A Novel Technique for Generation of Correlated Bit Sequences with Application to Gaussian Channels

Micael Andrade Dias, Juliana Martins de Assis and Francisco M. de Assis

***Abstract*— There are many applications to random sequences of bits, such as in computer science and cryptography. In this paper, we propose a low-complexity technique for generating sequences of correlated or uncorrelated bits. This technique allows the generation of different pairs of bits with the same correlation, as also controls if the bits are equiprobable on $\{0, 1\}$ or not. Additionally, we derived an expression and a numerical approximation to the performance of a binary symmetric channel obtained from the binary expansion of transformed Gaussian correlated random variables, which is related to a recently proposed scheme for quantum key distribution with continuous variables. Simulation of this binary symmetric channel agrees with the obtained expression and numerical approximation.**

***Keywords*— Binary expansion, Sampling, BSC.**

I. Introduction

Random sequence of bits are used in many applications. As examples, we mention complex numerical simulations, as seen in references [10], [12]. Moreover, distributed simulation of random variables are necessary in quantum computing and theoretical computer science [11]. The simulation of correlated Bernoulli vectors and its posterior summation has also applications in biology, where single nucleotide polymorphisms are involved with the risk of certain diseases [7]. Correlated bit streams are especially necessary in the context of stochastic computing [8], [1], and in cryptography [6].

Both real random processes and deterministic systems may produce random (or pseudorandom) sequences of bits [9]. For example, some papers propose the use of chaotic maps for a pseudorandom bit generation [3], [9]. Other papers propose using circuits and semiconductor lasers [10], [8], or even vacuum field fluctuations of an eletromagnetic field [12] to generate a random sequence of bits.

Mathematically speaking, a sequence of correlated bits may be undestood as the realization of a multivariate Bernoulli vector. We must notice, however, that given fixed marginal Bernoulli distributions, not all correlation matrices of the corresponding multivariate Bernoulli vector are possible [5]. The general correlation structure between any pair of random variables has been exploited in Fréchet-Hoeffding bounds, where any achievable correlation is a convex combination between these bounds. Specifically, there is a convexity parameter $\lambda \in [0, 1]$ which assumes value one when the upper correlation bound is achieved [4].

Interestingly, there is an important connection between arbitrary multivariate distributions and multivariate Bernoulli distributions. Assume the existence of a certain convexity parameter λ between a pair of random variables from a random vector with fixed marginals. Then, this value λ is possible if and only if there exists the same convexity parameter λ for a pair of Bernoulli variables (where the Bernoulli marginals have mean 1/2)[4, Theorem 2, p.604]. Thus, the problem of creating a sequence of correlated Bernoulli variables is equivalent to the more general problem of creating a random vector from other multivariate distributions.

When considering specially the context of cryptography, a random sequence of bits is essential, since the security of a cryptographic scheme must rely on its key. Recently, a new protocol for continuous variable quantum key distribution was developed by the authors, namely, Distributional Transform Expansion (DTE) [2]. The idea of this protocol is to use the copula theory to perform a transformation in the random variables in the input and in the output of the Gaussian channel. Also, the protocol expands these transformed random variables in a binary basis. The generated bits from this expansion are related as if they were input and output from binary symmetric channels (BSC).

In this paper, we address two main topics. Firstly, we propose a new method for generating random sequences of bits, with specific correlations between them. The method consists in generating a continuous random variable with support in the interval $[0, 1]$, respresenting it in its binary form (numeral-2 base) and then taking a number of binary digits after the point as the Bernoulli sample. For instance if the trial equals 0.72 we take this binary form $0.101110\ldots$ and the size 6 sample is $\{1, 0, 1, 1, 1, 0\}$. Despite the fact that our method does not allow for arbitrary correlations between any pair of bits, as will be shown in the simulations, it presents some interesting properties: (i) existence regions of equal (or nearly equal) correlations between different pairs of bits, (ii) low implementation complexity and (iii) parametrization by the distribution. By controlling, for example, the beta distribution parameters α and β, it is possible to control not only the correlations between some pairs of bits, but also if the generated bits are uniformly distributed on $\{0, 1\}$ or not.

Secondly, we evaluate the performance of a BSC obtained from the DTE protocol. Both topics are related to the binary expansion of random variables. However, the first topic deals with a single random variable, and determines how the Bernoulli variables achieved from its binary expansion are

Micael Andrade Dias, QuIIN - Quantum Industrial Innovation, Centro de Competência Embrapii Cimatec. SENAI CIMATEC, Salvador-BA, e-mail: micael.dias@fieb.org.br; Juliana Martins de Assis, Department of Statistics - Center for Exact and Natural Sciences, Federal University of Pernambuco, Recife-PE, e-mail: juliana@de.ufpe.br; Francisco M. de Assis, Department of Electrical Engineering, Federal University of Campina Grande, Campina Grande-PB, e-mail: fmarcos@dee.ufcg.edu.br. This work was partially supported by CNPq (311680/2022-4) and by Fundação de Amparo à Ciência e Tecnologia do Estado de Pernambuco -FACEPE (APQ-1341-1.02/22).

correlated. On the other hand, the second topic is more directly related to communication systems, dealing with two different, but correlated, random variables, and how the BSC obtained from their binary expansion performs.

The rest of the paper is organized as follows. Section II introduces some definitions that will be useful for obtaining the results, which are presented in Section III and in Section IV. Section V presents some simulations that corroborate with our findings in the previous sections. Finally, Section VI concludes the paper and presents directions for future work.

II. Preliminaries

Here we introduce some definitions that will be useful for the remaining of the text. Firstly, let X be a continuous random variable with probability density function f_X and support on $[0,1]$. A binary expansion of X with n bits precision will partition the unit interval in 2^n disjoint subsets of same length. If we write the n-bit binary expansion of $X \in [0,1]$ as $X = 0.B_1B_2\cdots B_n$ such that $X = \sum_{i=1}^{n} B_i(\frac{1}{2})^i$, one has that the values of the bits are

$$B_1 = \begin{cases} 0, & \text{if } X < 1/2, \\ 1, & \text{if } X \geq 1/2, \end{cases}$$

$$B_2 = \begin{cases} 0, & \text{if } X \in [0,1/4) \cup [1/2,3/4), \\ 1, & \text{if } X \in [1/4,1/2) \cup [3/4,1], \end{cases}$$

and for any positive integer i of the binary expansion we have:

$$B_i = \mathbb{I}\{X \in \cup_{j=1}^{2^{i-1}} [2^{-i}\cdot(2j-1), 2^{-i}\cdot 2j)\}, \tag{1}$$

where $\mathbb{I}\{A\}$ is the indicator function of an event A, which equals 1 when A occurs and 0 otherwise.

In Figure 1 we exemplify how the binary expansion works and the corresponding bit values for $n = 3$. Each possible $x \in [0,1]$ is contained in one of the partitions and is represented by a unique n-bit binary sequence.

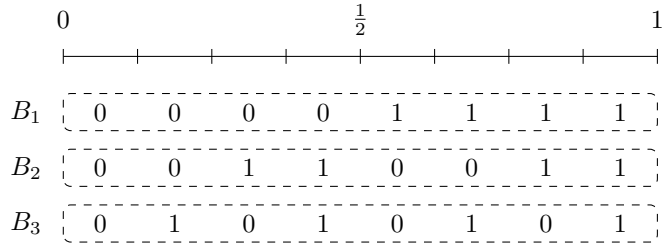

Fig. 1: Unit interval partition according to a 3-bit binary expansion and the bits corresponding values.

Two questions naturally arise: what is the distribution of B_i and are they correlated? Clearly, $B_i \sim Bern(p_i)$ and p_i and $\text{cor}(B_i, B_j)$ depends on the choice of f_X, but in which conditions $p_i = \frac{1}{2}$ and $\text{cor}(B_i, B_j) = 0$? In the next two propositions we prove statements about how X must be distributed in order to give the desired correlated (or uncorrelated) distributions of B_i. For the sake of clarity in the following arguments, let us define that a symmetric probability density function of a random variable X around $\frac{1}{2}$ as a function $f_X : [0,1] \to \mathbb{R}$ such that for any $\varepsilon \in [0, \frac{1}{2}]$, $f_X(\frac{1}{2} - \varepsilon) = f_X(\frac{1}{2} + \varepsilon)$.

III. Conditions for Symmetry and Independency

Here we present two propositions about the sequence of bits generated by the binary expansion of the realization of a random variable with support on $[0,1]$.

Proposition 1: The bits in the n-bit binary expansion of a continuous random variable X with probability density function f_X and support on the unit interval are $Bern(1/2)$ for any $n \in \mathbb{N}$ if and only if f_X is symmetric around $1/2$.

Proof: ($\rightarrow$) Let us define the family $\{A^n\}_{n\geq 1}$ of collections of disjoint subsets of $[0,1]$ of length 2^{-n}:

- $A^1 = \{[0,1/2), [1/2,1]\}$,
- $A^2 = \{[0,1/4), [1/4,1/2), [1/2,3/4), [3/4,1]\}$

and so on. Note that $\bigcup_{A\in A^n} A = [0,1]$ for any n. Let us also enumerate the subsets in A^n from 1 to n. Then, the n-th bit in the binary expansion of x informs whether x lies in an even of odd numbered subset of A^n:

- Odd numbered subset of A^n: $b_n = 0$,
- Even numbered subset of A^n: $b_n = 1$.

Now, define A_0^n and A_1^n as the set of odd and even (respectively) numbered subsets in A^n. Then, if f_X is symmetric around $\frac{1}{2}$,

$$\int_{A_0^n[j]} f_X(x)dx = \int_{A_1^n[2^{n-1}-j+1]} f_X(x)dx, \tag{2}$$

where $j = 1, \cdots, 2^{n-1}$. Also, we have that

$$\Pr[B_n = 0] = \Pr[X \in \bigcup_{j=1}^{2^{n-1}} A_0^n[j]] \tag{3}$$

$$= \sum_{j=1}^{2^{n-1}} \int_{A_0^n[j]} f_X(x)dx \tag{4}$$

$$= \sum_{j=1}^{2^{n-1}} \int_{A_1^n[2^{n-1}-j+1]} f_X(x)dx \tag{5}$$

$$= \Pr[X \in A_1^n] = \Pr[B_n = 1]. \tag{6}$$

Then, $\Pr[B_n = 0] = \Pr[B_n = 1] = \frac{1}{2}$ if f_X is symmetric around $\frac{1}{2}$.

($\leftarrow$) To show that the bits in the binary expansion are $Bern(\frac{1}{2})$ only if f_X is symmetric around $\frac{1}{2}$, assume that f_X is not symmetric around $\frac{1}{2}$. Then, there exists an ε such that $f_X(\frac{1}{2} - \varepsilon) \neq f_X(\frac{1}{2} + \varepsilon)$. Also, there is some $n \geq 1$ and at least one $j \in \{1, 2, \cdots, 2^{n-1}\}$ such that

$$\int_{A_0^n[j]} f_X(x)dx \neq \int_{A_1^n[2^{n-1}-j+1]} f_X(x)dx. \tag{7}$$

Then, $\Pr[B_n = 0] = \Pr[B_n = 1] = \frac{1}{2}$ only if f_X is symmetric around $\frac{1}{2}$. ∎

Example 1: Consider X a random variable that follows the trapezoidal distribution, where $f_X(x)$ is illustrated in Figure 2 and $D - C = \frac{1}{4}$ is fixed. Consider also that $0 \leq C \leq \frac{3}{4}$. In the binary expansion of X, the probability $Pr[B_1 = 1] = Pr[X \geq \frac{1}{2}] = 1 - F_X(\frac{1}{2})$, which is a function of the value of C. In Figure 3 we plotted the probabilities $Pr[B_i = 1]$ for the case of a binary expansion with $n = 2$. We can see that both bits are equiprobable when $C = \frac{3}{8}$, that is, the f_X is symmetric around $\frac{1}{2}$.

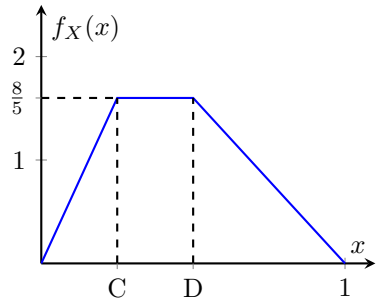

Fig. 2: Trapezoidal Distribution.

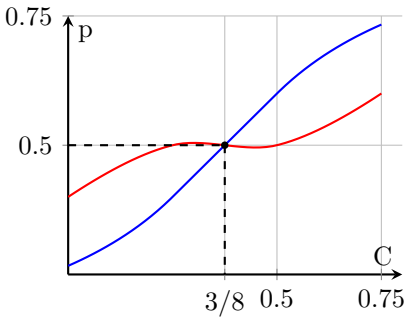

Fig. 3: Bit probabilities $Pr[B_1 = 1]$ (blue) and $Pr[B_2 = 1]$ (red) in the binary expansion of the trapezoidal distribution as a function of C.

Proposition 2: The bits in the n-bit binary expansion are independent if $f_X = \mathcal{U}(0,1)$.

Proof: ($\rightarrow$) Assume that $f_X = \mathcal{U}(0,1)$. Now consider an n-bit binary expansion of x drawn from X. Each possible n-bit sequence corresponds to an interval of length 2^{-n}. Since $X \sim \mathcal{U}(0,1)$ by hypothesis, the n-bit sequences are equiprobable: $p(b_1, \cdots, b_n) = 2^{-n}$. For any two $i, j = 1, \cdots, n$, $i \neq j$, we have that

$$p(b_i, b_j) = \sum_{\sim b_i, b_j} p(b_1, \cdots, b_n) = (2^{n-2}) \cdot 2^{-n} = \frac{1}{4}. \quad (8)$$

Then, by factoring $p(b_i, b_j) = p(b_j|b_i)p(b_i)$ and by Proposition 1 ensuring that $b_i \sim Bern(\frac{1}{2})$ for any $i > 0$,

$$\frac{1}{4} = p(b_j|b_i)\frac{1}{2} \rightarrow p(b_j|b_i) = \frac{1}{2} = p(b_j), \quad (9)$$

from which we conclude that if $X \sim \mathcal{U}(0,1)$ then the bits in the binary expansion are pairwise independent. ■

IV. From Gaussian to Binary Symmetric Channels

In this Section we address the performance of a BSC derived from the binary expansion of correlated Gaussian variables. Consider the Gaussian channel model:

$$Y = X + \sqrt{N}Z \quad X, Z \sim \mathcal{N}(0,1), \quad X \perp Z, \quad (10)$$

where we observe that the signal-to-noise ratio and correlation coefficient are given by

$$SNR = \frac{1}{N} = \gamma \quad (11)$$

$$\rho(X,Y) = \rho_{XY} = \frac{1}{\sqrt{1+N}} \quad (12)$$

Define the random variables as in [13, ch.13]

$$U \equiv F_X(X), \qquad V \equiv F_Y(Y) \quad (13)$$

and consider their binary basis numerical expansions

$$U = \sum_{i=1}^{\infty} U_i 2^{-i}, \qquad V = \sum_{i=1}^{\infty} V_i 2^{-i} \quad (14)$$

By the lemma of distribution we know that $U \sim \mathcal{U}(0,1)$ and similarly V [13]. Also from the results (Proposition 2) $\{U_i\}$ is a i.i.d. Bern$(1/2)$ and similarly it holds for $\{V_i\}$. Although, as $\rho_{XY} > 0$, $N > 0$, the correlation $\rho_{U_iV_i}$ can be calculated for the $i-$th BSC channel induced by the binary numerical expansion of X and Y (see Fig. 4) $U_i \longleftrightarrow V_i$ by

$$\rho_{U_iV_i} = 2(1-\alpha_i) - 1 \quad (15)$$

where $\alpha_i \equiv \Pr[V_i \neq U_i]$.

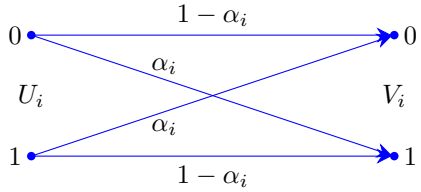

Fig. 4: Binary Symmetric Channel (BSC). $C = 1$ bit/use

For now on, we take $i = 1$ (the first "BSC"). The following sequence holds

$$\begin{aligned}
\alpha_1 &= \Pr[V_1 \neq U_1] && (16)\\
&= \Pr[V_1 = 1, U_1 = 0] + \Pr[V_1 = 0, U_1 = 1] && (17)\\
&= 2\Pr[V_1 = 1, U_1 = 0] && (18)\\
&= 2\Pr[V_1 = 1 | U_1 = 0] \times \frac{1}{2} && (19)\\
&= \Pr[V_1 = 1 | U_1 = 0]. && (20)
\end{aligned}$$

Now, back to the Gaussian channel, consider the equivalent events:

$$\begin{aligned}
D &= \left\{V_1 = 1 | U_1 = 0\right\}\\
&\equiv \left\{F_Y(Y) > \frac{1}{2} | F_X(X) \leq \frac{1}{2}\right\} && (21)\\
&\equiv \left\{F_Y(X + \sqrt{N}Z) > \frac{1}{2} | F_X(X) \leq \frac{1}{2}\right\} && (22)\\
&\equiv \left\{X + \sqrt{N}Z > 0 | X \leq 0\right\} && (23)\\
&\equiv \left\{\sqrt{N}Z > -X | X \leq 0\right\} && (24)\\
&\equiv \left\{Z > -X/\sqrt{N} | X \leq 0\right\}. && (25)
\end{aligned}$$

Notice that the event D probability depends on X and Z being itself a random variable. Therefore, the BSC transition probability must be calculated by the average

$$\begin{aligned}\alpha_1 &= \mathbb{E}\Pr[D] && (26)\\ &= \int_{-\infty}^{0} 2Q\left(\frac{-x}{\sqrt{N}}\right)\frac{1}{\sqrt{2\pi}}e^{-x^2/2}dx && (27)\\ &\overset{(a)}{=} 2\int_{0}^{\infty} Q\left(\frac{v}{\sqrt{N}}\right)\frac{1}{\sqrt{2\pi}}e^{-v^2/2}dv, && (28)\end{aligned}$$

where (a) is justified by change of variable $v = -x$. An approximation for integral (28) and its generalization can be given recalling that [14, p.83]:

$$Q(x) \leq \frac{1}{2}e^{-\frac{x^2}{2}}, \quad (29)$$

which, replaced in last expression for α_1 yields:

$$\begin{aligned}\alpha_1 &\leq 2\int_{0}^{\infty}\frac{1}{2}e^{-\frac{v^2}{2N}}\frac{1}{\sqrt{2\pi}}e^{-v^2/2}dv\\ &= \int_{0}^{\infty}\frac{1}{\sqrt{2\pi}}e^{-\frac{1}{2}\left(1+\frac{1}{N}\right)v^2}dv\end{aligned}$$

Defining $\nu = \sqrt{\frac{1}{1+1/N}}$ and multiplying and dividing the right hand by this we obtain

$$\begin{aligned}\alpha_1 &\leq \nu\int_{0}^{\infty}\frac{1}{\sqrt{2\pi}\nu}e^{-\frac{v^2}{2\sigma^2}}dv\\ &= \frac{1}{2}\sqrt{\frac{N}{1+N}}\\ &= \frac{1}{2}\sqrt{\frac{1}{1+SNR}}\end{aligned}$$

where the last line we observe that $SNR = \frac{1}{N}$ according the model $Y = X + \sqrt{N}Z$ for the Gaussian channel. We note that, consistently, if $SNR \to 0$, the transition probability goes near one half.

V. Simulations

Here we present some simulations relative to the results in Sections III and IV. For the first topic addressed in this paper, i.e. the generation of correlated bits, can evaluate the covariance between bits when the probability density function $f_X(x)$ is symmetric around $1/2$, which can be computed as

$$\begin{aligned}\text{cov}(B_i, B_j) &= \mathbb{E}(B_iB_j) - \mathbb{E}(B_i)\mathbb{E}(B_j)\\ &= \mathbb{E}(B_iB_j) - \frac{1}{4}\\ &= Pr[B_i = 1, B_j = 1] - \frac{1}{4} \quad (30)\end{aligned}$$

It is clear that if X has uniform distribution on $[0, 1]$, the generated bits from an outcome of X are independent and thus their correlation is null. In general, for any $f_X(x)$ with support on $[0, 1]$ and considering a 3-bit binary expansion, we have:

$$Pr[B_1 = 1, B_2 = 1] = \int_{\frac{3}{4}}^{1} f_X(x)dx, \quad (31)$$

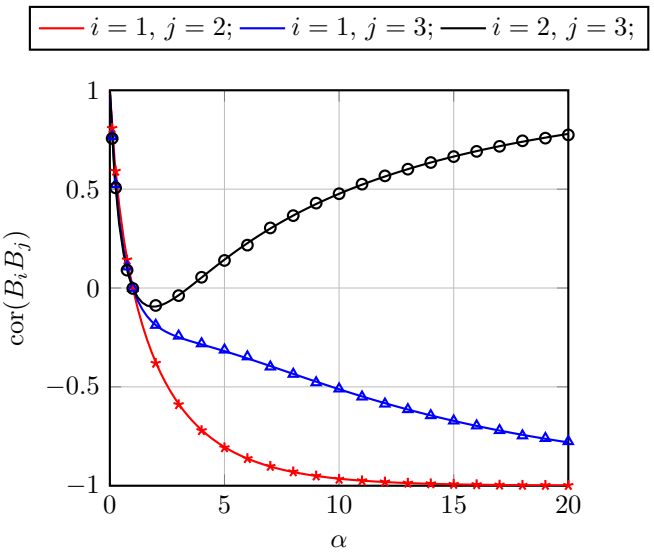

Fig. 5: Pairwise theoretical (continuous) and estimated (dots, triangles and stars) correlations of bits obtained from binary expansion of beta random variable. The beta distribution parameters are set to $\alpha = \beta$.

$$Pr[B_1 = 1, B_3 = 1] = \int_{\frac{5}{8}}^{\frac{6}{8}} f_X(x)dx + \int_{\frac{7}{8}}^{1} f_X(x)dx, \quad (32)$$

$$Pr[B_2 = 1, B_3 = 1] = \int_{\frac{3}{8}}^{\frac{1}{2}} f_X(x)dx + \int_{\frac{7}{8}}^{1} f_X(x)dx. \quad (33)$$

When $f_X(x)$ is symmetric around $1/2$, since the bits are $Bern(\frac{1}{2})$, the correlation between any pair of bits is given by $\text{cor}(B_i, B_j) = 4 \cdot \text{cov}(B_i, B_j)$, which are elements of the correlation matrix ρ.

In Fig. 6 we plotted the theoretical values of correlations obtained by applying the binary expansion to outcomes from beta and trapezoidal distributions with symmetric settings. The symmetry in the distributions is guaranteed by setting $\alpha = \beta$ in the beta distribution, and in the trapezoidal one, $C = \frac{1}{2} - \Delta$ and $D = \frac{1}{2} + \Delta$. We obtained not only the mathematical values of correlation between bits in a 3-bit binary expression, but we also provided estimates of correlation coefficients. Specifically, we simulated 10^5 outcomes of a beta distribution, for each parameter α in $\{0.1, 0.25, 0.75, 1, 2, 3, \ldots, 20\}$. For the trapezoidal distribution we sampled 10^5 outcomes for each Δ ranging 10 equally spaced values from 0 to 0.5.

In Figure 5 and 6, the red curves refer to the correlation between B_1 and B_2, the blue curves refer to the correlation between B_1 and B_3 and the black curves refer to the correlation between B_2 and B_3. We observe from Figure 5 that setting α with values inside $[0, 1]$ results in bits, in a 3-bits binary expasion, that have approximately the same correlation, considering any pair of bits. A similar result occurs when setting $\Delta \in [0.4, 0.5]$ in the trapezoidal distribution, as seen in Figure 6.

Now, for the second topic addressed in this paper, we calculated the expressions in Equation (28). We also simulated pairs of correlated Gaussian variables and observed the BSC

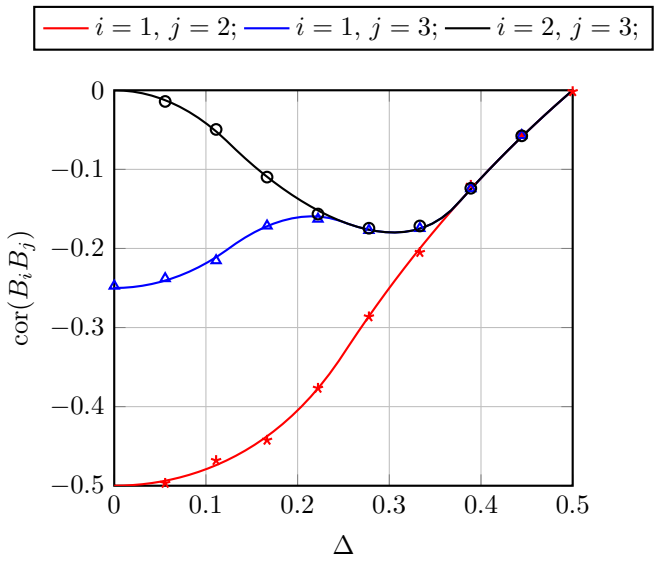

Fig. 6: Pairwise theoretical (continuous) and estimated (dots, triangles and stars) correlations of bits obtained from binary expansion of trapezoidal random variables. The trapezoidal distribution is symmetric around $\frac{1}{2}$ with upper basis equal to Δ.

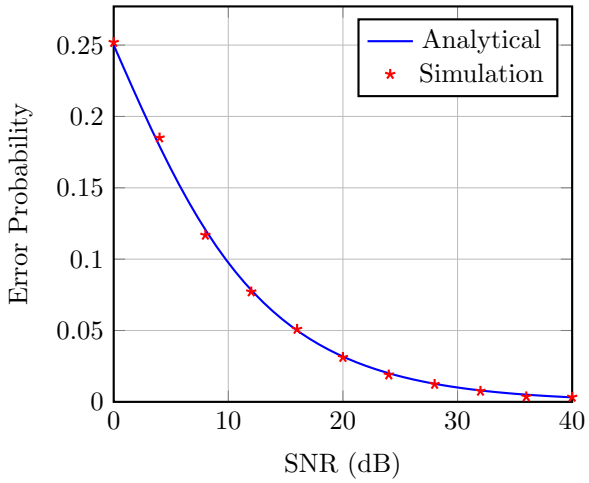

Fig. 7: Bit error probability for the simulated BSC (red dots) and the analytical solution (blue curve) to given by expression the in Equation (28).

obtained as explained before. Fig. 7 shows the results. Notice that error probability in simulation agrees with Equation (28).

VI. Conclusions

In this paper we explored two main topics: how to develop sequences of correlated or uncorrelated Bernoulli variables and how a binary symmetric channel, induced by the binary expansion of two "DTE" transformed Gaussian correlated variables, performs. In the first topic, we proposed a method for sampling Bernoulli variables from the binary expansion of a unit support interval random variable X, obtaining a low complexity procedure that enables pairs of bits with the same correlation, in accordance with the parameters of the density f_X. In the second topic, we obtained an approximation to the bit error probability of the BSC achieved from a Gaussian channel. As expected, this bit error probability approaches 1/2 as the SNR diminishes. As future work, we may evaluate how other BSC obtained from "DTE" transformed Gaussian variables perform (that is, BSCs obtained for the second, third and generally for the n-th bit in the binary expansion procedure).

Aknowledgements

We thank Rávilla Silva and Andresso Silva for the contributions with the computer simulations and implementing the analytical results. This work was supported in part by the National Council for Scientific and Technological Development (CNPq) under research Grant No. 305918/2019-2, the Coordination of Superior Level Staff Improvement (CAPES/PROEX), EMBRAPII and the Brazilian Ministry for Science, Technology and Innovation - MCTI.

References

[1] Yan Chen, Jinyo Wen, and Shijie Cheng. "Probabilistic Load Flow Method Based on Nataf Transformation and Latin Hypercube Sampling". 4(2):294–301, April 2013.

[2] Micael Andrade Dias and Francisco Marcos de Assis. Distributional transform based information reconciliation. *Journal of Communication and Information Systems*, 39(1):74–81, May 2024.

[3] Chunyan Han. An image encryption algorithm based on modified logistic chaotic map. *Optik*, 181:779–785, 2019.

[4] Mark Huber and Nevena Marić. Multivariate Distributions with Fixed Marginals and Correlations. *Journal of Applied Probability*, 52(2):602–608, June 2015.

[5] Mark Huber and Nevena Marić. Admissible Bernoulli correlations. *Journal of Statistical Distributions and Applications*, 6(1):2, December 2019.

[6] Md Saiful Islam. Using ecg signal as an entropy source for efficient generation of long random bit sequences. *Journal of King Saud University-Computer and Information Sciences*, 34(8):5144–5155, 2022.

[7] Winfield Lai. *Methods to Simulate Correlated Binomial Random Variables*. PhD thesis, 2021.

[8] Yin Liu, Megha Parhi, Marc D Riedel, and Keshab K Parhi. Synthesis of correlated bit streams for stochastic computing. In *2016 50th Asilomar Conference on Signals, Systems and Computers*, pages 167–174. IEEE, 2016.

[9] Lazaros Moysis, Aleksandra Tutueva, Christos Volos, Denis Butusov, Jesus M Munoz-Pacheco, and Hector Nistazakis. A two-parameter modified logistic map and its application to random bit generation. *Symmetry*, 12(5):829, 2020.

[10] N. Oliver, M. C. Soriano, D. W. Sukow, and I. Fischer. Fast random bit generation using chaotic laser: approaching the information theoretic limit. *IEEE Journal of Quantum Electronics*, 49:910–918, 2013.

[11] Madhu Sudan, Himanshu Tyagi, and Shun Watanabe. Communication for generating correlation: A unifying survey. *IEEE Transactions on Information Theory*, 66(1):5–37, 2019.

[12] Thomas Symul, Syed Muhamad Assad, and Ping K Lam. Real time demonstration of high bitrate quantum random number generation with coherent laser light. *Applied Physics Letters*, 98(23):231103, 2011.

[13] Joy A. Thomas Thomas M. Cover. *Elements of Information Theory*. Wiley John & Sons, 2006.

[14] J. M. Wozencraft and I. M. Jacobs. *Principles of Communication Engineering*. John Wiley & Sons, New York, 1965.