TRUE RANDOM NUMBER GENERATION VIA SAMPLING FROM BAND-LIMITED GAUSSIAN PROCESSES

by

Necmettin Caner Gov

B.Sc. Electrical & Electronics Engineering, Bilkent University, 2007

Submitted to the Institute for Graduate Studies in
Science and Engineering in partial fulfillment of
the requirements for the degree of
Master of Science

Graduate Program in Electrical & Electronics Engineering, Bogazici University

Boğaziçi University

2010

TRUE RANDOM NUMBER GENERATION VIA SAMPLING FROM BAND-LIMITED GAUSSIAN PROCESSES

APPROVED BY:

Assoc. Prof. M. Kivanc Mihcak .....
(Thesis Supervisor)

Assoc. Prof. Murat Saraçlar .....

Assist. Prof. A. Taylan Cemgil .....

DATE OF APPROVAL: .....05.07.2010.....

ACKNOWLEDGEMENTS

I am forever indebted to my parents who have shown me foremost financial and sentimental support and understanding throughout my entire period of study at Boğaziçi University. Without their support this thesis would not be possible.

I also would like to thank my advisor Dr. Mihcak for his support throughout this thesis and Dr. Saraçlar and Dr. Cemgil for examining this thesis.

ABSTRACT

TRUE RANDOM NUMBER GENERATION VIA SAMPLING FROM BAND-LIMITED GAUSSIAN PROCESSES

A true random number generator topology based on regular sampling of an "irregular" process is considered, which is obtained via thresholding a continuous-time Gaussian (normal) process, of which spectrum is assumed to be flat between two known frequencies and zero everywhere else. Per-sample joint entropy of the resulting bit sequence is introduced as the main figure of merit. Employing an approach based on statistical signal processing and information theory, novel analytical results on the optimum choice of the sampling period is presented that ensure maximal randomness of the resulting bit sequence together with asymptotic analysis and numerical experiments. In addition, new results that fully characterize the autocorrelation behavior (equivalently spectral properties) of the resulting bit sequence is presented and a related metric, termed "spectral correlation" is introduced to quantify the "uncorrelatedness" of the binary bit sequence output.

ÖZET

SINIRLI BANT GENİŞLİĞİNDEKİ GAUSS RASTGELE SÜREÇLERDEN ÖRNEKLEYEREK GERÇEK RASTGELE SAYI ÜRETİMİ

Düzensiz bir rastgele süreçten düzenli örnekleyerek rastgele sayı üreten bir sistem topolojisi incelenmektedir. Bu sistem geniş anlamda durağan Gauss dağılımlı ve iki bilinen frekans arasında düz haricinde sıfır değerli spektrumu olan bir rastgele süreci kaynak olarak kullanır. Örnek başına bileşik entropi asli başarım göstergesi olarak kullanılmaktadır. Örnekleme periyodunun en uygun seçimiyle ilgili azami rastgelelik sağlayan, istatistiksel işaret işleme ve bilgi kuramına dayalı yeni analitik sonuçlar asimptotik ve numerik deneylerle beraber sunulmaktadır. Ek olarak, elde edilen bit dizisinin özilinti davranışı (eşdeğer olarak spektral güç dağılımına bağlı özellikleri) üzerine yeni sonuçlar sunulmakta ve yeni ilgili bir metrik olan "spektrumsal ilinti" ikili bit dizisi çıktısının "ilintisizliğini" ölçmek amacıyla kullanılmaktadır.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS/ABBREVIATIONS

A	Lower cutoff frequency of $S_S(f)$
B	Upper cutoff frequency of $S_S(f)$
$C_Z(k)$	Autocovariance sequence of Z_n
$C(t)$	Binary process that results from thresholding $KS(t)$
$H^b(.)$	Binary entropy function
H_N	Per sample joint entropy of a sequence of discrete random variables of length N
k	Autocovariance lag index
K	Amplifier gain
n	Discrete time index
$N(t)$	Amplifier output
N_0	Twice the power spectral density amplitude of $S(t)$ in flat region
$q(\tau)$	Probability that $Z_n = 1$
$\mathbb{R}$	The set of real numbers
$R_N(u)$	Autocorrelation function of $N(t)$
$R_S(u)$	Autocorrelation function of $S(t)$
$R_X(k)$,$R_Y(k)$	Autocorrelation sequences of arbitrary wide sense stationary random processes X_n,Y_n
$\|\{s\}\|$	Cardinality of an arbitrary set s
$S(t)$	Naturally occuring random process
$S_N(f)$	Power Spectral Density of $N(t)$
$S_S(f)$	Power Spectral Density of $R_S(u)$
$S_X(\omega)$,$S_Y(\omega)$	Power spectral densities of processes X_n,Y_n
T_s	Sampling period
V	High voltage level
$\mathbf{W}$	Random vector obtained from the realizations of W_n
$\tilde{W}_n$	White random process that is closest to W_n

W_n	Equivalent discrete time random process obtained by uniformly sampling $N(t)$
$W_n \sim \mathcal{N}(\mu, \sigma^2)$	W_n has a Gaussian distribution with mean μ and variance σ^2
X_n,Y_n	Arbitrary discrete time real valued random processes
Z_n	Discrete time discrete valued binary output random process of the flip-flop indexed by discrete time n
$\mathbb{Z}$	The set of all integers
$\mathbb{Z}^+$	The set of all positive integers
$\delta_C(.)$	Continuous time delta function
$\delta_D(.)$	Continuous time delta function
θ_{X_n,Y_n}	Spectral correlation between X_n,Y_n
η	Twice the upper cutoff sampling period product
κ	Ratio of lower cutoff frequency to upper cutoff frequency
ρ_k	Correlation coefficient of the Gaussian random variables W_n, W_{n-k}
Σ_{ij}	Covariance matrix of $\mathbf{W}$ indexed by integers i, j
τ	Thresholding level
ω	Radian frequency
$\mathbb{1}_{\{.\}}$	Indicator function

BFGS	Band-limited Flat Gaussian Spectrum
DFT	Discrete Fourier Transform
diag	Diagonal matrix
i.i.d.	Independent and Identically Distributed

1. Introduction

Nowadays, because of the increasing demand on electronic official & financial transactions and digital signature applications, the need for information secrecy has increased. In this manner, random number generators (RNGs), which have been used primarily for military cryptographic applications in the past, got expanding usage for a typical digital communication equipment.

Almost all cryptographic systems require unpredictable values, therefore RNG is a fundamental component for cryptographic mechanisms. Generation of public/private key-pairs for asymmetric algorithms and keys for symmetric and hybrid crypto systems require random numbers. The one-time pad, challenges, nonces, padding bytes and blinding values are created using "true random number generator"s (TRNGs) [1]. "Pseudo-random number generator"s (PRNGs) generate bits using a deterministic algorithm of which state is determined by a seed. In order to appear to be generated by a TRNG, the pseudo-random sequences must be seeded from a shorter truly random sequence [2]. Random numbers are also used during the authentication procedure between two crypto equipments and initial value randomization of a crypto module that realizes an algorithm.

In the ideal case, a TRNG design should be carried out in such a way that, even if the design itself is publicly known, the output bit sequence should possess certain unpredictability properties. Ideally, for "perfect secrecy", a bit sequence should be "truly random", i.e., the output bits should be independent identically distributed Bernoulli-1/2 random variables. In practice, certain figures of merit that measure secrecy or true-randomness are utilized.

In most practical applications, to fulfill the requirements for secrecy of one-time pad, key generation and any other cryptographic applications, the TRNG must satisfy the following properties: The output bit stream of the TRNG must

pass all the statistical tests of randomness; the next random bit must be unpredictable; the same output bit stream of the TRNG should be irreproducible [3]. The best way to generate truly-random numbers is to exploit the natural randomness of the real world by finding a random event that happens regularly [3]. Examples of such a usable event include elapsed time during radioactive decay, thermal and shot noise, oscillator jitter and the amount of charge of a semiconductor capacitor [2].

There are a number integrated circuit (IC) RNG designs reported in the literature. In general, the techniques that exploit natural randomness to generate random numbers can be classified into (at least) four different categories: amplification of a noise source followed by thresholding [4, 5], jittered oscillator sampling [1, 6, 7], discrete-time chaotic maps [8–10] and continuous-time chaotic oscillators [11, 12].

Among all the RNGs, the most widely-used type utilizes the method of amplification of a noise source followed by thresholding, which effectively can be viewed as *regular sampling of random processes followed by* 1*-bit quantization*. A theoretical analysis of this approach under some certain assumptions constitutes the main topic of this thesis. Publications on this topic (RNGs via regular sampling of random processes) in the literature mostly involve practical device implementations and experimental results; while, notable exceptions that involve analytical investigation of the underlying setup include [13–16, 18], which are reviewed next.

In [13], Murry considers an underlying Gaussian noise source, of which spectrum is flat between two frequencies and zero everywhere else. Then, he analyzes a circuit topology, where random bits are produced from the noise via one-bit quantization. He introduces a rule of thumb for the quantification of the maximum sampling rate using the average number of zero-axis crossings of the underlying noise waveform. In particular, he provides an estimate of the maximum sampling

rate as 1.155 times the noise-band lowpass cutoff frequency.

In [14], Sokal uses the same model for the underlying noise waveform and the same circuit topology as Murry, but concentrates on the correlation function of the clipped waveform (output of the quantizer). Hence, Sokal analyzes the resulting continuous-time binary-valued stochastic process and presents results that show how to choose the optimum passband cutoff frequencies for a specified sampling rate and a maximum allowed bit-to-bit correlation.

In [15], Boyes also uses the bandlimited flat-spectrum Gaussian noise model, like [13] and [14]. Boyes' circuit topology, however, can be viewed as an extended "digitized" version of the one considered in [13, 14]: the underlying noise source is first passed through a one-bit quantizer, thereby producing the clipped waveform, subsequently followed by the application of a modulo-2 divider (such as a flip-flop) so as to remove the errors in the mean value. Similar to [14], Boyes treats the modulo-2 divider output as a continuous-time binary-valued stochastic process and analyzes its autocorrelation function in order to quantify the performance while assuming the transition times between the binary states are independent.

In [16], Morgan considers a similar, but more general setup than the above. He assumes that the underlying noise source is Gaussian, of which spectrum can be arbitrary; a bit sequence is generated via sampling the noise at regular time intervals, subsequently followed by applying the sign $(\cdot)$ function. Morgan focuses on the computational aspects of the per sample joint-entropy of the resulting bit sequence; he presents closed-form expressions for sequences of length-2 and length-3; for longer sequences, he obtains second-order results, which are used to obtain numerical results for various covariance matrices of interest.

More recently, in [18], Bucci *et. al.* assume that the underlying noise source is Gaussian white and they present results that quantify the autocorrelation function of the resulting bit sequence. They incorporate the frequency response of the

noise amplifier and the high pass filter due to the utilized offset zeroing system in the analysis. They obtain their analytical results via relating the autocorrelation functions of discrete-time wide sense stationary sequences before and after thresholding.

In this thesis, similar to [13–15], it is assumed that the underlying noise waveform is a continuous-time wide sense stationary Gaussian (normal) process, of which spectrum is flat between two known frequencies; the terminology "*B*andlimited *F*lat-*S*pectrum *G*aussian (normal) (BFSG) noise" is used to indicate such a process [1] . In a nutshell, new results are presented for true random number generators, that are based on sampling of BFSG noise sources using probabilistic and information theoretic measures together with analytical results that act as guidelines on the optimum choice of the sampling period that will yield the highest possible entropy of the generated bit sequence. Hence, analogous to the aforementioned prior art, a circuit topology is considered, which produces a binary bit sequence via sampling (at regular time intervals) the output of a comparator, of which input is an amplified version of an underlying naturally-occurring BFSG noise. Per-sample entropy is utilized as the main figure of merit and accordingly is used to investigate the randomness properties of the resulting binary sequence; furthermore it shall be argued that the approach in [13–15, 17] and [18] which uses the correlation between successive generated bits as the criteria for randomness (the lower the magnitude of the correlation the higher the randomness of the generated output sequence) is not a strong indicator of randomness because, it does not necessarily imply the independence of the bit sequence when it is zero whereas per sample joint entropy does when it achieves the independence bound on it. As long as the generated bits are dependent their conditional entropy is less than their marginal entropy which makes them predictable to some extent as stated in *Fano's Inequality* [19]. The reader is referred to texts such as [19] for fundamental information theoretic results. Main contributions of this thesis can

[1] In general, although the BFSG model may not perfectly fit a naturally-occurring noise process, it is possible to apply analog filters so as to flatten or pre-whiten the original noise spectrum, thereby justifying the utilized model.

be outlined as follows:

- It is shown that the aforementioned original circuit topology is equivalent to regular sampling of the input noise source, subsequently followed by thresholding (cf. Sec. 2.2) and a novel figure of merit the "spectral correlation" that yields a numerical output for quantifying how well the power spectral densities of two discrete time random processes are related (cf. Sec. 2.3) is introduced.
- Assuming the BFSG model on the input noise source, analytical conditions on the sampling period are quantified, which guarantee that the produced binary bit sequence achieve maximal randomness; numerical and asymptotical results on the loss in entropy when the sampling period is suboptimal is also presented (cf. Sec. 3); a similar procedure is carried out in case of low pass flat-spectrum Gaussian noise sources (cf. Sec. 4).
- Based on the BFSG model on the input noise source, the autocovariance sequence of the resulting binary bit sequence is quantified as well as numerical results for the spectral correlation between the power spectral density of an arbitrary zero mean, wide sense stationary, white Gaussian process and the power spectral density of the regularly sampled input noise source which is obtained by using the equivalent setup that is introduced in Sec. 2.2 (cf. Sec. 5).

In Sec. 2, the original problem is stated, an equivalent framework for analysis is developed, the utilized performance criteria to quantify randomness and mention the low pass approximation on the BFSG model is introduced. The fundamental analytical results (including asymptotical approximation) for the BFSG case (resp. low pass approximation case), together with supporting numerical results, are presented in Sec. 3 (resp. Sec. 4). Next, analytical and numerical results to quantify the autocovariance sequence and spectral behavior are provided in Sec. 5, followed by conclusions and future work in Sec. 6.

2. Problem Statement

In this section, an overview of the problems that are going to be investigated is provided and the fundamental assumptions and figures of merit that will be used in the rest of the thesis are presented. Sec. 2.1 entails the overall block diagram and the governing equations of the conventional circuitry that is used in the literature such as [4, 5] which is depicted along with the explicit statement of the functional form of the "BFSG noise" power spectrum and the corresponding autocorrelation function. The following Sec. 2.2, introduces a novel mathematically equivalent approach to the conventional setup in order to make the analysis of the problem more tractable. In order to quantify the performance of the RNG, the per sample joint entropy and achievable bounds on it are defined along with the necessary and sufficient conditions in Sec. 2.3; furthermore, a metric namely the "spectral correlation" is introduced that provides a quanta of the relation between the power spectral densities of two arbitrary real wide sense stationary processes $\{X_n\}, \{Y_n\}$. The significance of this metric will be justified in Section 5. The assumption that the entire noise spectrum is white up to the high cut-off frequency B is made in Sec. 2.4 and thus the lowpass approximation to the general case is presented, where its use is justified.

2.1. Original Problem Setup

The original circuit topology being considered in this paper is depicted in Fig. 2.1. The underlying naturally-occurring process is denoted by $S(t)$, which is then amplified, thereby forming $N(t)$. It is assumed that the amplifier is ideal and acts as "multiplication with a scaling factor K" (where $K > 1$) uniformly at all range of frequencies of interest; i.e., it is assumed that $N(t) = KS(t)$ for all t. The amplified signal $N(t)$ is passed through a comparator, which acts based on a threshold τ, forming $C(t)$.

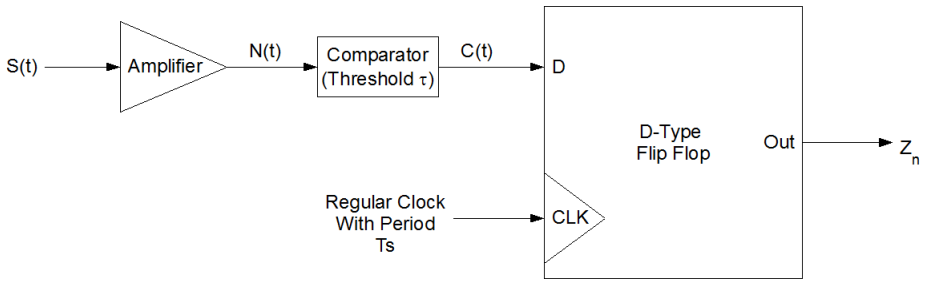

Figure 2.1. The original circuit topology investigated in this thesis.

$$C(t) = \begin{cases} V \text{ volts}, & \text{if } N(t) > \tau \\ 0 \text{ volts}, & \text{if else} \end{cases} \tag{2.1}$$

where V and 0 volts represent the values of digital 1 and 0, respectively. Then, the signal $C(t)$ is applied as input to a D-type flip flop, of which clock operates with period T_s, producing the digital binary output sequence $\{Z_n\}$, where for all n, $Z_n \in \{0, 1\}$. Hence,

$$Z_n = \begin{cases} 1, & \text{if } C(t)\Big|_{t=nT_s} = V \text{ volts}, \\ 0, & \text{if else} \end{cases} \tag{2.2}$$

It is assumed that the waveform $S(t)$ is a continuous-time zero-mean Gaussian (normal) noise process, such that

$$\begin{aligned} S_S(f) &= \mathcal{F}_c\{R_S(u)\} \\ &= \mathcal{F}_c\{\mathrm{E}[S(t)\,S(t-u)]\} \end{aligned}$$

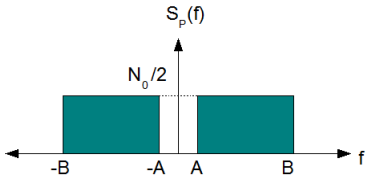

Figure 2.2. The power spectral density $S_N(f)$ of $N(t)$.

$$= \begin{cases} \frac{N_0}{2K^2} & \text{if } A < |f| < B, \\ 0 & \text{if else} \end{cases} \tag{2.3}$$

thereby justifying the usage of the term "BFSG noise" to characterize the behavior of $S(t)$. Now, since $N(t) = KS(t)$ for all t per assumption, this implies

$$S_N(f) = \begin{cases} \frac{N_0}{2}, & \text{if } A < |f| < B, \\ 0, & \text{if else} \end{cases} \tag{2.4}$$

meaning that $N(t)$ is BFSG noise as well; the power spectral density $S_N(f)$ is depicted in Fig. 2.2. Also, note that the corresponding autocovariance function is given by

$$\begin{aligned} R_N(u) &= \int_{-\infty}^{\infty} S_N(f)\, e^{j2\pi fu}\, df \\ &= \int_{-B}^{-A} \frac{N_0}{2} e^{j2\pi fu}\, df + \int_{A}^{B} \frac{N_0}{2} e^{j2\pi fu}\, df \\ &= N_0 B \text{sinc}(2Bu) - N_0 A \text{sinc}(2Au). \end{aligned} \tag{2.5}$$

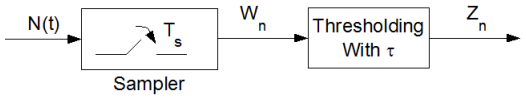

Figure 2.3. The scheme that is equivalent to the original problem setup.

Lastly, two new variables $\eta \stackrel{\triangle}{=} 2BT_s$ and $\kappa \stackrel{\triangle}{=} A/B$ are defined that will be used in the rest of the thesis.

2.2. Equivalent Problem Setup

Next, it is shown that the original problem setup introduced in Sec. 2.1 and shown in Fig. 2.1 is equivalent to the scheme shown in Fig. 2.3, based on which analysis and results presented throughout the rest of the thesis are developed.

In order to see the equivalence of Fig. 2.1 and Fig. 2.3, note that, using (2.1) in (2.2),

$$Z_n = \begin{cases} 1, & \text{if } N(t)\Big|_{t=nT_s} > \tau, \\ 0, & \text{if else} \end{cases} \tag{2.6}$$

which means that it can rewritten

$$Z_n = \mathbb{1}_{\{N(nT_s)>\tau\}} \quad \text{for all } n, \tag{2.7}$$

based on the schematic depicted in Fig. 2.1. Now, examining Fig. 2.3,

$$\left(W_n \triangleq N\left(nT_s\right) \quad \text{for all } n\right) \quad \text{and} \quad \left(Z_n = \mathbb{1}_{\{W_n > \tau\}}\right)$$

which amounts to (2.7), thereby confirming the equivalence of the two schematics.

2.3. Performance Criteria

Throughout the analysis, an information theoretic criterion is mainly used to quantify the randomness captured in the output sequence $\{Z_n\}$. Given the sequence $\left\{Z_1^N\right\}$, its per-sample joint entropy is defined $H_N \triangleq \frac{1}{N} H\left(\left\{Z_1^N\right\}\right)$ where N is the length of the sequence. Next note that the following series of inequalities hold

$$H_N = \frac{1}{N} H\left(\left\{Z_1^N\right\}\right) \leq \frac{1}{N} \sum_{n=1}^{N} H\left(Z_n\right) \leq \frac{1}{N} \sum_{n=1}^{N} \log \left| \{0,1\} \right| = 1,$$

where the first inequality is satisfied with equality if and only if $\{Z_n\}$ are independent, the second inequality is satisfied with equality if and only if all $\{Z_n\}$ are Bernoulli-1/2. Thus, the sequence $\{Z_n\}$ reach the upper bound of 1 in the sense of per-sample entropy if and only if they are i.i.d. Bernoulli-1/2, which is precisely what is desired for a truly random sequence. Hence, the goal in designing a true random number generator topology would be to achieve this upper bound; since the gap between the upper bound of 1 and per-sample entropy represents the deficiency of the system, particular concentration is put on this quantity and the analysis is based on that.

In addition, in Sec. 5, spectral properties of the resulting sequence is also concentrated on. In particular, a *novel* figure of merit is introduced, which is termed as "spectral correlation". For two given real, zero mean and wide sense stationary discrete time random processes $\{X_n, Y_n\}$ spectral correlation is the normalized inner product of the power spectral densities $S_X(\omega), S_Y(\omega)$ defined as

$$\theta_{\{X_n\},\{Y_n\}} \triangleq \frac{\int_{-\pi}^{\pi} S_X(\omega) S_Y(\omega) d\omega}{\sqrt{\int_{-\pi}^{\pi} (S_X(\omega))^2 d\omega \int_{-\pi}^{\pi} (S_Y(\omega))^2 d\omega}} \tag{2.8}$$

and it indicates how much the two power spectral densities $S_X(\omega), S_Y(\omega)$ are related.

Remark 1. *From the Cauchy-Schwarz Inequality and non-negativity of* $S_X(\omega), S_Y(\omega)$, $0 \leq \theta_{\{X_n\},\{Y_n\}} \leq 1$.

2.4. Low Pass Approximation

In [23] Van der Ziel points to the fact that flicker noise (alternatively "$1/f$ noise") in semiconductors is prevalent in extremely low frequencies and has a non-flat power spectral density. Thus, the noise source that is processed to generate the output sequence may be viewed as one with two statistically independent components, the flicker noise that spans the lowermost frequencies and the white noise that spans the entire frequency range up to the high cutoff frequency.

The dominant one however is the white noise which makes up for the most of the noise power found by integrating the power spectral density of the noise source in its support set. Consequently, the lowpass approximation is presented where it is regarded that the noise process has a flat power spectral density that is flat up to the high cutoff frequency B :

$$S_N(f) = \begin{cases} \frac{N_0}{2}, & \text{if } |f| < B \\ 0, & \text{if else} \end{cases} \tag{2.9}$$

and is shown in Fig. 2.4.

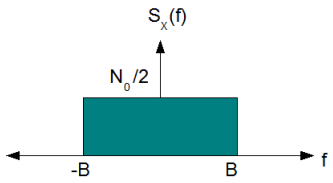

Figure 2.4. The Power Spectral Density of $S_N(f)$ of $N(t)$ for the Lowpass Approximation

3. Main Results for the General Bandlimited Flat-Spectrum Gaussian Case

Following the equivalent setup proposed in Sec. 2.2 $\{W_n\}$ are obtained from the zero mean wide sense stationary continuous time Gaussian process $N(t)$ via regular sampling. Thus, the random vector $\mathbf{W} \stackrel{\triangle}{=} [W_1, \ldots, W_N]^T$ has a multivariate Gaussian distribution with mean vector $\mu = \mathbf{0}$, covariance matrix Σ such that $\Sigma_{ij} \stackrel{\triangle}{=} N_0 B\text{sinc}((i-j)2BT_s) - N_0 A\text{sinc}((i-j)2AT_S)$ and every $\{W_n\}$ are identically distributed Gaussian random variables with distribution

$$f_{W_n}(w_n) \stackrel{\triangle}{=} \frac{1}{\sqrt{2\pi(N_0(B-A))}} \exp\left(-\frac{w_n^2}{2(N_0(B-A))}\right)$$

The output sequence is formed via thresholding $\{W_n\}$ that is given in (2.1) and (2.2). In this sense, $\{Z_n\}$ are a function of $\{W_n\}$ and identically distributed as a result. Marginal probability masses of $\{Z_n\}$ are calculated by the following

$$\begin{aligned} \Pr[Z_n = 1] &= \Pr[W_n > \tau] \\ &= \int_\tau^\infty \frac{1}{\sqrt{2\pi(N_0(B-A))}} \\ &\times \exp\left(-\frac{w_n^2}{2(N_0(B-A))}\right) dw_n \\ &\stackrel{\triangle}{=} q(\tau) \end{aligned} \tag{3.1}$$

Taking this fact into account the following proposition is made

Proposition 1. *The output sequence comprises of i.i.d. Bernoulli random variables if and only if* $\{W_n\}$ *are pairwise uncorrelated which is equivalent to their independence.*

Proof. See Appendix I. □

Corollary 1. *Under Proposition 1, the per sample joint entropy of* $\{Z_n\}$ *becomes*

$$\begin{aligned} H_N &= \frac{1}{N} H(\{Z_1^N\}) \\ &= \frac{1}{N} \sum_{n=1}^{N} H(Z_n) \\ &= \frac{1}{N} \sum_{n=1}^{N} -q(\tau) \log q(\tau) - (1 - q(\tau)) \log(1 - q(\tau)) \\ &= H^b\left(q\left(\tau\right)\right) \end{aligned} \tag{3.2}$$

(3.2) follows from the independence bound on per sample joint entropy as discussed in Sec. 2.3.

Remark 2. *From the concavity of* $H^b\left(q\left(\tau\right)\right)$ *it follows that if* $\{Z_n\}$ *are independent, having* $q(\tau) = \frac{1}{2}$ *maximizes per sample joint entropy as discussed in Sec. 2.3.*

Proposition 2. *The sequence* $\{W_n\}$ *are i.i.d. Gaussian if and only if either one of the two following conditions hold*

$$T_s \text{ is such that } 2BT_s, 2AT_s \in \mathbb{Z} \tag{3.3}$$

$$T_s \text{ is such that } (B-A)\,T_s \in \mathbb{Z} \tag{3.4}$$

Proof. See Appendix II. □

Remark 3. *(3.3) amounts to having* $(2BT_s, 2AT_s) = (\eta, \kappa\eta) \in \{\mathbb{Z}^+ \times \mathbb{Z}^+\}$ *and (3.4) amounts to having for* $k \in \mathbb{Z}^+$, $\eta = \frac{2k}{1-\kappa}$.

3.1. Asymptotic Analysis for the General Case

Having provided the necessary and sufficient conditions for generating i.i.d. Bernoulli-1/2 random variables in Propositions 1 and 2, a proposition is presented regarding the asymptotic behavior of the per sample joint entropy as η tends to infinity.

Proposition 3. *As* η *tends to infinity*

$$\lim_{\eta\to\infty} H_N = H^b(q(\tau)) \tag{3.5}$$

Proof. See Appendix III. □

3.2. Numerical Experiments for the General Case

In order to demonstrate the results of the Propositions 1 and 2, numerical results are shown for the per sample joint entropy of the output sequence versus η for the general case where the power spectral density of $N(t)$ is as defined in Sec. 2.1 and $q(\tau) = \frac{1}{2}$. Two values are used for κ, these are $\kappa = 0.1$ in Fig. 3.1 and $\kappa = 0.5$ in Fig. 3.2 respectively. Also included in the figures are the "Murry's Barrier", a vertical dashed line that corresponds to $\eta = \frac{2B}{1.155B} = 1.7316$ which is

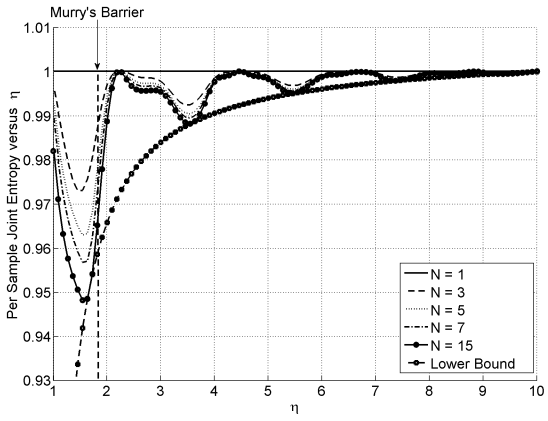

Figure 3.1. Per Sample Joint Entropy of the Output Sequence versus η for $\kappa = 0.1$

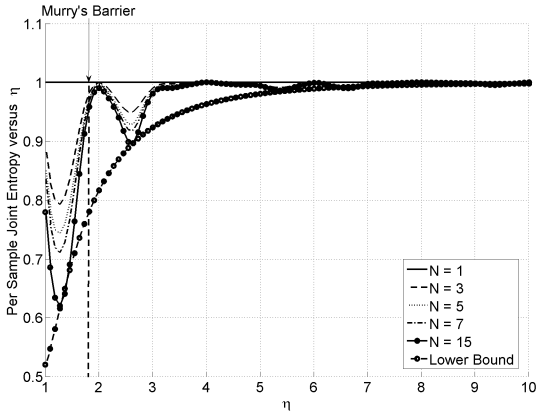

Figure 3.2. Per Sample Joint Entropy of the Output Sequence versus η for $\kappa = 0.5$

discussed in [13] that choosing the sampling period less than $\frac{1}{1.155B}$ will make a zero to one or vice versa transition in the output sequence an unlikely event.

Per Remark 3 it needs to be the case that when $\kappa = 0.1$, $\eta \in \{10, 20, 30, \ldots\} \cup \{\frac{20}{9}, \frac{40}{9}, \frac{60}{9}, \ldots\}$ and $\kappa = 0.5$, $\eta \in \{2, 4, 6, \ldots\} \cup \{4, 8, 12, \ldots\}$ in order for Proposition 2 to hold. In Figs. 3.1 and 3.2 it can be observed that these values of η make per sample joint entropy equal to unity with a certain magnitude of error introduced by numeric computation. Also observe in Figs. 3.1 and 3.2 that for a smaller κ value, the loss in per sample joint entropy is less and as η increases per sample joint entropy converges towards unity, supporting Proposition 3.

4. Main Results for the Low Pass Approximation Case

Following the results of the Secs. 3.1 and 3.2 the results for the lowpass approximation as a special case are provided. As A tends to zero, (3.3) becomes

$$T_s \text{ is such that } 2BT_s \in \mathbb{Z}^+ \tag{4.1}$$

which implies $\eta \in \mathbb{Z}^+$ on the other hand (3.4) becomes

$$T_s \text{ is such that } BT_s \in \mathbb{Z}^+ \tag{4.2}$$

so that $\frac{\eta}{2} \in \mathbb{Z}^+$ thus, $\eta = 2k,\ k \in \mathbb{Z}^+$. Consequently, for $\eta \in \{\mathbb{Z}^+ \cup \{2k,\ k \in \mathbb{Z}^+\}\} = \mathbb{Z}^+$ hence $\{W_n\}$ are i.i.d. that follows from (4.1) and (4.2).

4.1. Asymptotic Analysis for the Low Pass Case

The specialization of the results of Sec. 3.1 to the lowpass approximation case are trivial. Please see Appendix III for the proof.

4.2. Numerical Experiments for the Low Pass Case

Shown in Fig. 4.1 is the plot of the per sample joint entropy for the lowpass approximation where $q(\tau) = \frac{1}{2}$. As discussed in Sec. 4 for $\eta \in \mathbb{Z}^+$, H_N is equal to unity which is in agreement with results of Sec. 4 and as η becomes larger H_N

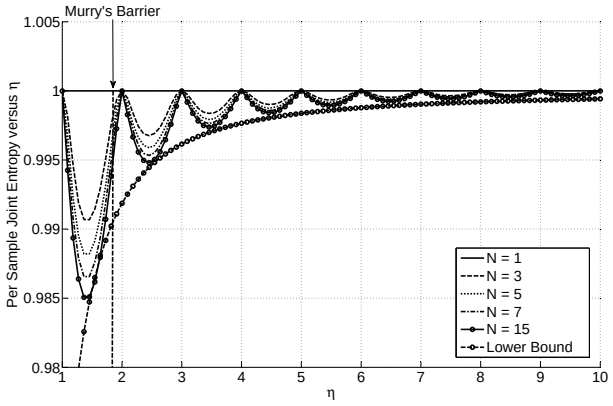

Figure 4.1. Per Sample Joint Entropy of the Output Sequence versus η for Lowpass Approximation

converges towards unity which is in agreement with the asymptotic results of Sec. 4.1.

An experiment was carried out to investigate the asymptotic behavior of per sample joint entropy. This involves fitting the third order function as a lower bound function $f_{lower}(\eta)$ shown as the bounding line from below in Figs. 3.1, 3.2 and 4.1 as follows

$$f_{lower}(\eta) \stackrel{\triangle}{=} \sum_{i=0}^{3} \alpha_i \eta^{-i} \tag{4.3}$$

and the following table of regression coefficients is obtained.

κ	a_0	a_1	a_2	a_3
0	1.004	-0.0036	-0.0207	-0.0092
0.1	1.0054	-0.0558	0.0150	-0.1247
0.5	0.9864	0.2750	-1.7177	0.9770

Table 4.1. Regression coefficients for the lower bound fitted using Eq. 4.3.

Hence it has been shown experimentally that roughly the per sample joint entropy converges towards unity in the form $H_N \approx 1 - K/\eta^3$.

5. Analysis of Autocorrelation Function and Spectral Behavior

The autocovariance sequence of the generated bits is expressed as

$$\begin{aligned} C_Z(k) &\stackrel{\triangle}{=} E[(Z_n - E[Z_n])(Z_{n-k} - E[Z_{n-k}])] \\ &= \sum_{i,j\in\{0,1\}} ij \Pr(Z_n = i, Z_{n-k} = j) \\ &- \Pr(Z_n = 1)\Pr(Z_{n-k} = 1) \\ &= \Pr(W_n > \tau, W_{n-k} > \tau) - q(\tau)^2 \end{aligned} \tag{5.1}$$

In order to have uncorrelated generated bits i.e., $C_Z(k) = 0,\ \forall k \neq 0$ it must hold that $\Pr(W_n > \tau, W_{n-k} > \tau) = q(\tau)^2$. This requires the integration of the bivariate normal distribution in the rectangular region $D \subset \mathbb{R}^2$, defined as $w_n, w_{n-k}\ :\ \forall w_n, w_{n-k} \in D;\ \tau < W_n < \infty,\ \tau < W_{n-k} < \infty\}$ which is not analytically possible. As a result numerical results are presented for $C_Z(k)$ versus ρ_k, the correlation coefficient of W_n, W_{n-k} defined as $|\rho_k \stackrel{\triangle}{=} R_W(k)/R_W(0)| \leq 1$, calculated for various $|\tau|$ values in Fig. 5.1.

Pictorially when referred to Fig. 5.1 it is seen that for large values of $|\tau|$ the bits are pairwise uncorrelated. If $C_Z(k)$ had been adopted as our figure of merit of randomness, this would imply that $|\tau|$ would have to be chosen as large as possible for generating uncorelated bits and this way $q(\tau)$ would be bounded away from $\frac{1}{2}$, implying H_N be bounded away from 1. This follows from the bound on per sample joint entropy as introduced in Sec. 2.3 and the concavity of the binary entropy function as discussed in [19]. As a consequence, relying on $C_Z(k)$ for generating truly random numbers in general is misleading in the sense that

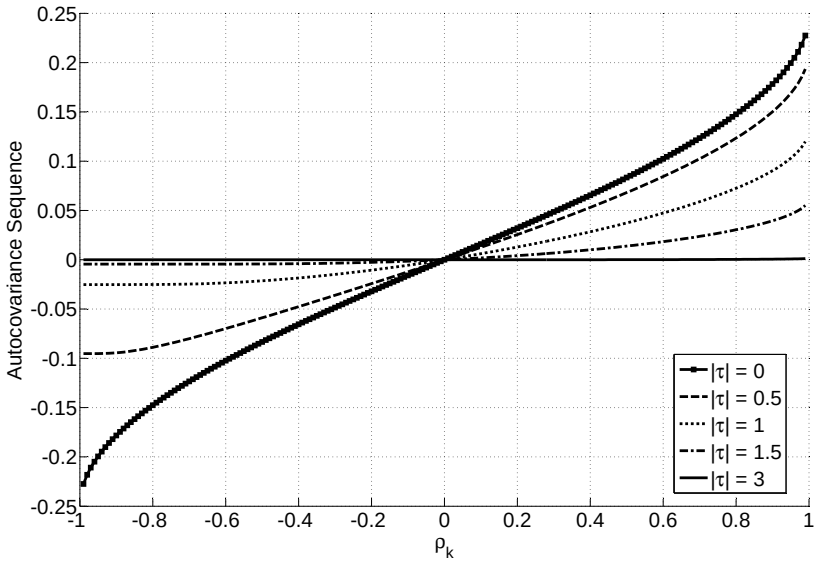

Figure 5.1. Autocovariance Sequence of Z_n versus ρ_k

having its magnitude zero is not necessarily equivalent to having $H_N = 1$ thus, attention must be confined to the case where $q(\tau) = \frac{1}{2}$ throughout the rest of this section so that the upper bound on per sample joint entropy is achievable with equality. In that case a closed form expression for (5.1) exists in [20, pp. 307]

$$-\frac{\pi}{2} < C_Z(k) = \frac{1}{2\pi} \sin^{-1}\left(\frac{R_W(k)}{R_W(0)}\right) \leq \frac{\pi}{2} \tag{5.2}$$

Also presented in Fig. 5.2 are plots of the covariance of successive bits for various κ values as given by (5.2). In the figure, for certain values of κ, the covariance of successive bits is zero while in general it exploits oscillatory behavior in κ and for increasing values of η, covariance almost vanishes.

The change in the covariance of the successive bits resulting from the change in η is a lot more dramatic than the change in κ and the output sequence is asymptotically uncorrelated $\forall k \neq 0$ as η tends to infinity which is derived analytically

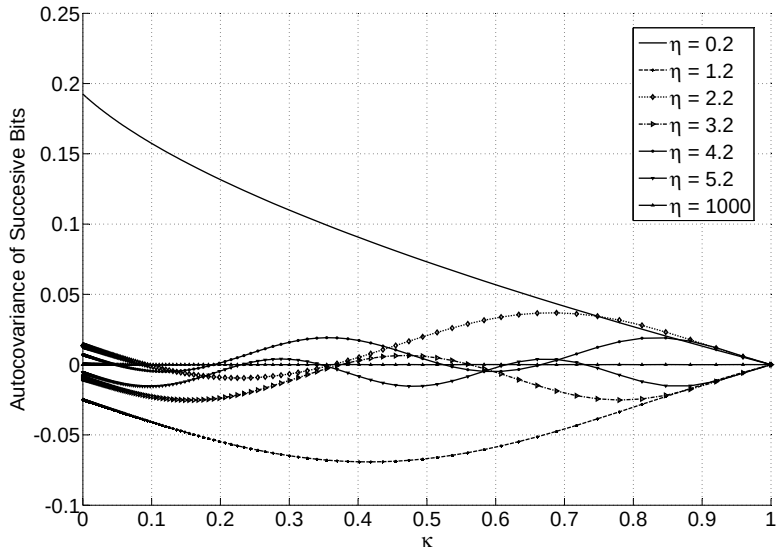

Figure 5.2. Autocovariance of Successive Bits versus κ

$$\begin{aligned}\lim_{\eta\to\infty} C_Z(k) &= \lim_{\eta\to\infty} \frac{1}{2\pi} \sin^{-1}\left(\frac{R_W(k)}{R_W(0)}\right) \\ &= \lim_{\eta\to\infty} \frac{N_0 B}{2\pi(N_0 B - N_0 A)} \sin^{-1}\left(\mathrm{sinc}(\eta k) - \kappa \mathrm{sinc}\left(\kappa\eta k\right)\right) \\ &= 0 \end{aligned} \tag{5.3}$$

(5.3) is in agreement with the previous asymptotic results that have been stated in Sec. 3.1 where it has been claimed that as $\eta \to \infty$ the generated bits are independent which implies their uncorrelatedness however, of course the converse need not be true in general.

For the result given in (5.2) the following remarks are made :

Remark 4. *For $\eta < \infty$ and $q(\tau) = \frac{1}{2}$, $C_Z(k) = 0,\ \forall k \neq 0$ whose necessary and sufficient conditions are stated in Proposition 2.*

Remark 5. *For $q(\tau) = \frac{1}{2}$ the condition $C_Z(k) = 0, \forall k \neq 0$ is equivalent to having*

$R_W(k) = 0,\ \forall k \neq 0$ in which case, the random variables $\{W_1^N\}$ are uncorrelated thus $\{Z_1^N\}$ are i.i.d. Bernoulli-1/2 random variables as stated in Proposition 1.

By Remarks 4 and 5 it is seen that in order to have independently generated bits, the condition $R_W(k) = 0,\ \forall k \neq 0$ needs to hold. In order to assert how close $R_W(k)$ is to satisfying the independence of $\{W_1^N\}$ spectral correlation between $\{W_n\}$ and $\{\tilde{W}_n\}$ is used where, $\{\tilde{W}_n\}$ is a zero mean, wide sense stationary, white Gaussian process such that $S_{\tilde{W}}(\omega) \stackrel{\triangle}{=} R_W(0)$. Firstly the two cases : $\eta \to 0$, $\eta \to \infty$ are evaluated and for intermediate values numerical results are presented.

Note that the power spectrum of W_n as η tends to zero is

$$\begin{aligned} \lim_{\eta \to 0} S_W(\omega) &= \lim_{\eta \to 0} \mathcal{F}\{R_W(k)\} \\ &= \mathcal{F}\{R_W(0)\} \\ &= R_W(0)\delta_C(\omega) \end{aligned} \tag{5.4}$$

where $\delta_C(\omega)$ is the continuous Dirac Delta Function [22, pp. 34] which is defined for $\Delta > 0$ as the limit $\delta_C(x) \stackrel{\triangle}{=} \lim_{\Delta \to 0} \delta_\Delta(x)$ where :

$$\delta_\Delta(x) = \begin{cases} \frac{1}{\Delta}, & \text{if } x < \Delta, \\ 0, & \text{if else} \end{cases} \tag{5.5}$$

Furthermore, $\delta_C(x)$ has the following properties

$$\int_{-\infty}^{\infty} \delta_C(x)dx = \lim_{\Delta\to 0} \int_{-\infty}^{\infty} \delta_\Delta(x)dx$$
$$= \lim_{\Delta\to 0} \frac{\Delta}{\Delta} \tag{5.6}$$
$$= 1 \tag{5.7}$$

and

$$\int_{-\infty}^{\infty} \delta_C(x)^2dx = \lim_{\Delta\to 0} \int_{-\infty}^{\infty} \delta_\Delta(x)^2dx$$
$$= \lim_{\Delta\to 0} \frac{\Delta}{\Delta^2}$$
$$= \infty \tag{5.8}$$

Thus, the spectral correlation between $\{\tilde{W}_n\}$ and $\{W_n\}$ as η tends to zero becomes

$$\lim_{\eta\to 0} \theta_{\{\tilde{W}_n\},\{W_n\}} = \lim_{\eta\to 0} \frac{\int_{-\pi}^{\pi} R_W(0)S_W(\omega)d\omega}{\sqrt{\int_{-\pi}^{\pi} R_W(0)^2d\omega \int_{-\pi}^{\pi} S_W(\omega)^2d\omega}}$$
$$= \frac{\int_{-\pi}^{\pi} R_W(0)^2\delta_C(\omega)d\omega}{\sqrt{\int_{-\pi}^{\pi} R_W(0)^2d\omega \int_{-\pi}^{\pi} R_W(0)^2\delta_C(\omega)^2d\omega}}$$
$$= \frac{R_W(0)^2}{R_W(0)^2\sqrt{2\pi \int_{-\pi}^{\pi} \delta_C(\omega)^2d\omega}}$$
$$= 0 \tag{5.9}$$

Next, as η tends to infinity, $S_W(\omega)$ is

$$\begin{aligned}\lim_{\eta\to\infty} S_W(\omega) &= \lim_{\eta\to\infty} \mathcal{F}\{R_W(k)\} \\ &= \mathcal{F}\{R_W(0)\delta(k)\} \\ &= R_W(0) \end{aligned} \tag{5.10}$$

so the spectral correlation as η tends to infinity becomes

$$\begin{aligned}\lim_{\eta\to\infty} \theta_{\{\tilde{W}_n\},\{W_n\}} &= \lim_{\eta\to\infty} \frac{\int_{-\pi}^{\pi} R_W(0) S_W(\omega) d\omega}{\sqrt{\int_{-\pi}^{\pi} R_W(0)^2 d\omega \int_{-\pi}^{\pi} S_W(\omega)^2 d\omega}} \\ &= \frac{\int_{-\pi}^{\pi} R_W(0)^2 d\omega}{\sqrt{\int_{-\pi}^{\pi} R_W(0)^2 d\omega \int_{-\pi}^{\pi} R_W(0)^2 d\omega}} \\ &= 1 \end{aligned} \tag{5.11}$$

Numerical results for $\theta_{\{\tilde{W}_n\},\{W_n\}}$ are presented in Fig. 5.3 for showing the behavior of $\theta_{\{\tilde{W}_n\},\{W_n\}}$ when $0 < \eta < \infty$.

Proposition 4. $\theta_{\{\tilde{W}_n\},\{W_n\}} = 1$ *if and only if* $\{W_1^N\}$ *are uncorrelated.*

Proof. See Appendix IV. □

Thus, spectral correlation achieves its lower bound as η tends to zero and the upper bound as η tends to infinity while for intermediate values, it behaves as given in Fig. 5.3. As a figure of merit $\theta_{\{\tilde{W}_n\},\{W_n\}}$ cannot be used in lieu of per sample joint entropy since it does not provide a measure of uncertainty present

in the output sequence. However, it may be used as an objective function in the sense that maximizing it is equivalent to achieving the uncorrelatedness of $\{W_n\}$ per Proposition 4 which in turn implies the independence of $\{Z_n\}$ per Proposition 1.

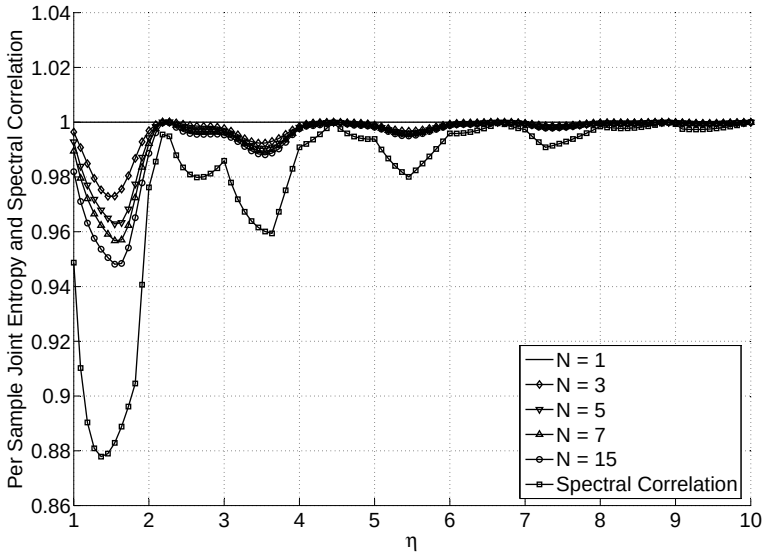

Figure 5.3. Per Sample Joint Entropy plotted together with Spectral Correlation between $\{\tilde{W}_n\}$ and $\{W_n\}$ versus η for $\kappa = 0.1$

The distance between two power spectral densities may also be measured by the Itakura-Saito distance [24, pp. 51]

$$D_{IS}(S_X(\omega), S_Y(\omega)) \triangleq \frac{1}{2\pi} \int_{-\pi}^{\pi} \left[\frac{S_X(\omega)}{S_Y(\omega)} - \log \frac{S_X(\omega)}{S_Y(\omega)} - 1 \right] d\omega \tag{5.12}$$

and the KL distance [19, pp. 19]

$$D_{KL}(S_X(\omega), S_Y(\omega)) \triangleq \int_{-\pi}^{\pi} S_X(\omega) \log \frac{S_X(\omega)}{S_Y(\omega)} d\omega \tag{5.13}$$

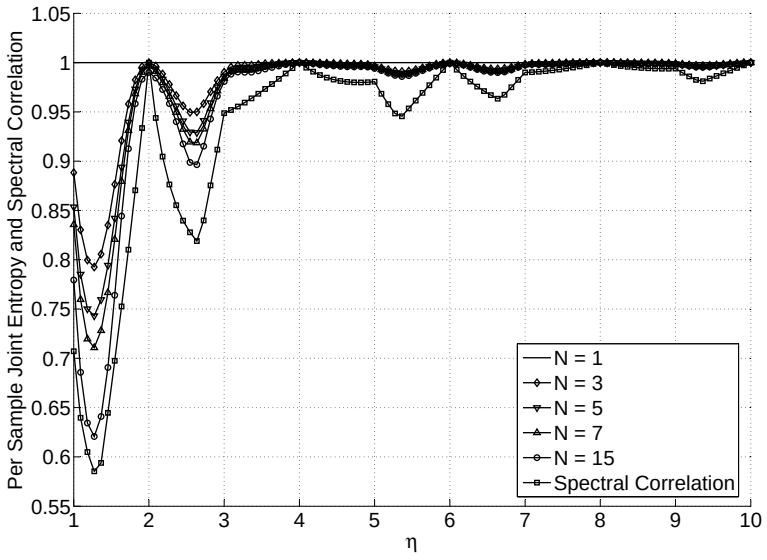

Figure 5.4. Per Sample Joint Entropy plotted together with Spectral Correlation between $\{\tilde{W}_n\}$ and $\{W_n\}$ versus η for $\kappa = 0.5$

Neither of the distances given in (5.12) and (5.13) accept interchangable parameters. However, this is not a problem with spectral correlation since spectral correlation is a legal metric and as such it satisfies the triangle inequality, symmetric with respect to a change in its parameters and also satisfies Cauchy-Schwarz inequality while on the other hand it does not use an interchange of parameters and the sole purpose of using it is to measure the whiteness of the given power spectral density. Next consider the bounds on (5.12) and (5.13) for vanishing and asymptotic η while letting $S_X(\omega) = S_W(\omega)$ and $S_Y(\omega) = R_W(0)$

$$\begin{aligned}
\lim_{\eta\to 0} D_{IS}(S_W(\omega), R_W(0)) &= \lim_{\eta\to 0} \frac{1}{2\pi}\int_{-\pi}^{\pi} \log \frac{e^{1+\frac{S_W(\omega)}{R_W(0)}}}{\frac{S_W(\omega)}{R_W(0)}} d\omega \\
&= \frac{1}{2\pi}\int_{-\pi}^{\pi} \log \frac{e^{1+\delta_C(\omega)}}{\delta_C(\omega)} d\omega \\
&= \lim_{\Delta\to 0} \frac{1}{2\pi}\int_{0}^{\Delta} \log \frac{e^{1+\frac{1}{\Delta}}}{\frac{1}{\Delta}} d\omega \\
&= \lim_{\Delta\to 0} \frac{\Delta}{2\pi} \log \frac{e^{1+\frac{1}{\Delta}}}{\frac{1}{\Delta}}
\end{aligned}$$

$$= \infty \tag{5.14}$$

$$\begin{aligned}
\lim_{\eta\to\infty} D_{IS}(S_W(\omega), R_W(0)) &= \lim_{\eta\to\infty} \frac{1}{2\pi}\int_{-\pi}^{\pi}\left[\frac{S_W(\omega)}{R_W(0)} - \log\frac{S_W(\omega)}{R_W(0)} - 1\right] \\
&= \frac{1}{2\pi}\int_{-\pi}^{\pi}\left[\frac{R_W(0)}{R_W(0)} - \log\frac{R_W(0)}{R_W(0)} - 1\right] \\
&= 0
\end{aligned} \tag{5.15}$$

$$\begin{aligned}
\lim_{\eta\to 0} D_{KL}(S_W(\omega), R_W(0)) &= \lim_{\eta\to 0}\int_{-\pi}^{\pi} S_X(\omega)\log\frac{S_X(\omega)}{S_Y(\omega)}d\omega \\
&= \int_{-\pi}^{\pi} R_W(0)\delta_C(\omega)\log\frac{R_W(0)\delta_C(\omega)}{R_W(0)}d\omega \\
&= \lim_{\Delta\to 0}\int_{0}^{\Delta} R_W(0)\frac{1}{\Delta}\log\frac{1}{\Delta}d\omega \\
&= \infty
\end{aligned} \tag{5.16}$$

$$\begin{aligned}
\lim_{\eta\to\infty} D_{KL}(S_W(\omega), R_W(0)) &= \lim_{\eta\to 0}\int_{-\pi}^{\pi} S_X(\omega)\log\frac{S_X(\omega)}{S_Y(\omega)}d\omega \\
&= \int_{-\pi}^{\pi} R_W(0)\log\frac{R_W(0)}{R_W(0)}d\omega \\
&= 0
\end{aligned} \tag{5.17}$$

The motivation for using a distance which is non-negative is to measure the difference between two power spectral densities and a zero distance implies the equivalence of the two densities. For non-zero values, the greater the magnitude, the farther separated the two power spectral densities are. A desirable property

for any distance used is that it is bounded from below and above yet neither the Itakura-Saito Distance nor the KL Distance is bounded from above in the worst case of no sampling which corresponds to the vanishing behavior of η and diverge indefinitely. This situation will cause problems when used for actual computation furthermore, spectral correlation may be computed using the equivalent form that follows from Parseval's Relation by summing over a large number of autocorrelation sequence samples however, the same method cannot be used for either the Itakura-Saito or the KL distance. Nevertheless, DFT may be used to perform this task which windows the signal before computation with a rectangular window causing the power spectral density to be smoothed by a sinc frequency kernel. For such computations, the DFT length needs to be set as large as possible to cope with the shortcomings of the algorithm.

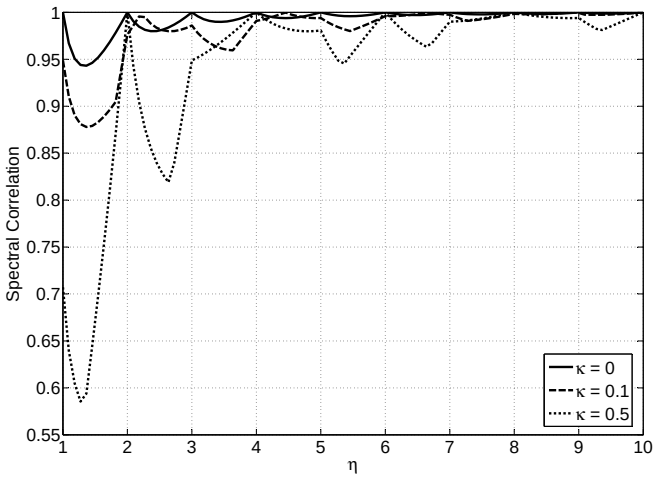

Figure 5.5. Spectral Correlation between $\{W_n\}$ and $\{\tilde{W}_n\}$ versus η for $\kappa = 0, 0.1, 0.5$

As distances, Itakura-Saito and KL exhibit a reciprocal behavior as compared to spectral correlation since the distances yield larger output for misaligned power spectral densities. As shown in Figs. 5.6 and 5.7 the Itakura-Saito Distance emphasizes the difference more than the KL distance i.e., for the worse case of $\kappa = 0.5$ the Itakura-Saito Distance is more than ten times grater in amplitude than the KL Distance.

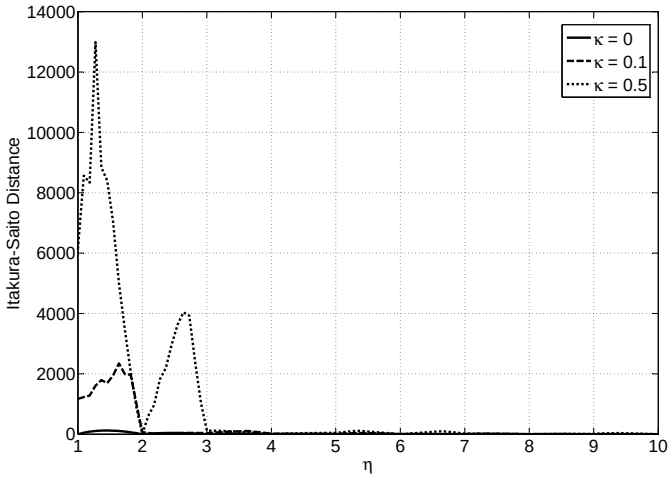

Figure 5.6. Itakura-Saito Distance between $\{W_n\}$ and $\{\tilde{W}_n\}$ versus η for $\kappa = 0, 0.1, 0.5$

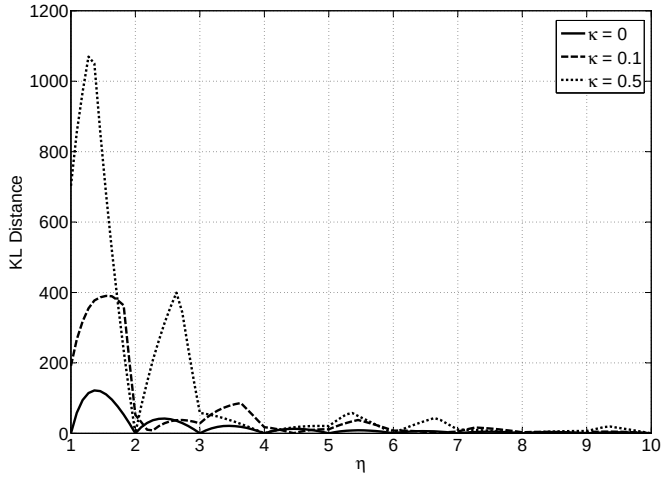

Figure 5.7. KL Distance between $\{W_n\}$ and $\{\tilde{W}_n\}$ versus η for $\kappa = 0, 0.1, 0.5$

6. Conclusions and Future Work

Given a continuous time BFSG, the necessary and sufficient conditions for generating i.i.d. Bernoulli-1/2 random variables via uniformly sampling from this process have been investigated while analytical and numerical results for the per sample joint entropy have also been provided. Generating independent random variables is essential for security applications because the conditional entropy of i.i.d. random variables is equal to their marginal entropies i.e., there is no decrease in uncertainty given the realization of any of the random variables. Throughout the analysis, an equivalent setup in place of the original one was used in order to make the derivations simpler. Spectral correlation was introduced as a novel figure of merit along with the analytical and numerical results for various noise bandwidth-sampling period product values and was shown to be equivalent to generating i.i.d. Bernoulli-1/2 random variables when it achieves its upper bound.

Rate of convergence of per sample joint entropy was characterized by using a third order inverse polynomial and roughly it has been demonstrated that for values of $\eta \approx 10$ such that $T_s \approx 5/B$ the generated bit sequence achieves the upper bound on per sample joint entropy and as such this choice of sampling period may be used as a rule of thumb with such systems. Itakura-Saito Distance and KL Distances were used to measure the difference between the power spectral densities of $\{W_n\}$ and $\{\tilde{W}_n\}$ which is the white wide sense stationary process closest to $\{W_n\}$ in mean square sense. These distances yield insight into the behavior of power spectral density of $\{W_n\}$ in the sense that a zero distance implies the alignment of the two densities which on the other hand implies the independence of $\{W_n\}$ and hence $\{Z_n\}$. However, spectral correlation can be used to measure the correlation between the two power spectral densities and yields a more intuitive result in the sense that shapewise it is similar to per sample joint entropy and is bounded between zero and unity where those values are attained at the same η values for both per sample joint entropy and spectral correlation.

Additionally, it is much simpler to compute the spectral correlation which follows from Parseval's Relation and for all these reasons it should be the merit of choice for assessing the randomness of the bits generated from wide sense stationary Gaussian processes.

For future work, the analysis will be extended to arbitrary finite vectors with a given or possibly unknown covariance structure and to processes possessing non-flat spectral structures or ones with flat power spectral densities and smooth transition regions. Furthermore, bounds on per sample joint entropy will be developed to be able to further characterize the system complexity and the achievable performance margins.

APPENDIX A: Proofs of Propositions

I. Proof of Proposition 1

For the zero mean jointly Gaussian random vector $\mathbf{W} = [W_1, \ldots, W_N]^T$ with covariance matrix Σ and marginal variances $\sigma_1^2, \ldots, \sigma_N^2$ pairwise uncorrelatedness of elements implies $\Sigma = \text{diag}[\sigma_1^2, \ldots, \sigma_N^2]$. In this case, the multivariate Gaussian distribution may be expressed as in the following form :

$$\begin{aligned} f_{\mathbf{W}}(\mathbf{w}) &= \frac{1}{\sqrt{(2\pi)^N \prod_{n=1}^N \sigma_n^2}} \exp\left(-\sum_{n=1}^N \frac{w_n^2}{2\sigma_n^2}\right) \\ &= \prod_{n=1}^N \frac{1}{\sqrt{2\pi\sigma_n^2}} \exp\left(-\frac{w_n^2}{2\sigma_n^2}\right) \\ &= \prod_{n=1}^N f_{W_n}(w_n) \end{aligned} \tag{I.1}$$

From (I.1) it follows that $W_1, \ldots, W_N$ are independent [20, pp. 184]. As a consequence, pairwise uncorrelatedness of jointly Gaussian random variables is equivalent to their independence. Since every Z_n is a function of every W_n in the form $Z_n = \mathbb{1}_{W_n > \tau}$ they are also independent [20, pp. 184]. □

II. Proof of Proposition 2

First, note that, for all n, $\mathrm{E}[W_n] = 0$ since $\mathrm{E}[N(t)] = 0$ for all t. Also, $\mathrm{E}[W_n^2]$ are invariant with respect to n since $\{W_n\}$ is a discrete time wide sense stationary process because $N(t)$ is a continuous time wide sense stationary process. So, it is seen that $\{W_n\}$ are i.i.d. if and only if $R_W(k) = 0$ for all $k \neq 0$. Next,

$$\begin{aligned} R_W(k) &= \mathrm{E}[W_n W_{n-k}] \\ &= \mathrm{E}[N(nT_s)\, N((n-k)T_s)] \\ &= R_N(u)\big|_{u=kT_s} \\ &= N_0 B \mathrm{sinc}(2BkT_s) - N_0 A \mathrm{sinc}(2AkT_s) \end{aligned} \tag{II.2}$$

where (II.2) follows from (2.5). Observe that, for $k \neq 0$,

$$\begin{aligned} R_W(k) &= \frac{N_0 B}{\pi 2BkT_s} \sin(2Bk\pi T_s) - \frac{N_0 A}{\pi 2AkT_s} \sin(2Ak\pi T_s) \\ &= \frac{N_0}{2k\pi T_s} [\sin(2Bk\pi T_s) - \sin(2Ak\pi T_s)] \end{aligned}$$

Hence, it is seen that $R_W(k) = 0$ for all $k \neq 0$ if and only if $h(k) = 0$ for all k, where

$$h(k) \stackrel{\triangle}{=} \sin(2Bk\pi T_s) - \sin(2Ak\pi T_s).$$

Next, define

$$\begin{aligned} p_B &\stackrel{\triangle}{=} \lfloor 2BT_s \rfloor, r_B \stackrel{\triangle}{=} 2BT_s - p_B, \\ p_A &\stackrel{\triangle}{=} \lfloor 2AT_s \rfloor, r_A \stackrel{\triangle}{=} 2AT_s - p_A. \end{aligned}$$

Note that, this implies, $p_A, p_B \in \mathbb{Z}$ and $r_A, r_B \in [0, 1)$. Then,

$$\begin{aligned} h_k &= \sin(\pi k p_B + \pi k r_B) - \sin(\pi k p_A + \pi k r_A) \\ &= \cos(\pi k p_B)\sin(\pi k r_B) - \cos(\pi k p_A)\sin(\pi k r_A) \\ &= (-1)^{kp_B}\sin(\pi k r_B) - (-1)^{kp_A}\sin(\pi k r_A) \end{aligned} \tag{II.3}$$

In order to investigate the condition of $h_k = 0$ for all k, the three following cases are analyzed step by step:

Case 1: Either $(r_A = 0)$ or $(r_B = 0)$:

If $(r_A = 0)$, using (II.3),

$$\begin{aligned} [\forall k,\ k = 0] \quad &\Leftrightarrow \quad \left[\forall k,\ (-1)^{kp_B}\sin(\pi k r_B) = 0\right] \\ &\Leftrightarrow \quad [\forall k,\ \sin(\pi k r_B) = 0] \\ &\Leftrightarrow \quad [r_B = 0] \end{aligned} \tag{II.4}$$

Similarly, if $(r_B = 0)$,

$$\begin{aligned} [\forall k,\ k = 0] \quad &\Leftrightarrow \quad \left[\forall k,\ (-1)^{kp_A}\sin(\pi k r_A) = 0\right] \\ &\Leftrightarrow \quad [\forall k,\ \sin(\pi k r_A) = 0] \\ &\Leftrightarrow \quad [r_A = 0] \end{aligned} \tag{II.5}$$

So, merging (II.4) and (II.5), if $r_A = r_B = 0$, then for all k, $h_K = 0$; this is equivalent to (3.3).

Case 2: $(0 < r_A, r_B < 1)$ and $(p_A - p_B$ is even$)$:

First, note that $p_A - p_B$ is even if and only if p_A, p_B are both odd or both even. Then, $(-1)^{kp_B} = (-1)^{kp_A}$ for all k. Hence, in this case,

$$\begin{aligned} [\forall k,\ h_k = 0] \quad &\Leftrightarrow \quad [\forall k,\ q_k = 0] \\ &\Leftrightarrow \quad [\forall w \in [-\pi, \pi],\ Q(w) = 0] \end{aligned}$$

where $q_k \triangleq \sin(\pi k r_B) - \sin(\pi k r_A)$, $Q(w) \triangleq \mathcal{F}\{\mathbf{q}\}$. Now, observe that

$$\begin{aligned} Q(w) = \frac{\pi}{j} \sum_{l=-\infty}^{\infty} [&\delta(w - \pi r_B - 2\pi l) - \delta(w + \pi r_B - 2\pi l) \\ &- \delta(w - \pi r_A - 2\pi l) + \delta(w + \pi r_A - 2\pi l)] \end{aligned}$$

Then, for all $w \in [-\pi, \pi]$,

$$\begin{aligned} Q(w) = &\frac{\pi}{j} [\delta(w - \pi r_B) - \delta(w - \pi r_A)] \\ &- \frac{\pi}{j} [\delta(w + \pi r_B) - \delta(w + \pi r_A)] \end{aligned}$$

since $0 < r_A, r_B < 1$. Thus, $Q(w) = 0$ for all $w \in [-\pi, \pi]$ if and only if $r_A = r_B$. Now, the conditions of ($p_A - p_B$ even) and ($r_A = r_B$) jointly together are equivalent to ($2BT_s - 2AT_s$ is even). In turn, this is equivalent to ($\exists n \in \mathbb{Z}$, s.t. $2(B - A)T_s = 2n$), which is equivalent to (3.4).

Case 3: $(0 < r_A, r_B < 1)$ and ($p_A - p_B$ is odd) :

First, note that $p_A - p_B$ is odd if either (p_A even, p_B odd) or (p_A odd, p_B even). Then, for all $k \in \mathbb{Z}$, $(-1)^{kp_B} = (-1)^{k(p_A+1)}$. Hence, in this case,

$$\begin{aligned} [\forall k,\ h_k = 0] \quad &\Leftrightarrow \quad [\forall k,\ s_k = 0] \\ &\Leftrightarrow \quad [\forall w \in [-\pi, \pi],\ S(w) = 0] \end{aligned}$$

where $s_k \triangleq (-1)^k \sin(\pi k r_B) - \sin(\pi k r_A)$ and $S(w) \triangleq \mathcal{F}\{\mathbf{s}\}$. Now, for all k,

$$\begin{aligned} s_k &= (-1)^k \sin(\pi k r_B) - \sin(\pi k r_A) \\ &= \sin(\pi k r_B + \pi k) - \sin(\pi k r_A) \\ &= \sin(\pi (r_B + 1) k) - \sin(\pi r_A k) \end{aligned}$$

which implies

$$S(w) = \frac{\pi}{j} \sum_{l=-\infty}^{\infty} [\delta(w - \pi(r_B + 1) - 2\pi l)$$

$$
\begin{aligned}
&- \delta\left(w + \pi\left(r_B + 1\right) - 2\pi l\right) \\
&- \delta\left(w - \pi r_A - 2\pi l\right) \\
&+ \delta\left(w + \pi r_A - 2\pi l\right)]
\end{aligned}
$$

Then, for all $w \in [-\pi, \pi]$,

$$
\begin{aligned}
S\left(w\right) = \frac{\pi}{j}[&\delta\left(w + \pi\left(1 - r_B\right)\right) - \delta\left(w - \pi\left(1 - r_B\right)\right) \\
&- \delta\left(w - \pi r_A\right) + \delta\left(w + \pi r_A\right)]
\end{aligned} \tag{II.6}
$$

which follows from noting $0 < \pi r_A < \pi$ and $\pi < \pi\left(r_B + 1\right) < 2\pi$ Since $\pi\left(1 - r_B\right)$ and πr_A are both in the range of $[0, 2\pi]$, (II.6) implies that in this case $S\left(w\right) = 0$ can never hold for any w.

Consequently, because Cases 1, 2, and 3 cover all the possibilities, the claim follows. □

III. Proof of Proposition 3

As η tends to infinity the entries of the covariance matrix Σ introduced in Sec. 3 has the following covariance matrix :

For $i \neq j$:

$$
\begin{aligned}
\lim_{\eta\to\infty} \Sigma_{ij} &= \lim_{\eta\to\infty} N_0 B(\mathrm{sinc}((i-j)2BT_s) - \kappa\mathrm{sinc}((i-j)2AT_s)) \\
&= \lim_{\eta\to\infty} N_0 B(\mathrm{sinc}((i-j)\eta) - \kappa\mathrm{sinc}((i-j)\kappa\eta))
\end{aligned}
$$

$$= \lim_{\eta\to\infty} N_0 B \left(\frac{\sin(\pi(i-j)\eta)}{\pi(i-j)\eta} - \kappa \frac{\sin(\pi(i-j)\kappa\eta)}{\pi(i-j)\kappa\eta} \right)$$
$$= 0 \tag{III.7}$$

For $i = j$:

$$\begin{aligned} \lim_{\eta\to\infty} \Sigma_{ij} &= \lim_{\eta\to\infty} N_0 B \text{sinc}((i-i')2BT_s)|_{i'=i} \\ &- N_0 A \, \text{sinc}((i-i')2AT_s)|_{i'=i} \\ &= N_0 B - N_0 A, \ \forall i = j \end{aligned} \tag{III.8}$$

From (III.7) and (III.8) it follows that :

$$\lim_{\eta\to\infty} \Sigma = \text{diag}[N_0 B - N_0 A, \ldots, N_0 B - N_0 A] \tag{III.9}$$

As η tends to infinity, the distribution of the zero mean, jointly Gaussian random vector $\mathbf{W} \stackrel{\triangle}{=} [W_1, \ldots, W_N]$ with covariance matrix Σ given by (III.9) is :

$$\begin{aligned} \lim_{\eta\to\infty} f_{\mathbf{W}}(\mathbf{w}) &= \lim_{\eta\to\infty} \frac{1}{\sqrt{2\pi|\Sigma|}} \exp\left(-\frac{\mathbf{w}^T \Sigma^{-1} \mathbf{w}}{2} \right) \\ &= \prod_{n=1}^{N} \frac{1}{\sqrt{2\pi(N_0 B - N_0 A)}} \\ &\times \exp\left(-\frac{w_n^2}{2(N_0 B - N_0 A)} \right) \end{aligned}$$

$$= \prod_{n=1}^{N} f_{W_n}(w_n) \tag{III.10}$$

where $W_n \sim \mathcal{N}(0, N_0 B - N_0 A)$. Also note that for the case $A \to 0$, (III.10) still holds, this time only the marginal distributions become $W_n \sim \mathcal{N}(0, N_0 B)$. As a consequence the results that have been derived for the general case apply to the lowpass approximation as a special case.

Since (III.10) is a legitimate multivariate probability distribution, it has no singularities or discontinuities and it is non-negative in its domain furthermore, its integral is bounded by unity that follows from the definition of total probability. As a consequence, $\Pr[\mathbf{W} \in I]$ where $\{\forall \mathbf{W} \in I : W_1 \in I_1, \ldots, W_N \in I_N; I_i \cap I_j = \emptyset,\ i \neq j; I = I_1 \times \ldots \times I_N\}$ and I is a compact region in $\mathbb{R}^N$, may equivalently calculated as η tends to infinity by a Riemann Sum that always converges [21, pp. 389] :

$$\begin{aligned}
\lim_{\eta \to \infty} \Pr[\mathbf{W} \in I] &= \lim_{\eta \to \infty} \int_I f_{\mathbf{W}}(\mathbf{w}) d\mathbf{w} \\
&= \lim_{k \to \infty} \lim_{\eta \to \infty} \sum_k f_{\mathbf{W}}(\mathbf{w_k}) \nu_k \\
&= \lim_{k \to \infty} \sum_k \lim_{\eta \to \infty} f_{\mathbf{W}}(\mathbf{w_k}) \nu_k \\
&= \int_I \lim_{\eta \to \infty} f_{\mathbf{W}}(\mathbf{w}) d\mathbf{w} \\
&= \prod_{n=1}^{N} \int_{I_n} f_{W_n}(w_n) dw_n \\
&= \prod_{n=1}^{N} \Pr[W_n \in I_n]
\end{aligned} \tag{III.11}$$

where ν_k is the volume of a region ζ_k such that $\{\forall \mathbf{w}_k \in \zeta_k : \zeta_k \subset \mathbb{R}^N; \zeta_i \cap$

$\zeta_j = \emptyset,\ i \neq j; I = \bigcup_k \zeta_k\}$. From (III.11) it is seen that as η tends to infinity, $W_1, \ldots, W_N$ are i.i.d. [20, pp. 184] in which case, the per sample joint entropy is given by Corollary 1. □

IV. Proof of Proposition 4

Using Parseval's Theorem [22, pp. 380] spectral correlation may equivalently expressed as :

$$\theta_{\{X_n\},\{Y_n\}} = \frac{\sum_{k=-\infty}^{\infty} R_X(k) R_Y(k)}{\sqrt{\sum_{k=-\infty}^{\infty} R_X(k)^2 \sum_{k=-\infty}^{\infty} R_Y(k)^2}} \tag{IV.12}$$

Now let $S_Y(\omega) = R_X(0)$ so that $R_Y(k) = R_X(0)\delta_D(k)$ where, $\delta_D(k)$ is the discrete Dirac Delta Function defined in [22, pp. 30] such that,

$$\delta_D(k) \triangleq \begin{cases} 1, & \text{if } k = 0 \\ 0, & \text{if else} \end{cases} \tag{IV.13}$$

implying Y_n is a white process with variance $R_X(0)$. Equating (IV.12) to unity yields,

$$\theta_{\{X_n\},\{Y_n\}} = \frac{\sum_{k=-\infty}^{\infty} R_X(k) R_X(0)\delta_D(k)}{\sqrt{\sum_{k=-\infty}^{\infty} R_X(k)^2 \sum_{k=-\infty}^{\infty} (R_X(0)\delta_D(k))^2}} = 1 \tag{IV.14}$$

By taking the square of both sides of (IV.14),

$$
\begin{aligned}
R_X(0)^4 &= R_X(0)^2 \sum_{k=-\infty}^{\infty} R_X(k)^2 \\
R_X(0)^2 &= \sum_{k=-\infty}^{\infty} R_X(k)^2 \\
0 &= \sum_{k\neq 0} R_X(k)^2 \qquad \text{(IV.15)}
\end{aligned}
$$

(IV.15) holds if and and only if $R_X(k) = 0,\ \forall k \neq 0$ which is equivalent to having $\{X_n\}$ uncorrelated. □

REFERENCES

1. B. Jun and P. Kocher, "The Intel Random Number Generator," Cryptography Research, Inc., *white paper prepared for Inter Corp.*, Apr. 1999. Available at http://www.cryptography.com/resources/whitepapers/IntelRNG.pdf.

2. A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

3. B. Schneier, *Applied Cryptography*, 2^{nd} ed. John Wiley & Sons, 1996.

4. W. T. Holman, J. A. Connelly, and A. B. Downlatabadi, "An Integrated Analog/Digital Random Noise Source", *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, vol. 44, no. 6, pp. 521–528, June 1997.

5. V. Bagini and M. Bucci, "A Design of Reliable True Random Number Generator for Cryptographic Applications", *Proc. Workshop Cryptographic Hardware and Embedded Systems (CHES '99)*, pp. 204–218, 1999.

6. M. Dichtl and N. Janssen, "A High Quality Physical Random Number Generator", *Proc. Sophia Antipolis Forum Microelectronics (SAME 2000)*, pp. 48–53, 2000.

7. C. S. Petrie and J. A. Connelly, "A Noise-Based IC Random Number Generator for Applications in Cryptography", *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, vol. 47, no. 5, pp. 615–621, May 2000.

8. T. Stojanovski, J. Pihl, and L. Kocarev, "Chaos-Based Random Number Generators-Part II: Practical Realization", *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, vol. 48, no. 3, pp. 382–

385, Mar. 2001.

9. S. Callegari, R. Rovatti, G. Setti, "Embeddable ADC-Based True Random Number Generator for Cryptographic Applications Exploiting Nonlinear Signal Processing and Chaos", *IEEE Transactions on Signal Processing*, vol. 53, pp. 793–805, no. 2, Feb. 2005.

10. M. Delgado-Restituto, F. Medeiro, and A. Rodriguez-Vazquez, "Nonlinear Switched-current CMOS IC for Random Signal Generation", *Electronics Letters*, vol. 29, no. 25, pp. 2190–2191, 1993.

11. M. E. Yalcin, J. A. K. Suykens, and J. Vandewalle, "True Random Bit Generation from a Double Scroll Attractor", *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, vol. 51, no. 7, pp. 1395–1404, 2004.

12. S. Ergün, S. Özoğuz, "Truly Random Number Generators Based On Non-Autonomous Continuous-time Chaos," *Int. J. Circ. Theor. Appl.*; published online, DOI: 10.1002/cta.520, 2008.

13. H. F. Murry, "A General Approach for Generating Natural Random Variables", *IEEE Transactions on Computers*, vol. 19, pp. 1210–1213, Dec. 1970.

14. N. O. Sokal, "Optimum Choice of Noise Frequency Band and Sampling Rate for Generating Random Binary Digits from Clipped White Noise", *IEEE Transactions on Computers*, vol. 21, pp. 614–615, June 1972.

15. J. D. Boyes, "Binary Noise Sources Incorporating Modulo-N Dividers", *IEEE Transactions on Computers*, vol. 23, pp. 550-552, May 1974.

16. D. R. Morgan, "Analysis of Digital Random Numbers Generated from Serial Samples of Correlated Gaussian Noise", *IEEE Transactions on Information Theory*, vol. 27, pp. 235–239, no. 2, March 1981.

17. C. S. Petrie, J. A. Connelly, "The sampling of noise for random number generation" , 1999. *IEEE International Symposium on Circuits and Systems (ISCAS '99)*, vol. 6, pp. 26 - 29, 1999

18. M. Bucci, L. Germani, R. Luzzi, P. Tommasino, A. Trifiletti, and M. Varanonuovo, "A High-Speed IC Random-Number Source for Smart Card Microcontrollers", *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, vol. 50, no. 11, pp. 1373–1380, Nov. 2003.

19. T. M. Cover and J. A. Thomas, *Elements of Information Theory*, New York: Wiley, 1991.

20. A. Papoulis, *Probability, Random Variables, and Stochastic Processes*, 3^{rd} ed. New York : McGraw-Hill, 1991.

21. T. M. Apostol, *Mathematical Analysis*, 2^{nd} ed. Addison Wesley, 1974.

22. A. V. Oppenheim, A. S. Willsky with S. H. Nawab, *Signals and Systems*, 2^{nd} ed. Prentice Hall, 1996.

23. A. Van Der Ziel, "Noise in Solid-state Devices and Lasers", *Proceedings of the IEEE*, vol. 58, pp. 1178–1206, Aug 1970.

24. A. H. S. Chan, S. I. Ao . *Advances in industrial engineering and operations research*, Springer, 2008.