Int. J. Electron. Commun. (AEÜ) 70 (2016) 301–310

Contents lists available at ScienceDirect

International Journal of Electronics and Communications (AEÜ)

journal homepage: www.elsevier.com/locate/aeue

Analysis of chaotic behavior in pipelined analog to digital converters

Esmaeil Fatemi-Behbahani*, Ebrahim Farshidi, Karim Ansari-Asl

Department of Electrical Engineering, Faculty of Engineering, Shahid Chamran University of Ahvaz, Ahvaz, Iran

ARTICLE INFO

Article history:
Received 21 June 2015
Accepted 10 December 2015

Keywords:
Pipelined ADC
Chaotic map
Half-bit redundancy
Probability density function (pdf)
Random number generator
Uniform distribution

ABSTRACT

This paper presents a new approach to analysis of chaotic behavior in pipelined analog to digital converters. To this end, the fundamental theorem for function of a random variable is exploited and the propagation of the output pdf of chaotic maps in successive stages of pipelined converter is shown. It is illustrated that 1-bit stage of this converter can be used to implement the Bernoulli map, and also the 2^k-way Bernoulli shift map can be implemented using $k \times 1$-bit stages or one k-bit stage. It is revealed that in the half-bit redundant structure, after a sufficiently large number of cycles, residue density becomes concentrated in the center half of the stage full-scale range. In this way, the 1.5-bit stage characteristic will be fully equivalent to the common chaotic map that is employed to generate random number sequences. By applying the proposed approach to the joint density of residue stages, it is shown that residues become independent and uniformly distributed. This feature is used to design multi bit chaotic random number generator using full-bit and half-bit redundant pipelined ADC structure. The validity of the proposed random number generator is confirmed by passing all NIST statistical tests even in the presence of nonidealities.

1. Introduction

There are some trade-offs between speed, power consumption, resolution, and circuit area in designing analog to digital converters (ADCs) [1,2]. A popular structure for both high resolution and high speed data conversion is pipelined ADC [3]. This converter is used for medium to high resolutions (8–16 bits) and sampling rate of 10 MHz to 2.5 GHz in video and telecommunication receivers [4]. In this architecture, the analog to digital conversion is performed by using a number of successive simple stages in a way that makes the simultaneous raise in speed and resolution possible [5]. The stages can be identical or nonidentical.

One of the most important issues in analog to digital converters is the quantization noise theory presented by Widrow [6], in which the required and sufficient conditions of the uniformity of the noise distribution have been described using quantizing theorems. Quantizing theorems, similar to the sampling theorem but based on the sampling of the probability density function (pdf), clarify the required conditions of signal characteristic function in details [6,7]. In [8], investigating the statistical properties of quantization noise in a uniform quantizer, the required and sufficient conditions for having uniform and white output noise are expressed. In [9], it has been shown that with the passage of signal from different stages of a full-bit pipelined converter, the residue density and the residue joint probability density function at different times converge to uniformity. This indicates that residue signals become asymptotically independent. The same feature exists for all multistage ADCs such as pipelined, algorithmic (cyclic), and successive approximation register (SAR) converters, with full-bit and half-bit redundant structures. These properties allow us to use them as random number generators (RNGs) and produce independent and identically distributed (i.i.d.) random bit sequences.

Random number generators have numerous applications in cryptography algorithms [10,11], communication systems [12] as well as calibration of algorithmic and pipelined ADCs by dither injection [13,14]. RNGs can be divided into two categories: pseudo random number generators (PRNGs) and true random number generators (TRNGs) [10,15]. PRNGs have periodic behaviors and are far from the ideal features required in some important applications such as information security and cryptography [15,16]. Also, TRNGs have low throughput and high cost of embedding in digital circuits [11,17]. Therefore, chaotic RNGs which use chaotic maps have found widespread applications. Some of these chaotic maps are very similar to the building blocks of practical electronic circuits. For instance, the characteristic of the half-bit redundant stage which has been exploited in designing the pipelined ADC in [18] is fully equivalent to chaotic map that has been used in [12,19]. Hence, in [10,17] this 1.5-bit stage was employed to implement chaotic RNG. Although, today such a stage is not commonly used in

* Corresponding author. Tel.: +98 6152721230.
E-mail addresses: e-fatemi@phdstu.scu.ac.ir (E. Fatemi-Behbahani), farshidi@scu.ac.ir (E. Farshidi), karim.ansari@scu.ac.ir (K. Ansari-Asl).

http://dx.doi.org/10.1016/j.aeue.2015.12.008
1434-8411/

multistage ADCs, it is shown that the popular used full-bit and half-bit redundant stages are also efficient to design the chaotic maps. Since the analog to digital converters are capable of being used in high speeds [20], the chaotic RNG by using pipelined ADC building blocks is suitable for these applications. Furthermore, because analog and digital circuits are placed together on one chip in analog to digital converters, ADC-based RNGs impose no problem for embedding in other analog or digital circuits.

In this paper, the input–output characteristics of the various stages of the pipelined ADC are compared with some of the common chaotic maps that are used in chaotic RNGs; and it is shown that they are fully similar to each other. One of these chaotic maps is Bernoulli map [15,21], which fully matches with the characteristic of the ideal 1-bit stage. The characteristic of the full k-bit stage is also fully identical to the N-way Bernoulli shift map with $N=2^k$ [22], which is the more general form of the Bernoulli map. Furthermore, a new approach to analyze the output of chaotic maps as well as the different stage residues of multistage ADCs is presented. To this end, the fundamental theorem for function of a random variable [23] is exploited and the propagation of the output pdf of the chaotic maps in different stages of the pipelined ADC is illustrated. It is demonstrated that in full-bit stages, with an increase in the number of converter bits, the residue pdf converges to uniformity in the stage full-scale range. Therefore, regarding the random nature and the uniform distribution of the output bits, this converter can be directly used to implement N-way Bernoulli shift map and generate random sequences. For the half-bit redundant structure, the residue pdf in the center half of the stage full-scale range converges to uniformity and out of it converges to zero. Thus, after a sufficiently large number of stages, each stage will be fully equivalent to the common chaotic map which has been used in [12,19].

The proposed analysis approach is extended to the joint pdf of output residues in the full-bit and half-bit redundant structures at different times. It is illustrated that with increasing the number of converter bits, residue joint pdf converges to uniformity. This fact shows the statistical independency of the different stages residue in pipelined ADC for the very high number of converter bits. So, this converter can be used to generate multi bit and high-speed i.i.d. random number sequences.

The performance of the proposed ADC-based RNG is evaluated by using the U.S. National Institute for Standards and Technology (NIST) randomness test suite [24] which is widely used to investigate the statistical properties of random number generators [25–28]. Since analog to digital converters are sensitive to device parameters variations [20], these nonidealities are also going to be considered. The NIST statistical test results show that proposed chaotic RNG provides very good quality of generated bit stream in the presence of mismatches.

The rest of the paper is organized as follows. In Section 2, some of the common maps used in chaotic RNGs, which are very similar to the characteristic of ADC building blocks, are investigated. Section 3 introduces the pipelined ADC architecture. In Section 4, the use of full-bit pipelined ADC and in Section 5, the application of half-bit redundant converter in random bit generation is explored. Section 6 evaluates the performance of the proposed RNG using the NIST statistical test suite. A brief conclusion is drawn in Section 7.

2. Chaotic RNGs

Random sequence generation can be modeled by the toss of an ideal coin, which the probability of each side is 1/2. Such tosses are independent from each other and seeing each toss does not affect the probability of the next tosses observations. That is, the system state cannot be predicted. This behavior can be described as the two-state Markov chain of Fig. 1, which is a special kind of Markov processes. Several chaotic maps were presented for this

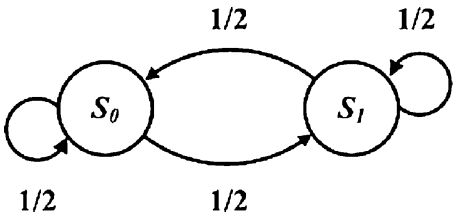

Fig. 1. Markov chain of the toss of an ideal coin (random bit generator).

Markov chain. One of them is 2-way Bernoulli map, also known as Bernoulli map, which is expressed as follows [15,21].

$$M:[-1,1]\to[-1,1],\quad M(x)=2x\,mod2-1 \tag{1}$$

Eq. (1) can be rewritten as

$$M:[-1,1]\to[-1,1],\quad M(x)=\begin{cases}2\left(x+\frac{1}{2}\right), & -1<x<0\\ 2\left(x-\frac{1}{2}\right), & 0<x<1.\end{cases} \tag{2}$$

In Section 4, it will be shown that after sufficient iterations of this map, the distribution of the x-samples becomes uniform over [−1,1]. In this way, the Bernoulli map is equivalent to Markov chain of Fig. 1 and knowing the previous sequences reveals no information about its future values. Also, since the probability of being in each of two states equals 1/2, the entropy of the source is one bit.

The more general form of (1) and (2) is N-way Bernoulli shift map [22], which can be expressed as follows.

$$M:[0,1]\to[0,1],\quad M(x)=Nx\bmod 1. \tag{3}$$

The above map over [−1,1] can be written as

$$M:[-1,1]\to[-1,1],\quad M(x)=Nx\bmod 2-1. \tag{4}$$

This map that is widely used in signal processing tasks is shown in Fig. 2 for different values of N.

Another chaotic map that has been found to have a good performance in RNGs is [12,19]

$$M:[-1,1]\to[-1,1],\quad M(x)=(2x+1)\bmod 2-1 \tag{5}$$

and is shown in Fig. 3. This map is identical to the characteristic of the 1.5-bit stage used in [18] for pipelined ADC which uses the half-bit redundancy in order to achieve the related advantages. An important feature of this map compared with Bernoulli map, is its flexibility against noise and nonideality impacts on electronic circuits in a way that it has all the needed conditions for a piecewise affine Markov chaotic maps [17]. In this map the distribution of x-samples over [−1,1] converges to uniformity. It can be shown that from the statistical point of view and after sufficient iterations, the behavior of the map can be illustrated exactly as the Bernoulli process and two-state Markov chain of Fig. 1 [10].

It will be shown that such chaotic maps fully matches with the characteristics of the ideal full-bit and half-bit redundant stages of pipelined ADC and, thus, such converter building blocks can be used to implement the chaotic maps.

3. Pipelined ADC architecture

The architecture of a pipelined analog to digital converter is shown in Fig. 4. This ADC consists of an input sample-and-hold amplifier (SHA) and one or several number of successive simple stages. All signals are normalized to V_{ref} so the converter dynamic range is [−1,1]. The SHA converts the continuous-time input signal x_{in} into a sampled sequence $x(k)=x_{in}(kT_s)$, where T_s denotes the sampling period. Each pipeline stage consists of a flash sub-ADC, a sub-DAC, a subtractor and an interstage amplifier. In the ith stage,