Pseudo-random number generation with β-encoders

Kalle, C.; Verbitskiy, E.; Zeegers, B.

DOI
10.1142/S2661335224500266

Publication date
2024

Document Version
Final published version

Published in
International Journal of Mathematics for Industry

OPEN ACCESS
International Journal of Mathematics for Industry
Vol. 16, No. 1 (2024) 2450026 (11 pages)

DOI: 10.1142/S2661335224500266

World Scientific
www.worldscientific.com

Pseudo-random number generation with β-encoders

Charlene Kalle [*,‡], Evgeny Verbitskiy [*,†,§] and Benthen Zeegers [*,¶]
*Mathematisch Instituut, Leiden University
Niels Bohrweg 1, 2333CA Leiden, The Netherlands
†Korteweg-de Vries Institute for Mathematics
University of Amsterdam, Postbus 94248
1090 GE Amsterdam, The Netherlands
‡kallecccj@math.leidenuniv.nl
§evgeny@math.leidenuniv.nl
¶benthen_zeegers@math.leidenuniv.nl; benthen_zeegers@live.nl

Received 26 March 2023
Accepted 13 October 2024
Published 16 December 2024

The β-encoder is an analog circuit that converts an input signal $x \in [0,1]$ into a finite bit stream $\{b_i\}$. The bits $\{b_i\}$ are correlated and therefore are not immediately suitable for random number generation, but they can be used to generate bits $\{a_i\}$ that are (nearly) uniformly distributed. In this paper, we study two such methods. In the first part the bits $\{a_i\}$ are defined as the digits of the base-2 representation of the original input x. Under the assumption that there is no noise in the amplifier we then study a question posed by Jitsumatsu and Matsumura on how many bits $b_1, \ldots, b_m$ are needed to correctly determine the first n bits $a_1, \ldots, a_n$. In the second part, we show this method fails for random amplification factors. Nevertheless, even in this case, nearly uniformly distributed bits can still be generated from $b_1, \ldots, b_m$ using modern cryptographic techniques.

Keywords: β-encoder; binary expansions; Lochs' Theorem; random number generation.

1. Introduction

Any real number $x \in [0,1]$ can be represented in base 2 as

$$x = \sum_{n=1}^{\infty} \frac{a_n}{2^n}, \quad a_n \in \{0,1\}. \tag{1}$$

With the exception of a countable set of dyadic rationals of the form $x = \frac{K}{2^N}$, $K, N \in \mathbb{Z}_+$, the representation (1) is unique. The digits $\{a_n = a_n(x)\}$ can be obtained iteratively as follows: let $x_0 = x$, and for $n \geq 1$, we let

$$a_n = \begin{cases} 0, & \text{if } 2x_{n-1} < 1, \\ 1, & \text{if } 2x_{n-1} \geq 1 \end{cases} \quad \text{and} \tag{2}$$
$$x_n = 2x_{n-1} - a_n.$$

¶Corresponding author.

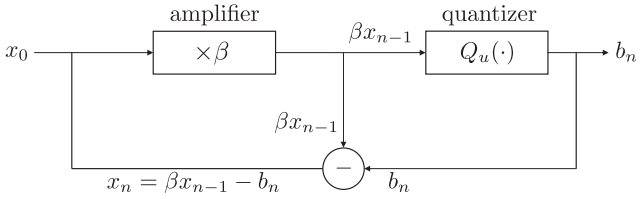

Fig. 1. Iteration process of the β-encoder.

Similarly, for $\beta \in (1,2)$, any number $x \in [0,1]$ can also be represented in *non-integer base* β as

$$x = \sum_{n=1}^{\infty} \frac{b_n}{\beta^n}, \tag{3}$$

again with binary digits b_n in $\{0,1\}$. (In fact, any number $x \in [0, \frac{1}{\beta-1}]$ has an expansion of the form (3).) Since $\beta \in (1,2)$ is not an integer, Lebesgue almost all points x have uncountably many different β-expansions.[1,2] This somewhat curious fact from number theory has some interesting applications in signal processing. As is well known, for each $u \in [1, \frac{1}{\beta-1}]$ expansions of the form in (3) can be obtained in a similar fashion as the base 2 expansions by setting $x_0 = x$, and for $n \geq 1$,

$$b_n = \begin{cases} 0, & \text{if } \beta x_{n-1} < u, \\ 1, & \text{if } \beta x_{n-1} \geq u \end{cases} \quad \text{and} \qquad x_n = \beta x_{n-1} - b_n. \tag{4}$$

This iteration scheme is used in β-encoders, which were introduced in Ref. 3 by Daubechies *et al.* Using an *amplifier* with amplification factor β and a *quantizer*

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

for an input signal $x = x_0$ in $[0,1]$ a β-encoder outputs bits $b_n = Q_u(\beta x_{n-1})$ where $x_n = \beta x - Q_u(\beta x_{n-1})$, see Fig. 1, which corresponds to the iteration scheme in (4). In practice, however, due to the intrinsic presence of noise in analogue circuits, the amplification factor β and the threshold value u fluctuate during the operation of a β-encoder circuit. If we denote by $(\beta_n)_{n\geq 1}$ and $(u_n)_{n\geq 1}$ the consecutive (random) amplification factors β_n and threshold values u_n, respectively, used at each time step of the approximation algorithm, the β-encoder in reality outputs bits $b_n = Q_{u_n}(\beta_n x_{n-1})$ where $x_n = \beta_n x - Q_{u_n}(\beta_n x_{n-1})$. The robustness of the β-encoder in the A/D-conversion process has been studied in e.g., Refs. 4–11 and 12.

In recent years β-encoders were also considered as sources for random number generation, see Refs. 13–15 and 16. If x is chosen uniformly at random in $[0,1]$, then the digits $\{a_n(x)\}_{n\geq 1}$ from (1) form a sequence of binary independent identically distributed random variables with $\mathbb{P}(a_n = 0) = \mathbb{P}(a_n = 1) = \frac{1}{2}$. On the other hand, it is known that successive bits $\{b_n\}$ in the output of a β-encoder are correlated and therefore not immediately applicable as pseudo-random numbers. Under the assumption that the amplification factor β does not fluctuate, Jitsumatsu and Matsumura proposed in Ref. 13, a coding scheme which 'removes' the dependence between the bits and converts the output bits $\{b_n\}$ of the β-encoder into the binary digits $\{a_n\}$ in base 2 of the number it represents. It is verified in Ref. 13 that the resulting output sequences $\{a_n\}$ pass the NIST statistical test suite from Ref. 17, which shows that this method performs well as a pseudo-random number generator. A natural question asked in Ref. 13 is the following: If we use $\boldsymbol{u} = (u_n)_{n\geq 1}$ to denote the consecutive (random) threshold values u_n, what is the number $k(m, \boldsymbol{u}, x)$ of bits $\{b_n\}$ from the β-encoder that are necessary to obtain m digits in base 2 of the number x via this process? In Ref. 13, the lower bound $k(m, \boldsymbol{u}, x) \geq \frac{m \log 2}{\log \beta}$ was found.[a] The authors of Ref. 13 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.

The question from Ref. 13 is reminiscent of the considerations of Lochs in Ref. 18 from 1964, where Lochs asked how many regular continued fraction digits of a real number x one can determine from knowing only the first n decimal digits of x. If we call this number of digits $m_L(n,x)$, then Lochs' Theorem states that for Lebesgue almost every $x \in [0,1]$,

$$\lim_{n\to\infty} \frac{m_L(n,x)}{n} = \frac{6 \log 2 \log 10}{\pi^2}. \tag{5}$$

[a]This bound was found in Ref. 13 for bits $\{b_n\}$ from a *scale-adjusted* β-encoder, that is, if the iteration scheme is given by (4) but with $u \in [\beta - 1, 1]$ and $x_n = \beta x_{n-1} - (\beta - 1) b_n$. This difference is not principal in the first three sections where the amplification factor is assumed to be fixed. However, in reality, the amplifier and scale-adjuster are subject to noise as well, and to minimize this influence we therefore consider a model without scale-adjuster.

The somewhat mysterious expression on the right-hand side turns out to be a ratio of *entropies* of the interval maps $T(x) = 10x \bmod 1$ and $S(x) = 1/x \bmod 1$ that generate the decimal expansions and regular continued fraction expansions, respectively. Lochs' result was extended in Ref. 19 to other types of number expansions including binary expansions and β-expansions by placing it in a dynamical systems framework, see also Ref. 20. These results are further generalized in Ref. 21 to number expansions generated by random dynamical systems. Unfortunately the results from Refs. 18–21 do not immediately apply to the question from Ref. 13 due to the uncertainty in the threshold value u. In this paper, we adapt the methods from Refs. 19 and 21 to the specific iteration scheme of the β-encoder.

The first goal of this paper is to address the question posed in Ref. 13. In our first main result we recover the lower bound from Ref. 13 and we obtain a statement on an upper bound for $k(m, \boldsymbol{u}, x)$. More precisely, we obtain the following results. Here λ denotes the one-dimensional Lebesgue measure.

Theorem 1.1. *Consider $\beta \in (1,2)$ and a sequence of thresholds $\boldsymbol{u} = (u_n)_{n\geq 1} \in [1, (\beta-1)^{-1}]^{\mathbb{N}}$. For all $x \in [0,1]$ and all $m \in \mathbb{N}$ it holds that*

$$k(m, \boldsymbol{u}, x) \geq \frac{m \log 2}{\log \beta}. \tag{6}$$

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

$$\lambda\left(\left\{x \in [0,1] : k(m, \boldsymbol{u}, x) - \frac{m \log 2}{\log \beta} > C(\varepsilon)\right\}\right) < \varepsilon. \tag{7}$$

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

Corollary 1.1. *For any real positive sequence $(n_m)_{m\in\mathbb{N}}$ with $\lim_{m\to\infty} n_m = \infty$, each $\boldsymbol{u} \in [1, (\beta-1)^{-1}]^{\mathbb{N}}$ and $\varepsilon > 0$ it holds that*

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

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

In particular, the above corollary has the following implications:

- Taking $n_m = \sqrt{m}$ for each m gives a Central Limit Theorem result where the limiting distribution has zero variance;
- Taking $n_m = m$ for each m we retrieve a limit statement in the spirit of (5), but with convergence in probability instead of almost surely.

By adjusting the setup from Ref. 19 to suit our purposes, we obtain the stronger result of almost sure convergence for the specific sequence $(n_m)_{m\geq 1}$ with $n_m = m$ for each m that is stated in the next theorem.

Theorem 1.2. *For each $\boldsymbol{u} \in [1, (\beta-1)^{-1}]^{\mathbb{N}}$, it holds that*

$$\lim_{m\to\infty} \frac{k(m, \boldsymbol{u}, x)}{m} = \frac{\log 2}{\log \beta} \quad \text{for } \lambda - \text{a.e. } x \in [0,1].$$

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

Since the implementation of β-encoders it has been observed that (like for the threshold value u) there is uncertainty about the precise value of β during the encoding process. The actual value of β can only be determined to lie within an interval $[\beta_{\min}, \beta_{\max}]$. Possible solutions to this problem were studied in Refs. 5, 6 and 12. We will argue that in this case, one is not able to extract a large number of digits $(a_1, \ldots, a_n)$ in the base 2 expansion of the input value x using the output bits $(b_1, \ldots, b_m)$ from the β-encoder. Nevertheless, the output bits $(b_1, \ldots, b_m)$ are still sufficiently random, and using modern cryptographic techniques, one is still able to extract n nearly independent bits from $\gamma n \frac{\log 2}{\log \beta}$ output bits, where $\gamma > 1$ is a fixed factor, which depends on how close to 'nearly independent' the final output bits should be.

The paper is organized as follows. In the next section, we introduce the necessary notation and preliminaries on base 2 expansions and β-expansions. In Sec. 3, we prove Theorem 1.1, Corollary 1.1 and Theorem 1.2. Here it is assumed that the amplification factor is fixed and only the threshold value fluctuates. Finally, in Sec. 4, we discuss modern cryptographic techniques to apply for the case that the amplification factor fluctuates as well.

2. Preliminaries

For a set A and an integer $m \geq 1$ we use the notation $A^m = \{(a_1, \ldots, a_m) : a_i \in A, 1 \leq i \leq m\}$ and $A^{\mathbb{N}} = \{(a_k)_{k\geq 1} : a_k \in A, k \geq 1\}$. If I is an interval in the real line, then we write ∂I for the set containing the two boundary points of I and we use I^- and I^+ to denote the left and right endpoints of I, respectively.

For each $m \geq 1$ the collection of *dyadic intervals of order* m is given by

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

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 $[\frac{k}{2^m}, \frac{k+1}{2^m})$ contains precisely those $x \in [0,1)$ that have $d_1, \ldots, d_m$ as their first m binary 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 interval by $\mathcal{D}_m(x)$. Then

$$\lambda(\mathcal{D}_m(x)) = 2^{-m}. \tag{8}$$

Hence, each collection $\mathcal{D}_m$ is a partition of $[0,1)$ by intervals of length 2^{-m}. By adding the point 1 to the last interval of $\mathcal{D}_m$, we obtain a partition of the closed interval $[0,1]$ without disturbing any of the properties mentioned above.

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 following form:

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

is called a β-expansion of x. The set of numbers that can be written in this way is equal to the interval $[0, \frac{1}{\beta-1}]$. We now briefly explain how one can get a β-expansion of a number x from the β-encoder introduced in the introduction with varying threshold values u_n.

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

$$T_u(y) = \begin{cases} \beta y & \text{if } y < \dfrac{u}{\beta}, \\ \beta y - 1 & \text{if } y \geq \dfrac{u}{\beta}. \end{cases} \tag{9}$$

The graph of such a map is shown in Fig. 2. If we let u_n denote the threshold value of the quantizer at time n, then the dynamics of the β-encoder can be represented as

$$x_n = T_{u_n}(x_{n-1}) = T_{u_n} \circ \cdots \circ T_{u_1}(x), \quad n \geq 1. \tag{10}$$

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

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

so that

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

Since $T_{u_n} \circ \cdots \circ T_{u_1}(x) \in [0, (\beta-1)^{-1}]$ holds for each n, we immediately conclude that $x = \sum_{n=1}^\infty \frac{b_n}{\beta^n}$. From Fig. 2, it becomes clear that each threshold value u_n must lie in the interval $[1, (\beta-1)^{-1}]$ to obtain a recursive process and bits that correspond to β-expansions. It follows from Theorem 2 in Ref. 22, where for the case that $\beta \in (1,2)$ only the choices $u_n \in \{1, (\beta-1)^{-1}\}$ for each $n \geq 1$ are considered, that in fact all β-expansions can be generated using the above iteration process.

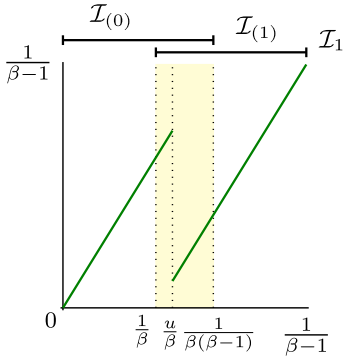

Fig. 2. (Color online) The graph of one of the maps T_u is shown for $\beta = \frac{1+\sqrt{5}}{2}$, the golden mean. The yellow area in the middle relates to the interval in which the threshold value u may be chosen. At the top we see the two intervals $\mathcal{I}_{(0)}$ and $\mathcal{I}_{(1)}$ that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

Remark 2.1. Note that if one starts this process with a number $x \in [0,1]$, then typically $x_n > 1$ for many n. The reason to look at $x \in [0,1]$ instead of $x \in [0, \frac{1}{\beta-1}]$ is to make the comparison with the dyadic intervals $\mathcal{D}_m(x)$, which are defined on $[0,1]$, easier.

Given the first k output bits $b_1, \ldots, b_k$ of the β-encoder, we know that the input signal $x \in [0,1]$

has to satisfy

$$x \in \left[\sum_{n=1}^{k}\frac{b_n}{\beta^n}, \sum_{n=1}^{k}\frac{b_n}{\beta^n} + \sum_{n\geq k+1}\frac{1}{\beta^k}\right] = \left[\sum_{n=1}^{k}\frac{b_n}{\beta^n}, \sum_{n=1}^{k}\frac{b_n}{\beta^n} + \frac{1}{\beta^k(\beta-1)}\right].$$

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

$$\mathcal{I}_{(b_1,\ldots,b_k)} = \left[\sum_{n=1}^{k}\frac{b_n}{\beta^n}, \sum_{n=1}^{k}\frac{b_n}{\beta^n} + \frac{1}{\beta^k(\beta-1)}\right].$$

Comparable to the partitions $\mathcal{D}_m$ for binary expansions, we consider for each $k \geq 1$ the *cover* $\mathcal{I}_k$ of $[0, (\beta-1)^{-1}]$ 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 Fig. 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 $\boldsymbol{u} \in [1, (\beta-1)^{-1}]^{\mathbb{N}}$ 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. Note that

$$\lambda(\mathcal{I}_k(\boldsymbol{u}, x)) = \frac{1}{\beta^k(\beta-1)}. \tag{11}$$

Furthermore,

$$k(m, \boldsymbol{u}, x) = \inf\{k \geq 1 : \mathcal{I}_k(\boldsymbol{u}, x) \subseteq \mathcal{D}_m(x)\}. \tag{12}$$

3. Fixed Amplification Factor

In this section, we prove our first main results where the amplification factor is assumed to be fixed. We start with the proof of Theorem 1.1, which provides bounds for the quantities $k(m, \boldsymbol{u}, x)$. This proof is inspired by the proof of Theorem 2.3 in Ref. 23.

Proof of Theorem 1.1 Fix $\boldsymbol{u} = (u_n)_{n\geq 1} \in [1, (\beta-1)^{-1}]^{\mathbb{N}}$. For all $m \in \mathbb{N}$ and $x \in [0,1]$ we find by (8) and (11) that $\lambda(\mathcal{D}_m(x)) = 2^{-m}$ and $\lambda(\mathcal{I}_{k(m,\boldsymbol{u},x)}(\boldsymbol{u}, x)) = \beta^{-k(m,\boldsymbol{u},x)}(\beta-1)^{-1}$. Hence,

$$k(m, \boldsymbol{u}, x) - \frac{m\log 2}{\log\beta} + \frac{\log(\beta-1)}{\log\beta} = \frac{1}{\log\beta}\cdot\log\left(\frac{\lambda(\mathcal{D}_m(x))}{\lambda(\mathcal{I}_{k(m,\boldsymbol{u},x)}(\boldsymbol{u}, x))}\right). \tag{13}$$

Furthermore, 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 since $\beta \in (1,2)$ the above yields

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

This gives (6).

For (7) let $\varepsilon \in (0,1)$ and fix some integer $m \geq 1$. By the definition of $k(m, \boldsymbol{u}, x)$, we have that $\mathcal{I}_{k(m,\boldsymbol{u},x)-1}(\boldsymbol{u}, x) \not\subseteq \mathcal{D}_m(x)$. 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

$$\log\left(\frac{\lambda(\mathcal{D}_m(x))}{\lambda(\mathcal{I}_{k(m,\boldsymbol{u},x)}(x))}\right) \leq \log\lambda(\mathcal{D}_m(x)) + \log\beta - \log|x - \partial\mathcal{D}_m(x)|. \tag{14}$$

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 $\frac{\varepsilon}{2}\cdot 2^{-m}$ and let $C_m = \bigcup_{J\in\mathcal{D}_m} J'$. Then $\lambda(J') = (1-\varepsilon)\cdot 2^{-m}$ and $\lambda(C_m) = 1-\varepsilon$. For $x \in C_m$ we have the bound $|x - \partial\mathcal{D}_m(x)| \geq \frac{\varepsilon}{2}\lambda(\mathcal{D}_m(x))$. Combining this with (13) and (14) gives for each integer $m \in \mathbb{N}$ and each $x \in C_m$ that

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

Hence, we obtain (7) with constant $C(\varepsilon) = \frac{\log\frac{2}{\varepsilon}}{\log\beta} + 1$. □

Theorem 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 1.1 that we prove next.

Proof of Corollary 1.1 Let $(n_m)_{m\geq 1}$ be a sequence of positive real numbers that satisfy $\lim_{m\to\infty} n_m = \infty$. From (6) we get that for each $x \in [0,1]$ and $m \in \mathbb{N}$,

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

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

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

This immediately follows from (7) by taking $M \in \mathbb{N}$ big enough such that $\frac{C(\delta)}{n_m} \leq \varepsilon$ for all $m \geq M$, which is possible because $\lim_{m\to\infty} n_m = \infty$. □

As we saw in the introduction, by choosing $n_m = m$ for all $m \geq 1$, Corollary 1.1 gives a limit statement reminiscent of Lochs' Theorem, but with convergence in probability. Our final result, Theorem 1.2, shows that this limit statement also holds almost surely. The proof we present for Theorem 1.2 below is inspired by the proof of Theorem 4 in Ref. 19.

Proof of Theorem 1.2 Fix some $\boldsymbol{u} \in [\beta - 1, 1]^{\mathbb{N}}$. It follows from (6) 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

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

Since $\mathcal{D}_m$ has $2^m = \beta^{\frac{m \log 2}{\log \beta}}$ elements, we have

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

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

$$\begin{aligned}
&\lambda(\{x \in [0,1] : x \in \mathcal{P}_m \\
&\qquad \text{for infinitely many } m \in \mathbb{N}\}) = 0.
\end{aligned}$$

Hence,

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

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

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

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

Remark 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.

4. Random Amplification Factor

In practice, it is not only the threshold value u that is subject to fluctuations present in the circuit, but also the amplification factor β. This issue and its implications for signal processing were discussed extensively in Refs. 5, 6 and 12. Under some extra assumptions, e.g., amplification factors varying slowly and smoothly, one can find some ways to remedy this issue. However, in the general case, as the following simple consideration shows, in the presence of random amplification factors, one cannot expect to reliably determine *a significant number* of digits in the base 2 expansion of the input signal x by linking them to the digits from a random β-expansion of x.

Let us start by modeling the random amplification factors. Suppose that at each iteration the amplification factor β assumes a random value in some interval $[\beta_{\min}, \beta_{\max}] \subseteq (1,2)$. Denote by $\boldsymbol{\beta} = (\beta_n)_{n\geq 1} \in [\beta_{\min}, \beta_{\max}]^{\mathbb{N}}$ the corresponding sequence. Similarly, we denote by $\boldsymbol{u} = (u_n)_{n\geq 1}$ again the sequence of the corresponding random threshold values. We assume $u_n \in [1, (\beta_{\max} - 1)^{-1}]$ for all n. As we will see below, the sequence $\boldsymbol{u}$ will not have any effect on the conclusions.

Again, randomly choose $x_0 = x$ uniformly in $[0,1]$. The bits b_n, $n \geq 1$, are defined iteratively by

$$\begin{aligned}
b_n &= Q_{u_n}(\beta_n x_{n-1}) \\
&= \begin{cases} 0 & \text{if } \beta_n x_{n-1} < u_n, \\ 1 & \text{if } \beta_n x_{n-1} \geq u_n \end{cases} \quad \text{and } x_n = \beta_n x_{n-1} - b_n.
\end{aligned} \tag{15}$$

Thus for all n, one has

$$x = \sum_{i=1}^{n} \frac{b_i}{\prod_{j=1}^{i} \beta_j} + \frac{x_n}{\prod_{j=1}^{n} \beta_j}. \tag{16}$$

Lemma 4.1. *We have* $x_n \le (\beta_{\max}-1)^{-1}$ *for all* n.

Proof. We have $x_0 \le 1 \le (\beta_{\max}-1)^{-1}$. Now suppose $x_n \le (\beta_{\max}-1)^{-1}$ holds for some n. If $b_{n+1}=0$, then

$$x_{n+1} = \beta_{n+1}x_n - b_{n+1} = \beta_{n+1}x_n < u_{n+1} \le (\beta_{\max}-1)^{-1}.$$

On the other hand, if $b_{n+1}=1$, then

$$x_{n+1} = \beta_{n+1}x_n - 1 \le \frac{\beta_{n+1}}{\beta_{\max}-1} - 1 \le \frac{\beta_{\max}-\beta_{\max}+1}{\beta_{\max}-1} = (\beta_{\max}-1)^{-1}.$$

So the statement holds in both cases. □

Setting $\varkappa = (\beta_{\max}-1)^{-1}$, it follows from the above lemma and (16) that

$$0 \le x - \sum_{i=1}^{n} \frac{b_i}{\prod_{j=1}^{i}\beta_j} \le \frac{\varkappa}{\beta_{\min}^n} \to 0 \quad \text{as } n\to\infty. \tag{17}$$

Hence, the digits b_n correspond to an expansion of x of the form $x = \sum_{i=1}^{\infty} \frac{b_i}{\prod_{j=1}^{i}\beta_j}$. These are called a *Cantor real base expansions* and are studied in Ref. 24.

However, given the first m output digits $b_1,\dots,b_m$, without exact knowledge on the sequence $\boldsymbol{\beta}$ of random β-encoder amplifications, the only certain conclusion about the location of $x=x_0$ one can draw from (16) is that

$$x \in \hat{\mathcal{I}}_{(b_1,\dots,b_m)} := \left[\sum_{k=1}^{m}\frac{b_k}{\beta_{\max}^k}, \sum_{k=1}^{m}\frac{b_k}{\beta_{\min}^k} + \frac{\varkappa}{\beta_{\min}^m}\right].$$

The immediate conclusion is that the length $\hat{\mathcal{I}}_{(b_1,\dots,b_m)}$ does not converge[b] to 0 as $m\to\infty$, and hence we cannot reliably determine a large number of binary digits of x. Hence, under the assumption that amplification factors fluctuate in the β-encoder circuit, one cannot guarantee the quality of the corresponding pseudo-random number generators studied earlier in the literature.

Nevertheless, it is absolutely clear, that the 'random' β-expansion circuit does produce digits (b_m) which are sufficiently random, and hence can, in principle, be used in random number generators. The natural practical questions are how much randomness is in $(b_1,\dots,b_m)$, and how can one *extract* this randomness?

Let us start with the first question. Suppose $\boldsymbol{\beta} = (\beta_n)$ is a random process of random amplification factors assuming values $\beta_n \in [\beta_{\min},\beta_{\max}]$ for all n. We denote by ρ the corresponding probability law on $[\beta_{\min},\beta_{\max}]^{\mathbb{N}}$. As we will see, the threshold values $\boldsymbol{u}=(u_n)$ will not be important. For convenience we will assume $u_n=1$ for all n. The initial point $x=x_0$ will be chosen uniformly in $[0,1]$. Recall that λ denotes the Lebesgue measure on $[0,1]$. Let $\Omega = [\beta_{\min},\beta_{\max}]^{\mathbb{N}}\times[0,1]$ and let $\mathbb{P}=\rho\times\lambda$ denote the corresponding probability law. Consider now the first m β-digits $(b_1,\dots,b_m)$ obtained according to (15). We will view $b_1=b_1(\omega),\dots,b_m=b_m(\omega)$ as random variables on Ω with $\omega=(\boldsymbol{\beta},x_0)$ distributed according to $\mathbb{P}=\rho\times\lambda$.

One way to quantify randomness in $(b_1,\dots,b_m)$ is to estimate the so-called min-*entropy* $\mathbf{H}_\infty(\mathbb{P}_m)$ of the corresponding probability distribution $\mathbb{P}_m$ on the space of binary strings of length m. If we write $c_1^m := c_1\cdots c_m \in \{0,1\}^m$ for a word of length m, then

$$\begin{aligned}\mathbf{H}_\infty(\mathbb{P}_m) &:= \min_{c_1^m\in\{0,1\}^m} \log^2\frac{1}{\mathbb{P}_m(c_1^m)}\\ &= -\log^2 \max_{c_1^m\in\{0,1\}^m} \mathbb{P}_m(c_1^m)\\ &= -\log^2 \max_{c_1^m\in\{0,1\}^m} \mathbb{P}(\{\omega\in\Omega : b_1(\omega)\\ &\quad = c_1,\dots,b_m(\omega)=c_m\}).\end{aligned}$$

The lower bound on $\mathbf{H}_\infty(\mathbb{P}_m)$ is relatively straightforward: indeed, for any $c_1^m\in\{0,1\}^m$, by the law of total probability,

$$\begin{aligned}\mathbb{P}_m(c_1^m) &= \mathbb{P}(\{(\boldsymbol{\beta},x)\in\Omega : b_1(\boldsymbol{\beta},x)\\ &\quad = c_1,\dots,b_m(\boldsymbol{\beta},x)=c_m\})\\ &= \int_{[\beta_{\min},\beta_{\max}]^{\mathbb{N}}} \lambda(\{x\in[0,1] : b_1(\boldsymbol{\beta},x)\\ &\quad = c_1,\dots,b_m(\boldsymbol{\beta},x)=c_m\})\rho(d\boldsymbol{\beta}).\end{aligned}$$

For fixed $\beta_1,\dots,\beta_m$, one has

$$\{x\in[0,1] : b_1(\boldsymbol{\beta},x)=c_1,\dots,b_m(\boldsymbol{\beta},x)=c_m\} \subseteq \left[\sum_{i=1}^{m}\frac{c_i}{\prod_{j=1}^{i}\beta_j}, \sum_{i=1}^{m}\frac{c_i}{\prod_{j=1}^{i}\beta_j} + \frac{\varkappa}{\prod_{j=1}^{m}\beta_j}\right] \tag{18}$$

[b]Unless all β-digits b_n are 0.

and hence,

$$\mathbb{P}_m(c_1^m) \le \int_{[\beta_{\min},\beta_{\max}]^{\mathbb{N}}} \frac{\varkappa}{\prod_{j=1}^m \beta_j}\rho(d\boldsymbol{\beta}) \le \frac{\varkappa}{(\beta_{\min})^m}\int_{[\beta_{\min},\beta_{\max}]^{\mathbb{N}}}\rho(d\boldsymbol{\beta}) = \frac{\varkappa}{(\beta_{\min})^m}.$$

Therefore,

$$\mathbf{H}_\infty(\mathbb{P}_m) \ge m\log^2\beta_{\min} - \log^2\varkappa. \tag{19}$$

This argument shows that the min-entropy of our physical source of randomness—the β-encoder circuit—grows linearly in m, and that the growth-rate is at least $\frac{\log\beta_{\min}}{\log 2}$, i.e., the entropy of the 'worst' or the least random β-transformation, which is present in the mix. A random variable X is called an (m,k)-*source* if X takes values in $\{0,1\}^m$ and $\mathbf{H}_\infty(X) \ge k$. The computation above shows that, independent of ρ, the string of the first m bits of the β-encoder $\boldsymbol{b}_m = (b_1,\dots,b_m)$ is an (m,k)-source for any $k \le m\frac{\log\beta_{\min}}{\log 2} - \log_2\varkappa$.

For the next step, we turn to the theory of randomness extractors developed in the 1980s by Chor, Goldreich, Cohen, Wigderson, Zuckerman and many others (c.f., Refs. 25 and 26). The basic idea is, given a sufficiently random binary vector of length m, $X \in \{0,1\}^m$, find a possibly smaller integer n, $n \le m$, and an extractor function Ext mapping from $\{0,1\}^m$ into $\{0,1\}^n$, such that $Y = \mathsf{Ext}(X)$ is (nearly) uniformly distributed in $\{0,1\}^n$. To formalize this idea further, we say that a random variable Y taking values in $\{0,1\}^n$ is ε-close to the uniform distribution $\mathbb{U}_n$ on $\{0,1\}^n$ if the distribution $\mathbb{P}_Y$ of Y satisfies

$$d_{\mathrm{TV}}(\mathbb{P}_Y,\mathbb{U}_n) = \frac{1}{2}\sum_{w\in\{0,1\}^n}|\mathbb{P}_Y(w) - 2^{-n}| < \varepsilon,$$

where d_{TV} is the total variation metric. Unfortunately, a simple argument (e.g., Ref. 27) shows that it is not possible to construct a universal extractor, capable of producing an output bit, which is ε-close to uniform, $\varepsilon < 1/2$, for all random vectors with $X \in \{0,1\}^m$ with large min-entropy $\mathbf{H}_\infty(X) \ge m-1$. Indeed, suppose that such an extractor $\mathsf{Ext}: \{0,1\}^m \to \{0,1\}$ exists. Let

$$S_0 = \{x \in \{0,1\}^m : \mathsf{Ext}(x) = 0\} \quad \text{and}$$
$$S_1 = \{x \in \{0,1\}^m : \mathsf{Ext}(x) = 1\}.$$

Note also, that since $S_0 \cup S_1 = \{0,1\}^m$, one of the sets S_0 and S_1 has cardinality at least 2^{m-1}. Suppose for simplicity that $|S_0| \ge 2^{m-1}$ and consider a random element X_0, which is uniformly distributed on S_0. Then $\mathbf{H}_\infty(X_0) \ge m-1$. However, $Y = \mathsf{Ext}(X_0) = 0$ identically, and hence Y is not ε-close to $\mathbb{U}_1$.

Hence, given a random (m,k)-source X, in order to construct an extractor $\mathsf{Ext}: \{0,1\}^m \to \{0,1\}^n$ such that $Y = \mathsf{Ext}(X)$ is ε-close to uniform, more information on the distribution of X is needed than only a lower bound on the min-entropy. Writing $X: \Omega \to \{0,1\}^m$ for the first m bits of the β-encoder and as before $\Omega = [\beta_{\min},\beta_{\max}]^{\mathbb{N}} \times [0,1]$, to get more insight into the distribution $\mathbb{P}_m(\cdot) = \rho\times\lambda(X^{-1}(\cdot))$ beyond min-entropy would require at least a better understanding on the sets $X^{-1}(c_1^m)$ and further assumptions on ρ. However, even if we know more about the sets $X^{-1}(c_1^m)$ and ρ, finding Ext such that $\mathsf{Ext}(X)$ is ε-close to uniform would still be very involved and most probably not practical, since this problem in principle is even more difficult than a weakened version of the problem of Lochs' Theorem generalized from $([0,1],\lambda)$ to $(\Omega,\rho\times\lambda)$.

Indeed, more generally, if $X: \Omega \to \{0,1\}^m$ is a random vector, note that any function $\mathsf{Ext}: \{0,1\}^m \to \{0,1\}^n$ gives a random vector $Y: \Omega \to \{0,1\}^n$ satisfying, for each $c_1^m \in \{0,1\}^m$,

$$X^{-1}(c_1^m) \subseteq Y^{-1}(a_1^n) \tag{20}$$

(compare with (12)) where $a_1^n = \mathsf{Ext}(c_1^m)$ by setting, for each $\omega \in \Omega$,

$$Y(\omega) = \mathsf{Ext}(X(\omega)). \tag{21}$$

Conversely, any $Y: \Omega \to \{0,1\}^n$ such that for each $c_1^m \in \{0,1\}^m$ there exists $a_1^n \in \{0,1\}^n$ such that (20) holds, defines by setting $\mathsf{Ext}(c_1^m) = a_1^n$ a function $\mathsf{Ext}: \{0,1\}^m \to \{0,1\}^n$ that satisfies (21) for each $\omega \in \Omega$. Hence, constructing an extractor for which the output bits have distribution ε-close to uniform and for which the number $n = n(m)$ of output bits grows as the number m of input bits $X = X_m$ grows implies the weaker[c] result of finding $Y_n: \Omega \to \{0,1\}^n$ for each n such that

(i) $\mathbb{P}_{Y_n}(\cdot) = \mathbb{P}(Y_n^{-1}(\cdot))$ is ε-close to $\mathbb{U}_n$ for each n,
(ii) for each m and $c_1^m \in \{0,1\}^m$ there is n and $a_1^n \in \{0,1\}^n$ such that $X_m^{-1}(c_1^m) \subseteq Y_n^{-1}(a_1^n)$ with $n \to \infty$ as $m \to \infty$,

[c]Indeed, note that in (ii) the n depends not only on m but on c_1^m as well.

where $\mathbb{P}$ is the underlying probability measure on Ω under consideration. In the case where $X_m : \Omega \to \{0,1\}^m$ are the first m bits of the β-encoder and as before $(\Omega, \mathbb{P}) = ([\beta_{\min}, \beta_{\max}]^{\mathbb{N}} \times [0,1], \rho \times \lambda)$, we see from (18) that (ii) requires that

$$\bigcup_{\boldsymbol{\beta} \in [\beta_{\min}, \beta_{\max}]^{\mathbb{N}}} \{\boldsymbol{\beta}\} \times A(\boldsymbol{\beta}, c_1^m) = X_m^{-1}(c_1^m) \subseteq Y_n^{-1}(a_1^n)$$

for certain sets $A(\boldsymbol{\beta}, c_1^m)$ that satisfy

$$A(\boldsymbol{\beta}, c_1^m) \subseteq \left[\sum_{i=1}^m \frac{c_i}{\prod_{j=1}^i \beta_j}, \sum_{i=1}^m \frac{c_i}{\prod_{j=1}^i \beta_j} + \frac{\varkappa}{\prod_{j=1}^m \beta_j} \right].$$

In general, there does not seem to be an obvious choice of Y_n's that satisfy both (i) and (ii) and their construction would depend on the in principle unknown ρ. (As we saw before, setting each $Y_n(\boldsymbol{\beta}, x)$ to be equal to the first n digits in the base-2 representation of x would give (i) with $\mathbb{P}_{Y_n} = \mathbb{U}_n$ and (ii) with the exception that $n \to \infty$ as $m \to \infty$ only if $\beta_{\min} = \beta_{\max}$.)

Nevertheless, even though constructing the Y_n's for the β-encoder is not obvious, they do exist. Indeed, more generally it is known (see e.g., Proposition 3.9 of Ref. 28 and references therein) that for a given random (m,k)-source X, if $n \leq k - 2\log_2(1/\varepsilon) - O(1)$ and $\mathsf{Ext} : \{0,1\}^m \to \{0,1\}^n$ is chosen uniformly at random (from the 2^{m+n} possibilities), then $Y = \mathsf{Ext}(X)$ is ε-close to $\mathbb{U}_n$ with probability $1 - 2^{-\Omega(2^k \varepsilon^2)}$. Here $f(x) = O(g(x))$ (respectively, $\Omega(g(x))$) is the usual big-O (respectively, big-Ω) notation meaning that $f(x)$ grows asymptotically not faster (respectively, slower) than $g(x)$. This shows that, for a fixed distribution ρ on $[\beta_{\min}, \beta_{\max}]^{\mathbb{N}}$, mapping the first m bits of the β-encoder under a randomly chosen function $\mathsf{Ext} : \{0,1\}^m \to \{0,1\}^n$ with $n \leq m \frac{\log \beta_{\min}}{\log 2} - 2\log_2(1/\varepsilon) - O(1)$ gives n bits with a nearly uniform distribution with high probability (if $\beta_{\min}^{-m} \varkappa^{-1} \ll \varepsilon^2$). Unfortunately, this result is nonconstructive and also gives no indication whether extractors exist that can be computed e.g., in time polynomial in m. Fortunately, one can turn to the so-called seeded randomness extractors.

Definition 4.1 ((k,ε)-extractor, Ref. 29). A function $\mathsf{Ext} : \{0,1\}^m \times \{0,1\}^d \to \{0,1\}^n$ is a (k,ε)-extractor if for every random vector $X \in \{0,1\}^m$ with min-entropy at least k, $Y = \mathsf{Ext}(X, Z)$ is ε-close to uniform, when Z is uniformly distributed on $\{0,1\}^d$. An extractor is *explicit* if it is computable in polynomial time.

A (k,ε)-extractor, if it exists, is able to take an arbitrary sufficiently random input X (measured in terms of its min-entropy), and, hopefully, a relatively short uniformly distributed random seed Z, to produce a nearly uniformly distributed output. The principal question is under which conditions on m, d, k, n, and ε, a seeded extractor exists. There are numerous results of such nature. Let us recall the following:

Theorem 4.1 (Theorem 1.5, Ref. 29). *For every constant $\alpha > 0$, and all positive integers n, k and all $\varepsilon > 0$, there is an explicit construction of a (k,ε)-extractor $\mathsf{Ext} : \{0,1\}^m \times \{0,1\}^d \to \{0,1\}^n$ with $d = O(\log m + \log(1/\varepsilon))$ and $n \geq (1-\alpha)k$.*

Taking into account that the distribution of digits produced by the β-encoder has min-entropy at least of the order of $m \frac{\log \beta_{\min}}{\log 2}$, the above theorem states that we can produce $n = (1-\alpha) m \frac{\log \beta_{\min}}{\log 2}$ of nearly uniformly distributed binary digits $(a_1, \ldots, a_n)$. Equivalently, we need $m = \frac{1}{1-\alpha} n \frac{\log 2}{\log \beta_{\min}}$ output bits of the random β-encoder to obtain n binary well-distributed bits.

One can compare this result with the result of Theorem 1.1, which states that we would need at least $n \frac{\log 2}{\log \beta}$ output bits of the β-encoder, while the more robust universal randomness extractor would require $\frac{1}{(1-\alpha)} n \frac{\log 2}{\log \beta}$, i.e., only a fixed fraction more. Thus, the price we have to pay is rather small since the bits are produced by a relatively cheap circuit working at high clock frequency. Therefore, switching from a specific extraction scheme based on entropy encoding suggested by Jitsumatsu *et al.*[15] to a universal randomness extractor does not constitute a significant limitation.

However, the important point we have not yet taken into account is the need to use a relatively short, but "purely random", seed of length $d = O(\log m + \log(1/\varepsilon))$. In practice, one does not have access to such sources of "pure randomness". Fortunately, weak sources of randomness, such as β-encoders, can be used as seeds as well. This brings us to the discussion of extractors with weak random seeds. In Ref. 27, the following definition of two-sources-extractors is given.

Definition 4.2 (Two-Sources-Extractor, Ref. 27). A function $\mathsf{Ext} : \{0,1\}^{m_1} \times \{0,1\}^{m_2} \to \{0,1\}^n$ is an $[(m_1,k_1),(m_2,k_2) \mapsto n \sim \varepsilon]$-two-sources-extractor if for every (m_1,k_1) source X_1 and every independent (m_2,k_2)-source X_2, the distribution of the random variable $\mathsf{Ext}(X_1,X_2)$ is ε-close to $\mathbb{U}_n$ (i.e., the uniform distribution over $(\{0,1\}^n)$).

Similarly, one can define source extractors for any number of sources $\ell \geq 2$,

$$\mathsf{Ext} : \{0,1\}^{m_1} \times \{0,1\}^{m_2} \times \cdots \times \{0,1\}^{m_\ell} \to \{0,1\}^n$$

such that the extractor $\mathsf{Ext}(X_1,\ldots,X_\ell)$ is ε-close to $\mathbb{U}_n$ for all independent $(m_1,k_1),\ldots,(m_\ell,k_\ell)$-sources $(X_1,\ldots,X_\ell)$.

The theory of multiple source extractors was actively developed in the past 25 years. It turns out that there is a significant difference between the cases $\ell = 2$ and $\ell \geq 3$. The case $\ell = 2$ is substantially more complicated. It is indeed possible to construct good, efficient two-source extractors, say for $m_1 = m_2 = m$ with the min-entropy of at least $\frac{1}{2}m$.

Theorem 4.2 (Ref. 30). *For every constant $\delta > 0$ there is a constant $C > 0$ such that for large enough m, setting $k = (1/2+\delta)m$ and $\varepsilon \leq 2^{-\log^4 m}$ there is an explicit $[(m,k),(m,k) \mapsto n \sim \varepsilon]$-two-source extractor $\mathsf{Ext} : \{0,1\}^m \times \{0,1\}^m \to \{0,1\}^n$ for $n = 2k - C\log(1/\varepsilon)$.*

In our case, given the bound on min-entropy (19), that would necessarily imply that we need an extra assumption that

$$\beta_{\min} > \sqrt{2}.$$

It is not immediately clear whether such a restriction would constitute a serious limitation for applications, but it is clear that such an a priori assumption would be undesirable. On the other hand, if one turns to randomness extractors for ℓ weak sources with $\ell \geq 3$, assumptions on $\beta_{\min}$ can be relaxed. Barak *et al.*[31] showed using techniques from additive combinatorics that for any $\delta > 0$, there exist randomness extractors requiring only $\ell = \mathrm{poly}(1/\delta)$ independent $(m,\delta m)$-sources, where poly is some polynomial function. It means that assuming that $\beta_{\min} > 1$, i.e., $\beta_{\min} = 1 + \tilde{\delta}$ for some $\tilde{\delta} > 0$ is sufficient. These results were further improved by Raz[27] who showed that $\ell = 3$ is indeed sufficient.

The final point of discussion is whether one could get $\ell > 1$ independent weak sources of randomness. This could be achieved by running the β-encoder several times, or, running it once, generating a very long series of bits $N \gg 1$, and then extracting strings of length m, with sufficiently large gaps between them.

Acknowledgment

We would like to thank Yutaka Jitsumatsu for valuable discussions.

ORCID

Charlene Kalle https://orcid.org/0000-0002-3178-996X
Evgeny Verbitskiy https://orcid.org/0000-0002-4049-5197
Benthen Zeegers https://orcid.org/0000-0001-6142-9140

References

1. P. Erdös, I. Joó and V. Komornik, Characterization of the unique expansions $1 = \sum_{i=1}^{\infty} q^{-n_i}$ and related problems, *Bull. Soc. Math. France* **118**(3) (1990) 377–390.
2. N. Sidorov, Almost every number has a continuum of β-expansions, *Amer. Math. Monthly* **110**(9) (2003) 838–842.
3. I. Daubechies, R. A. DeVore, C. S. Güntürk and V. A. Vaishampayan, Beta expansions: A new approach to digitally corrected A/D conversion, *Proc. IEEE Int. Symp. Circ. Syst.* **2** (2002) 784–787.
4. I. Daubechies, R. A. DeVore, C. S. Güntürk and V. A. Vaishampayan, A/D conversion with imperfect quantizers, *IEEE Trans. Inform. Theory* **52**(3) (2006) 874–885.
5. I. Daubechies, S. Güntürk, Y. Wang and Ö. Yılmaz, The golden ratio encoder, *IEEE Trans. Inform. Theory* **56**(10) (2010) 5097–5110.
6. I. Daubechies and Ö. Yilmaz, Robust and practical analog-to-digital conversion with exponential precision, *IEEE Trans. Inform. Theory* **52**(8) (2006) 3533–3545.
7. D. Jiménez and Y. Wang, The $\beta\alpha$-encoders for robust A/D conversion, *Acta Appl. Math.* **107**(1–3) (2009) 313–323.
8. T. Kohda, Y. Horio and K. Aihara, Beta-expansion attractors observed in a/d converters, *Chaos* **22** (2012) 047512.

9. T. Kohda, Y. Horio, Y. Takahashi and K. Aihara, Beta encoders: Symbolic dynamics and electronic implementation, *Int. J. Bifur. Chaos Appl. Sci. Eng.* **22**(9) (2012) 1230031.
10. T. Makino, Y. Iwata, K. Shinohara, Y. Jitsumatsu, M. Hotta, H. San and K. Aihara, Rigorous estimates of quantization error for A/D converters based on beta-map, *Nonlinear Theory Appl., IEICE* **6**(1) (2015) 99–111.
11. H. San, T. Kato, T. Maruyama, K. Aihara and M. Hotta, Non-binary pipeline analog-to-digital converter based on beta-expansion, *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **E96.A**(2) (2013) 415–421.
12. R. Ward, On robustness properties of beta encoders and golden ratio encoders, *IEEE Trans. Inform. Theory* **54**(9) (2008) 4324–4334.
13. Y. Jitsumatsu and K. Matsumura, A β-ary to binary conversion for random number generation using a β encoder, *Nonlinear Theory Appl., IEICE* **7** (2016) 38–55.
14. Y. Jitsumatsu, K. Matsumura, T. Kohda and K. Aihara, Pseudo-random number generator using beta-encoder cmos circuit, *The 3rd Int. Symp. Innovative Mathematical Modelling* (Tokyo, 2013) p. 107.
15. I. Koji and Y. Jitsumatsu, Random number generation using outputs from multiple beta encoders, in *Proc. NOLTA 2016*, 27–30 November 2016, Yugawara, Japan, pp. 249–252.
16. Y. Shu, Y. Jitsumatsu and K. Oda, Performance evaluation of a random number generation using a beta encoder, in *2015 Int. Symp. Nonlinear Theory and its Applications, NOLTA2015*, 1–4 December 2015, Kowloon, Hong Kong, China, pp. 511–514.
17. A. Rukhin, J. Soto, J. Nechvatal, M. Smid and E. Barker, A statistical test suite for random and pseudorandom number generators for cryptographic applications, Technical Report, Booz-Allen and Hamilton, Inc. McLean VA (2001).
18. G. Lochs, Vergleich der Genauigkeit von Dezimalbruch und Kettenbruch, *Abh. Math. Sem. Univ. Hamburg* **27** (1964) 142–144.
19. K. Dajani and A. Fieldsteel, Equipartition of interval partitions and an application to number theory, *Proc. Amer. Math. Soc.* **129**(12) (2001) 3453–3460.
20. W. Bosma, K. Dajani and C. Kraaikamp, Entropy and counting correct digits, Technical Report 9925, University of Nijmegen (1999), http://www-math.sci.kun.nl/math/onderzoek/reports/reports1999.html.
21. C. Kalle, E. Verbitskiy and B. Zeegers, Random Lochs' theorem, *Studia Math.* **208**(1) (2022) 11–29.
22. K. Dajani and M. de Vries, Measures of maximal entropy for random β-expansions, *J. Eur. Math. Soc.* **7**(1) (2005) 51–68.
23. A. Herczegh, Central limit theorems in ergodic theory, Master's thesis, Eötvös Loránd University (2009).
24. É. Charlier and C. Cisternino, Expansions in Cantor real bases, *Monatsh. Math.* **195**(4) (2021) 585–610.
25. L. Trevisan, Extractors and pseudorandom generators, *J. ACM* **48**(4) (2001) 860–879.
26. A. Wigderson, *Mathematics and Computation: A Theory Revolutionizing Technology and Science* (Princeton University Press, 2019).
27. R. Raz, Extractors with weak random seeds, in *Proc. Thirty-Seventh Annual ACM Symp. Theory of Computing, STOC '05* (ACM, New York, 2005), pp. 11–20.
28. E. Chattopadhyay, J. Goodman and M. Gurumukhani, Extractors for polynomial sources over $\mathbb{F}_2$, in *15th Innovations in Theoretical Computer Science Conference (ITCS 2024)* (Schloss-Dagstuhl-Leibniz Zentrum für Informatik, 2024), pp. 28:1–28:24.
29. V. Guruswami, C. Umans and S. Vadhan, Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes, *J. ACM* **56**(4) (2009) 1–34.
30. R. Shaltiel, How to get more mileage from randomness extractors, *Random Struct. Algorithms* **33**(2) (2008) 157–186.
31. B. Barak, R. Impagliazzo and A. Wigderson, Extracting randomness using few independent sources, in *45th Annual IEEE Symp. Foundations of Computer Science* (IEEE, 2004), pp. 384–393.