag{6.1}$$

Moreover, for each $\varepsilon \in (0, 1)$ there exists a constant $C(\varepsilon) > 0$ such that for all $m \in \mathbb{N}$

$$\lambda\Big(\Big\{x \in [0, 1) \,:\, k(m, \boldsymbol{u}, x) - \frac{m \log 2}{\log \beta} > C(\varepsilon)\Big\}\Big) < \varepsilon. \tag{6.2}$$

From these bounds we obtain the following corollary on the asymptotic behaviour of the sequences $(k(m, \boldsymbol{u}, x))_{m\geq 1}$.

Corollary 6.1.2. *For any real positive sequence $(a_m)_{m\in\mathbb{N}}$ with $\lim_{m\to\infty} a_m = \infty$, each $\boldsymbol{u} \in [\beta - 1, 1]^{\mathbb{N}}$ and each $\varepsilon > 0$ it holds that*

$$\lim_{m\to\infty} \lambda\Big(\Big\{x \in [0, 1) \,:\, \frac{1}{a_m}\Big|k(m, \boldsymbol{u}, x) - \frac{m \log 2}{\log \beta}\Big| > \varepsilon\Big\}\Big) = 0,$$

i.e. the sequence $\big(\frac{1}{a_m}\big(k(m, \boldsymbol{u}, x) - \frac{m \log 2}{\log \beta}\big)\big)_{m\geq 1}$ converges to 0 in λ-probability.

In particular, the above corollary has the following implications:
- Taking $a_m = \sqrt{m}$ for each m gives a Central Limit Theorem result where the limiting distribution has zero variance;
- Taking $a_m = m$ for each m we retrieve a limit statement in the spirit of (5.1), but with convergence in probability instead of almost surely.

By adjusting the setup from [DF01] to suit our purposes, we obtain the stronger result of almost sure convergence for the specific sequence $(a_m)_{m\geq 1}$ with $a_m = m$ for each m that is stated in the next theorem.

Theorem 6.1.3. *For each $\boldsymbol{u} \in [\beta - 1, 1]^{\mathbb{N}}$ it holds that*

$$\lim_{m\to\infty} \frac{k(m, \boldsymbol{u}, x)}{m} = \frac{\log 2}{\log \beta} \qquad \lambda\text{-a.e.}$$

More specifically, for typical x and large m one needs approximately $\frac{m \log 2}{\log \beta}$ output bits of the β-encoder to obtain m correct base 2 digits.

The remainder of this chapter is organised as follows. In the next section we introduce the necessary notation and preliminaries on binary and β-expansions. In the third section we prove our main results. We conclude with some final remarks. Here we discuss in particular what happens if not only the threshold value u but also the values of the amplification factor β or the scaling factor $\beta - 1$ fluctuate over time, a fact that has been observed for β-encoders and discussed in e.g. [DY06, W08, DGWY10].

§6.2 Preliminaries

If A is an interval in the real line, then we write ∂A for the set containing the two boundary points of A and we use A^- and A^+ to denote the lower and upper endpoint of A, respectively.

For each m the collection of *dyadic intervals of order m* is given by

$$\mathcal{D}_m = \Big\{ \Big[\frac{k}{2^m}, \frac{k+1}{2^m} \Big) \,:\, 0 \leq k \leq m-1 \Big\}.$$

If we write the point $\frac{k}{2^m} = \sum_{i=1}^m \frac{d_i}{2^i}$, $d_i \in \{0, 1\}$, in its binary expansion, then we see that the interval $\big[\frac{k}{2^m}, \frac{k+1}{2^m}\big)$ contains precisely those $x \in [0, 1)$ that have $d_1, \ldots, d_m$ as their first m base 2 digits. For each $x \in [0, 1)$ and each $m \geq 1$ there is a unique element of $\mathcal{D}_m$ that contains x. We denote this by $\mathcal{D}_m(x)$. Then

$$\lambda(\mathcal{D}_m(x)) = 2^{-m}. \tag{6.3}$$

Hence, each collection $\mathcal{D}_m$ is a *partition* of $[0, 1)$ by intervals of length 2^{-m}.

Usually A/D-converters rely on binary expansions of numbers to produce good approximations of the input signal. The β-encoder is based on β-expansions instead. Fix a value of $\beta \in (1, 2)$. An expression of the form

$$x = \sum_{i\geq 1} \frac{b_i}{\beta^i}, \quad b_i \in \{0, 1\},$$

is called a β-expansion of x, see also Example 5.7.5. One easily sees that if x has such a β-expansion, then $x \in \left[0, \frac{1}{\beta-1}\right]$. The β-encoder as described in [JM16] considers as input signal a number $x \in [0,1)$ and thus has rescaled the setup by a factor $\beta - 1$. Below we briefly explain how one can get a β-expansion of a number $\frac{x}{\beta-1}$ for $x \in [0,1)$ from the β-encoder given in the introduction but with varying threshold values u_n.

For each $u \in [\beta - 1, 1]$ define the interval map $T_u : [0,1) \to [0,1)$ by

$$T_u(y) = \begin{cases} \beta y, & \text{if } y < \frac{u}{\beta}, \\ \beta y - (\beta - 1), & \text{if } y \geq \frac{u}{\beta}. \end{cases}$$

The graph of such a map is shown in Figure 6.2. If we let u_n denote the threshold value of the quantiser at time n, then the dynamics of the β-encoder can be represented by

$$x_n = T_{u_n}(x_{n-1}) = T_{u_n} \circ \cdots \circ T_{u_1}(x), \quad n \geq 1.$$

For each $n \geq 1$, set $b_n = b_n(x) = 0$ if $\beta x_{n-1} < u_n$ and 1 otherwise. Putting $x_0 = x$, then for each $n \geq 1$,

$$T_{u_n}(x_{n-1}) = \beta x_{n-1} - (\beta - 1) b_n,$$

so that

$$x = (\beta - 1) \sum_{i=1}^{n} \frac{b_i}{\beta^i} + \frac{T_{u_n} \circ \cdots \circ T_{u_1}(x)}{\beta^n}.$$

Since $T_{u_n} \circ \cdots \circ T_{u_1}(x) \in [0,1)$ for each n, we obtain that $x = (\beta - 1) \sum_{i=1}^{\infty} \frac{b_i}{\beta^i}$. From Figure 6.2 it becomes clear that each threshold value u_n must lie in the interval $[\beta - 1, 1]$ to obtain a recursive process and bits that correspond to β-expansions.

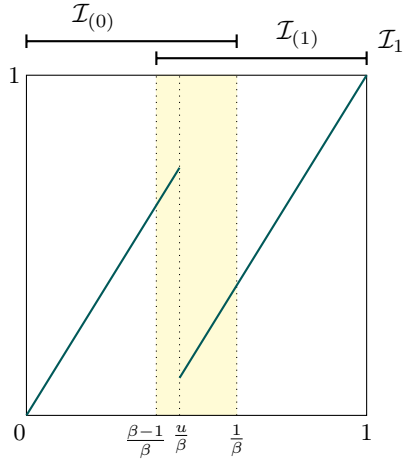

Figure 6.2: The graph of one of the maps T_u is shown for $\beta = \frac{1+\sqrt{5}}{2}$, the golden mean. The yellow area in the middle relates to the interval in which the threshold value u may be chosen. At the top we see the two intervals $\mathcal{I}_{(0)}$ and $\mathcal{I}_{(1)}$ that are the elements of the cover $\mathcal{I}_1$.

Given the first k output bits $b_1, \ldots, b_k$ of the β-encoder, we know that the input signal x has to satisfy

$$\frac{x}{\beta - 1} \in \Big[\sum_{i=1}^{k} \frac{b_i}{\beta^i}, \sum_{i=1}^{k} \frac{b_i}{\beta^i} + \sum_{i \geq k+1} \frac{1}{\beta^i}\Big] = \Big[\sum_{i=1}^{k} \frac{b_i}{\beta^i}, \sum_{i=1}^{k} \frac{b_i}{\beta^i} + \frac{1}{\beta^k(\beta - 1)}\Big].$$

For each $b_1, \ldots, b_k \in \{0, 1\}$ define

$$\mathcal{I}_{(b_1,\ldots,b_k)} = \Big[(\beta - 1)\sum_{i=1}^{k} \frac{b_i}{\beta^i}, (\beta - 1)\sum_{i=1}^{k} \frac{b_i}{\beta^i} + \frac{1}{\beta^k}\Big].$$

Comparable to the partitions $\mathcal{D}_m$ for binary expansions, we consider for each $k \geq 1$ the *cover* $\mathcal{I}_k$ of $[0, 1)$ associated to β-expansions given by

$$\mathcal{I}_k = \{\mathcal{I}_{(b_1,\ldots,b_k)} \,:\, b_i \in \{0, 1\},\, 1 \leq i \leq k\}.$$

See Figure 6.2 for an illustration of $\mathcal{I}_1 = \{\mathcal{I}_{(0)}, \mathcal{I}_{(1)}\}$.

If for $k \geq 1$ the first k output bits of the β-encoder for an input signal $x \in [0, 1)$ and a threshold value sequence $\boldsymbol{u} \in [\beta - 1, 1]^{\mathbb{N}}$ are $b_1, \ldots, b_k$, then we set

$$\mathcal{I}_k(\boldsymbol{u}, x) = \mathcal{I}_{(b_1,\ldots,b_k)},$$

since the information that the bits $b_1, \ldots, b_k$ give us is that x is contained in this interval.[1] Note that

$$\lambda(\mathcal{I}_k(\boldsymbol{u}, x)) = \beta^{-k}. \tag{6.4}$$

Furthermore,

$$k(m, \boldsymbol{u}, x) = \inf\{k \geq 1 \,:\, \mathcal{I}_k(\boldsymbol{u}, x) \subseteq \mathcal{D}_m(x)\}. \tag{6.5}$$

§6.3 Proofs of the main results

In this section we prove the main results. We start with the proof of Theorem 6.1.1, which provides bounds for the quantities $k(m, \boldsymbol{u}, x)$. This proof is inspired by the proof of [H09, Theorem 2.3].

[1] This is the setting of (5.11). Indeed, defining $A_{u,0} = [0, \frac{u}{\beta})$, $A_{u,1} = [\frac{u}{\beta}, 1)$ for each $u \in [\beta - 1, 1]$ and setting $\chi(0) = 1$,$\chi(1) = \beta - 1$ and $I = [\beta - 1, 1]$, note that

$$\mathcal{I}_{(b_1,\ldots,b_k)} = \bigcap_{i=1}^{k} T^{-1}_{\chi(b_1)\cdots\chi(b_{i-1})} A_{\chi(b_i),b_i} = \bigcup_{(\omega_1,\ldots,\omega_k)\in I^k} \bigcap_{i=1}^{k} T^{-1}_{\omega_1\cdots\omega_{i-1}} A_{\omega_i,b_i}.$$

Proof of Theorem 6.1.1. Fix $\boldsymbol{u} = (u_n)_{n\geq 1} \in [\beta - 1, 1]^{\mathbb{N}}$. For all $m \in \mathbb{N}$ and $x \in [0, 1)$ we find using (6.3) and (6.4) that

$$\begin{aligned} k(m, \boldsymbol{u}, x) - \frac{m \log 2}{\log \beta} &= \frac{k(m, \boldsymbol{u}, x) \log \beta + \log \lambda(\mathcal{I}_{k(m,\boldsymbol{u},x)}(\boldsymbol{u}, x))}{\log \beta} \\ &\quad + \frac{-\log \lambda(\mathcal{I}_{k(m,\boldsymbol{u},x)}(\boldsymbol{u}, x)) + \log \lambda(\mathcal{D}_m(x))}{\log \beta} \\ &\quad + \frac{-\log \lambda(\mathcal{D}_m(x)) - m \log 2}{\log \beta} \\ &= \frac{1}{\log \beta} \cdot \log \left(\frac{\lambda(\mathcal{D}_m(x))}{\lambda(\mathcal{I}_{k(m,\boldsymbol{u},x)}(\boldsymbol{u}, x))} \right). \end{aligned} \tag{6.6}$$

By the definition of $k(m, \boldsymbol{u}, x)$ we have $\mathcal{I}_{k(m,\boldsymbol{u},x)}(\boldsymbol{u}, x) \subseteq \mathcal{D}_m(x)$ and thus the above yields

$$k(m, \boldsymbol{u}, x) \geq \frac{m \log 2}{\log \beta}.$$

This gives (6.1).

For (6.2) let $\varepsilon \in (0, 1)$ and fix some integer $m \geq 1$. By the definition of $k(m, \boldsymbol{u}, x)$ we have that $\mathcal{I}_{k(m,\boldsymbol{u},x)-1}(\boldsymbol{u}, x) \nsubseteq \mathcal{D}_m(x)$. Hence, the distance between x and the nearest boundary point of $\mathcal{D}_m(x)$, denoted by $|x - \partial\mathcal{D}_m(x)|$, is at most equal to $\lambda(\mathcal{I}_{k(m,\boldsymbol{u},x)-1}(\boldsymbol{u}, x))$. Furthermore, we have

$$\log \lambda(\mathcal{I}_{k(m,\boldsymbol{u},x)-1}(\boldsymbol{u}, x)) - \log \lambda(\mathcal{I}_{k(m,\boldsymbol{u},x)}(\boldsymbol{u}, x)) = \log \beta.$$

Together this gives that

$$\log \left(\frac{\lambda(\mathcal{D}_m(x))}{\lambda(\mathcal{I}_{k(m,\boldsymbol{u},x)}(x))} \right) \leq \log \lambda\big(\mathcal{D}_m(x)\big) + \log \beta - \log |x - \partial\mathcal{D}_m(x)|. \tag{6.7}$$

We slightly adjust the intervals in $\mathcal{D}_m$ by removing small intervals at the endpoints: For each $m \in \mathbb{N}$ and interval $J \in \mathcal{D}_m$, let J' be the interval obtained by removing on both ends of J an interval of length $\frac{\varepsilon}{6} \cdot 2^{-m}$ and let $C_m = \bigcup_{J\in\mathcal{D}_m} J'$. Then $\lambda(J') = \big(1 - \frac{\varepsilon}{3}\big) \cdot 2^{-m}$ and $\lambda(C_m) = 1 - \frac{\varepsilon}{3}$. For $x \in C_m$ we have the bound $|x - \partial\mathcal{D}_m(x)| \geq \frac{\varepsilon}{6}\lambda(\mathcal{D}_m(x))$. Combining this with (6.6) and (6.7) gives for each integer $m \in \mathbb{N}$ and each $x \in C_m$ that

$$k(m, \boldsymbol{u}, x) - \frac{m \log 2}{\log \beta} \leq \frac{\log \frac{6}{\varepsilon}}{\log \beta} + 1.$$

Hence, we obtain (6.2) with constant $C(\varepsilon) = \frac{\log \frac{6}{\varepsilon}}{\log \beta} + 1$. □

Theorem 6.1.1 gives bounds on the value of $k(m, \boldsymbol{u}, x)$ and immediately leads to the statement on the asymptotics of the sequence $(k(m, \boldsymbol{u}, x))_{m\geq 1}$ from Corollary 6.1.2 that we prove next.

Proof of Corollary 6.1.2. Let $(a_m)_{m\geq 1}$ be a sequence that satisfies the conditions of the corollary. From (6.1) we get that for each $x \in [0, 1)$ and $m \in \mathbb{N}$,

$$\frac{1}{a_m} \left(k(m, \boldsymbol{u}, x) - \frac{m \log 2}{\log \beta} \right) \geq 0.$$

Hence, it suffices to show that for all $\delta, \varepsilon > 0$ there exists an $M \in \mathbb{N}$ such that for all $m \geq M$ we have

$$\lambda\Big(\Big\{x \in [0,1) \,:\, \frac{1}{a_m}\Big(k(m,\boldsymbol{u},x) - \frac{m\log 2}{\log\beta}\Big) > \delta\Big\}\Big) < \varepsilon.$$

This immediately follows from (6.2) by taking $M \in \mathbb{N}$ big enough such that $\frac{C(\varepsilon)}{a_m} \leq \delta$ for all $m \geq M$, which is possible because $\lim_{m\to\infty} a_m = \infty$. □

As we saw in the introduction, by choosing $a_m = m$ for all $m \geq 1$ Corollary 6.1.2 gives a limit statement reminiscent of Lochs' Theorem, but with convergence in probability. Our final result, Theorem 6.1.3 which we prove next, shows that this limit statement also holds almost surely. This proof is inspired by the proof of [DF01, Theorem 4].

Proof of Theorem 6.1.3. Fix some $\boldsymbol{u} \in [\beta-1, 1]^{\mathbb{N}}$. It follows from (6.1) that for all $x \in [0,1)$

$$\liminf_{m\to\infty} \frac{k(m,\boldsymbol{u},x)}{m} \geq \frac{\log 2}{\log\beta}.$$

Conversely, let $\varepsilon \in (0,1)$ and for each $m \geq 1$ define $\bar{k}(m) = \lceil (1+\varepsilon)\frac{m\log 2}{\log\beta}\rceil$. Let

$$\begin{aligned}\mathcal{P}_m &= \{x \in [0,1) \,:\, \mathcal{I}_{\bar{k}(m)}(\boldsymbol{u},x) \not\subseteq \mathcal{D}_m(x)\}\\ &\subseteq \bigcup_{B\in\mathcal{D}_m} \bigcup_{A\in\mathcal{I}_{\bar{k}(m)} \,:\, A\not\subseteq B} A \cap B\\ &\subseteq \bigcup_{B\in\mathcal{D}_m} [B^-, B^- + \beta^{-(1+\varepsilon)\frac{m\log 2}{\log\beta}}] \cup [B^+ - \beta^{-(1+\varepsilon)\frac{m\log 2}{\log\beta}}, B^+],\end{aligned}$$

where B^- and B^+ denote the lower and upper endpoint of B, respectively. Since $\mathcal{D}_m$ has $\beta^{\frac{m\log 2}{\log\beta}}$ elements, we have

$$\lambda\big(\mathcal{P}_m\big) \leq \beta^{\frac{m\log 2}{\log\beta}} \cdot 2 \cdot \beta^{-(1+\varepsilon)\frac{m\log 2}{\log\beta}} \leq 2\cdot\beta^{-\varepsilon\frac{m\log 2}{\log\beta}},$$

which gives that $\sum_{m=1}^{\infty} \lambda\big(\mathcal{P}_m\big) < \infty$. From the Borel-Cantelli Lemma it follows that

$$\lambda\big(\{x \in [0,1) \,:\, x \in \mathcal{P}_m \text{ for infinitely many } m \in \mathbb{N}\}\big) = 0.$$

Hence,

$$\lambda\big(\{x \in [0,1) \,:\, \exists M \in \mathbb{N} \text{ s.t. } \forall m \geq M\ \mathcal{I}_{\bar{k}(m)}(\boldsymbol{u},x) \subseteq \mathcal{D}_m(x)\}\big) = 1,$$

or in other words, for Lebesgue almost all $x \in [0,1]$ there exists an $M \in \mathbb{N}$ such that for all $m \geq M$ it holds that $k(m,\boldsymbol{u},x) \leq \bar{k}(m)$. This gives

$$\limsup_{m\to\infty} \frac{k(m,\boldsymbol{u},x)}{m} \leq \limsup_{m\to\infty} \frac{\bar{k}(m)}{m} = (1+\varepsilon)\frac{\log 2}{\log\beta}, \qquad \lambda\text{-a.e.}$$

Since $\varepsilon > 0$ was arbitrary, this concludes the proof. □

Remark 6.3.1. Note that the first part of the previous proof holds for all $x \in [0,1]$. It is the second part that only holds Lebesgue almost everywhere.

§6.4 Final remarks

In practice it is not only the threshold value u that is subject to fluctuations due to noise on the circuit, but also the amplification factor β and the scaling factor $\beta - 1$. This issue and possible solutions to it were discussed in [DY06, W08, DGWY10]. Here we discuss the consequences for the value $k(m, \boldsymbol{u}, x)$.

Assume that the amplification factor and scaling factor fluctuate within intervals $[\beta_{\min}, \beta_{\max}], [\tilde{\beta}_{\min}, \tilde{\beta}_{\max}] \subseteq (1, 2)$, respectively. We use $\boldsymbol{\beta} = (\beta_n)_{n\geq 1} \in [\beta_{\min}, \beta_{\max}]^{\mathbb{N}}$ and $\tilde{\boldsymbol{\beta}} = (\tilde{\beta}_n)_{n\geq 1} \in [\tilde{\beta}_{\min}, \tilde{\beta}_{\max}]^{\mathbb{N}}$ to denote the sequence of consecutive amplification factors β_n and scaling factors $\tilde{\beta}_n - 1$, respectively. For an input value $x = x_0 \in [0, 1)$, the bits b_n are produced iteratively by setting $x_n = \beta_n x_{n-1} - (\tilde{\beta}_n - 1)b_n$ and

$$b_n = \begin{cases} 0, & \text{if } \beta_n x_{n-1} < u_n, \\ 1, & \text{if } \beta_n x_{n-1} \geq u_n. \end{cases}$$

This gives, for each n,

$$x = \sum_{i=1}^{n} \frac{(\tilde{\beta}_i - 1)b_i}{\prod_{j=1}^{i} \beta_j} + \frac{x_n}{\prod_{j=1}^{n} \beta_j}.$$

Note that

$$\sum_{i=1}^{\infty} \frac{(\tilde{\beta}_i - 1)b_i}{\prod_{j=1}^{i} \beta_j} \leq (\tilde{\beta}_{\max} - 1) \sum_{i=1}^{\infty} \frac{1}{\beta_{\min}^i} < \infty,$$

so

$$\varkappa := \lim_{n\to\infty} \frac{x_n}{\prod_{j=1}^{n} \beta_j} = x - \sum_{i=1}^{\infty} \frac{(\tilde{\beta}_i - 1)b_i}{\prod_{j=1}^{i} \beta_j}$$

is finite.

If for $k \geq 1$ the first k output bits of the β-encoder are $b_1, \ldots, b_k$ for an input signal $x \in [0, 1)$, an amplification sequence $\boldsymbol{\beta} \in [\beta_{\min}, \beta_{\max}]^{\mathbb{N}}$, a scaling sequence $\tilde{\boldsymbol{\beta}} \in [\tilde{\beta}_{\min}, \tilde{\beta}_{\max}]^{\mathbb{N}}$ and a threshold sequence $\boldsymbol{u} \in [0, 1]^{\mathbb{N}}$, then optimally (that means, knowing the value of $\varkappa$) we know that x lies in the interval

$$\tilde{\mathcal{I}}_k(\boldsymbol{u}, \boldsymbol{\beta}, \tilde{\boldsymbol{\beta}}, x) = \Big[(\tilde{\beta}_{\min} - 1) \sum_{i=1}^{k} \frac{b_i}{\beta_{\max}^i} + \varkappa, (\tilde{\beta}_{\max} - 1) \sum_{i=1}^{k} \frac{b_i}{\beta_{\min}^i} + \frac{\tilde{\beta}_{\max} - 1}{\beta_{\min} - 1} \frac{1}{\beta_{\min}^k} + \varkappa\Big].$$

The lower and upper endpoints of the sets $\{\tilde{\mathcal{I}}_k(\boldsymbol{u}, \boldsymbol{\beta}, \tilde{\boldsymbol{\beta}}, x)\}$ form an increasing and decreasing sequence, respectively, so

$$\bigcap_{k\geq 1} \tilde{\mathcal{I}}_k(\boldsymbol{u}, \boldsymbol{\beta}, \tilde{\boldsymbol{\beta}}, x) = \Big[(\tilde{\beta}_{\min} - 1) \sum_{i=1}^{\infty} \frac{b_i}{\beta_{\max}^i} + \varkappa, (\tilde{\beta}_{\max} - 1) \sum_{i=1}^{\infty} \frac{b_i}{\beta_{\min}^i} + \varkappa\Big], \tag{6.8}$$

which has length > 0 if $x \neq 0$ and either $\beta_{\min} < \beta_{\max}$ or $\tilde{\beta}_{\min} < \tilde{\beta}_{\max}$ or both are the case. (Indeed, note that in case $x \neq 0$ there exists $i \in \mathbb{N}$ such that $b_i = 1$.) Similar as to (6.5), we define $k(m, \boldsymbol{u}, \boldsymbol{\beta}, \tilde{\boldsymbol{\beta}}, x)$ to be the number of bits from the β-encoder

subject to noise in the amplification, the scaling and the threshold that are necessary to obtain m base 2 digits of the number x, i.e.

$$k(m, \boldsymbol{u}, \boldsymbol{\beta}, \tilde{\boldsymbol{\beta}}, x) = \inf\{k \geq 1 : \tilde{\mathcal{I}}_k(\boldsymbol{u}, \boldsymbol{\beta}, \tilde{\boldsymbol{\beta}}, x) \subseteq \mathcal{D}_m(x)\}.$$

We see from (6.8) that if $\beta_{\min} < \beta_{\max}$ or $\tilde{\beta}_{\min} < \tilde{\beta}_{\max}$, then for all $x \in (0,1)$, all $\boldsymbol{\beta} \in [\beta_{\min}, \beta_{\max}]^{\mathbb{N}}$, all $\tilde{\boldsymbol{\beta}} \in [\tilde{\beta}_{\min}, \tilde{\beta}_{\max}]^{\mathbb{N}}$ and all $\boldsymbol{u} \in [0,1]^{\mathbb{N}}$ there exists $M > 0$ such that for all integers $m > M$ we have

$$k(m, \boldsymbol{u}, \boldsymbol{\beta}, \tilde{\boldsymbol{\beta}}, x) = \infty.$$

In other words, the expected number of bits from the β-encoder that are necessary to obtain m base 2 digits of the number x is infinite for large m. Hence, this indicates that the proposed pseudo-random number generator of [JM16] is not efficient for generating large pseudo-random numbers if the β-encoder in this process is subject to noise in the amplification or scaling as well.