A Simple Digital FPGA Pseudo–Chaos Generator

L. Azzinnari*, A. Mozsáry*, K. Krol†, and V. Porra*

Abstract

In this paper, the feasibility of replacing a chaos source by an equivalent digital pseudo-random generator realized using Linear Feedback Shift Register (LFSR) is studied. Particular emphasis is given on the digital implementation Piece–Wise Linear Affine Maps (PWAM). As an application, an FPGA implementation of four different maps has been experimentally verified in a FM–DCSK test radio system.

1 Introduction

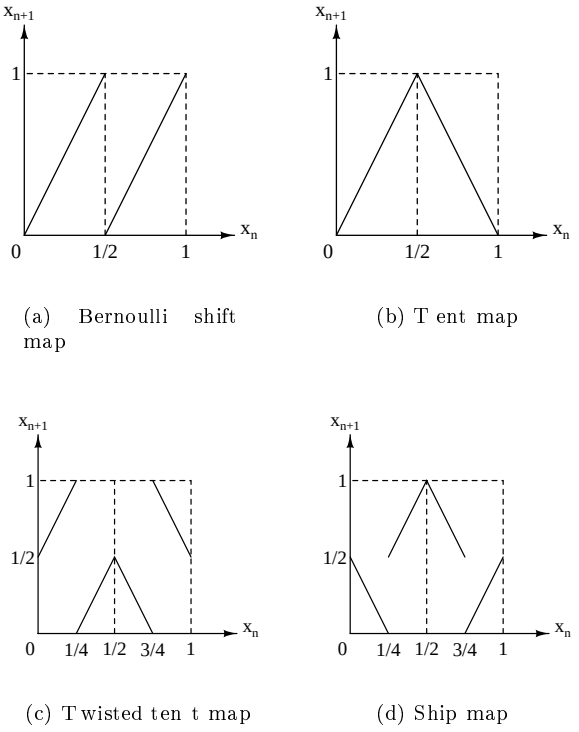
Chaos generators have been proposed as sources of noise–like signals in many applications. In the present study, a chaos source was needed in a spread-spectrum "chaos radio" system based on Differential Chaos Shift Keying (DCSK) [1] – [3]. Analogue continuous time or discrete time chaos sources have been demonstrated, but they suffer from high sensitivity to system parameters and circuit noise. Systems requiring chaos synchronization will be difficult to realize using analogue chaos sources. A clock synchronized digital system can not show chaotic behavior, but digital non–linear mappings may be modeled to find "almost chaotic" periodic orbits with a very long period. Especially the periodic orbits of Chaotic Piecewise Linear Affine Maps (PWAM) such as Bernoulli Shift map and different tent maps with slope equal to 2 can be realized by Linear Feedback Shift Registers (LFSR) commonly used as pseudo–noise sequence generators. The aim of the present paper is to demonstrate the feasibility of such pseudo–chaos sources. Four periodic PWAM mappings with a very long period have been implemented in a simple FPGA circuit and used as "chaos generators" of a digital FM-DCSK chaos radio.

2 Mathematical background

A proper piece–wise linear one–dimensional map together with a delay element can be used as a discrete-time chaos source. In this family, the simplest maps are the Bernoulli shift map and tent map with different modifications obtained from the Bernoulli shift by a simple mathematical transformation, as shown in Figure 1 [4]. Symmetric variations of these maps with delta–function shaped autocorrelation function have been shown well suited for DCSK chaos communication systems using correlation receiver [5]. Any rational number $x_0 \in [0, 1]$ can be expressed in the binary base as

$$x_0 = 0.b_1 b_2 b_3 b_4 \ldots = \sum_{k=1}^{\infty} 2^{-k} b_k, \qquad (1)$$

In the Bernoulli shift mapping, the number is first



(a) Bernoulli shift map

(b) Tent map

(c) Twisted tent map

(d) Ship map

Figure 1: Some piecewise linear one–dimensional maps.

multiplied by 2 and then the integer part (first digit) is turned to 0. The iteration sequence is $(2x \bmod 2)$. If the successive digits are stored into a binary shift register, one Bernoulli shift mapping step is performed by shifting the content one step up and dropping out the highest bit.

Starting from x_0 the mapping sequence begins as

*Electronic Circuit Design Laboratory, Helsinki University of Technology, POB-3000, FIN-02015 HUT, Finland. E-mail: Veikko.Porra@hut.fi, http://www.ecdl.hut.fi

†Presently with Spirea AB, Sweden

follows:

$$x_0 = 0.b_1b_2b_3b_4\ldots$$
$$x_1 = 0.b_2b_3b_4b_4\ldots$$
$$x_2 = 0.b_3b_4b_5b_4\ldots$$

For a finite sequence of n digits the iteration decays to zero after n steps. For a rational number represented by an infinite periodic sequence the mapping finds a limit cycle. For example for the initial value

$$x_0 = \frac{14}{15} = \frac{1110}{1111} = 0.111011101110\ldots$$

the limit cycle is 1110.

For chaos applications, irrational seed numbers should be used to reach chaotic orbits. For practical needs, a digital realization based on rational seed numbers with a very long period of digits can as well be used.

3 Technical considerations

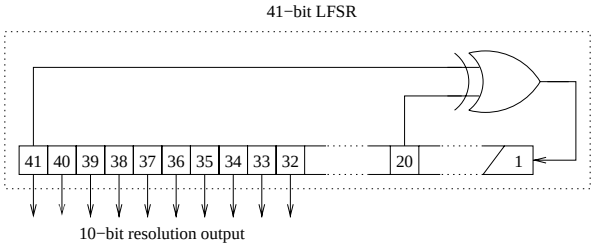
A Linear–Feedback Shift Register (LFSR), commonly used as a pseudo–noise generator, can generate rational numbers with a very long period of digits in binary form. At each shift step, a combination of the highest and some intermediate bits is used as the lowest bit. In the simplest form of a LFSR, prior to the shift operation, the highest bit is combined with the lowest one using XOR operation. After the shift the result is fed to the register as the new last bit.

It can be shown [6], that the period length of such a sequence generator of p bits can be $2^p - 1$. At a clock frequency of GHz, the period length for a 30–bit shift register is 1.1 seconds, but grows to 36 years for a register with double length or 60 bits.

In the present study ,the LFSR circuit shown in Figure 2(a) was used. It was taken from the `ARIB/ETSI/UMTS/WCDMA` standard. This 30–bit circuit realizes the $(2x \bmod 2)$ mapping with a limit cycle of 30 hours at the 20 MHz clock frequency

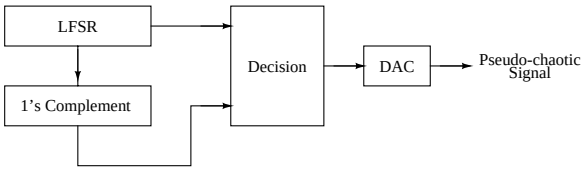
The tent, twisted tent and ship maps can be obtained from the Bernoulli shift map by properly applying function $(1 - x)$ during iteration. Because number $1 = 0.11111\ldots$, this mapping is simply inversion of the digits. After inversion, the result of the iteration should be reloaded to the shift register core. Significant improvement is gained in hardware and speed by omitting this step. The trick is based on the LFSR linearity: if all register content had been inverted, the feedback number would be the same.

As shown in Figure 2(c), in this case a block performing inversion and a simple decision block



(a) 41–bit LFSR

(b) Bernoulli shift generator



(c) Tent map generator

Figure 2: A 41–bit LFSR pseudo–random generator for Bernoulli shift mapping, conversion into analog form, tent map realization.

(which checks if x is smaller or larger than 1/2) need to be added to the LFSR.

The resulting "pseudo–chaos" signal samples are converted analogue by a digital to analogue converter (DAC). The accuracy depends on the DAC resolution l which is less than or at most equal to the shift register length p. In the experimental study, an $l = 10$–bit DAC was used.

4 Practical solution: the tent map

According to the previous considerations, the pseudo–chaotic sequence can be generated by means of mapping

$$x_{n+1} = |x_{n-1}\,(\mathrm{MSB}) \cdot o_l - \overline{x}_n| \qquad (2)$$

Here $x_{n-1}\,(\mathrm{MSB})$ is the most significant bit (MSB) of the $(n-1)$–th iterate, l is the bit resolution of the l–bit DAC ($p \geq l$). o_l is a vector of l "1"–bits and $\overline{x}_n$ is the vector of highest "1"–bits from the n–th iterate x_n.

The system described by (2) can be physically implemented using the circuit sketched in Figure 3. Other piecewise linear one–dimensional maps (as

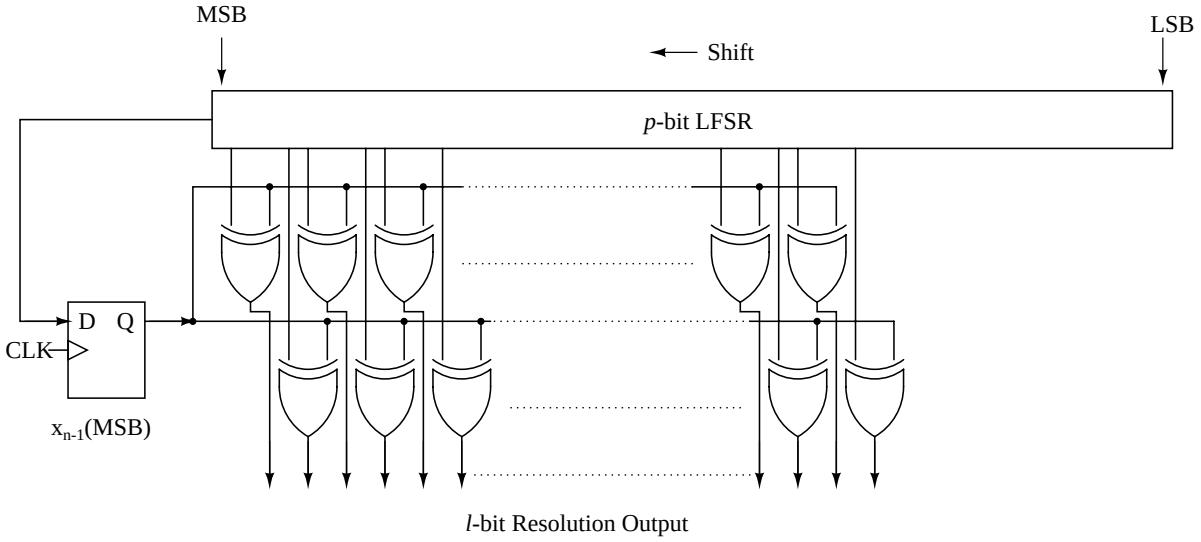


Figure 3: Digital realization of the "pseudo–chaos" tent map.

the ones shown in Figures 1(c) and 1(d)) need a bit more complex architecture – few more logic gates and flip-flops) but they are still easily realizable.

Figure 4 shows the autocorrelation function of the signal generated by a digital tent mapping.

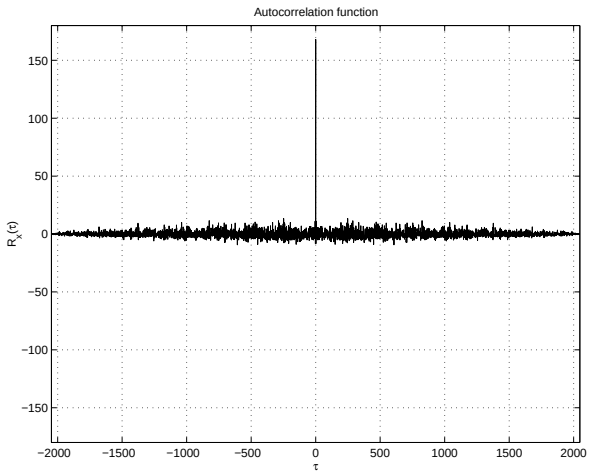


Figure 4: Autocorrelation function of 2048 samples of the LFSR tent map generator.

5 Conclusion

The proposed digital circuits have been implemented in a field programmable gate array (FPGA) circuit, and used as chaos generator for an experimental FM-DCSK radio system [1]. Figure 5 shows the IF signals obtained using the Bernoulli shift and tent pseudo–chaos generators. The FPGA implementation includes all four maps sketched in Figure 1.

Acknowledgements

This work, as a part of the hardware implementation of the FM-DCSK radio has been performed at HUT/ECDL under ESPRIT project No. 31103 INSPECT and the Telectronics program of the Academy of Finland.

References

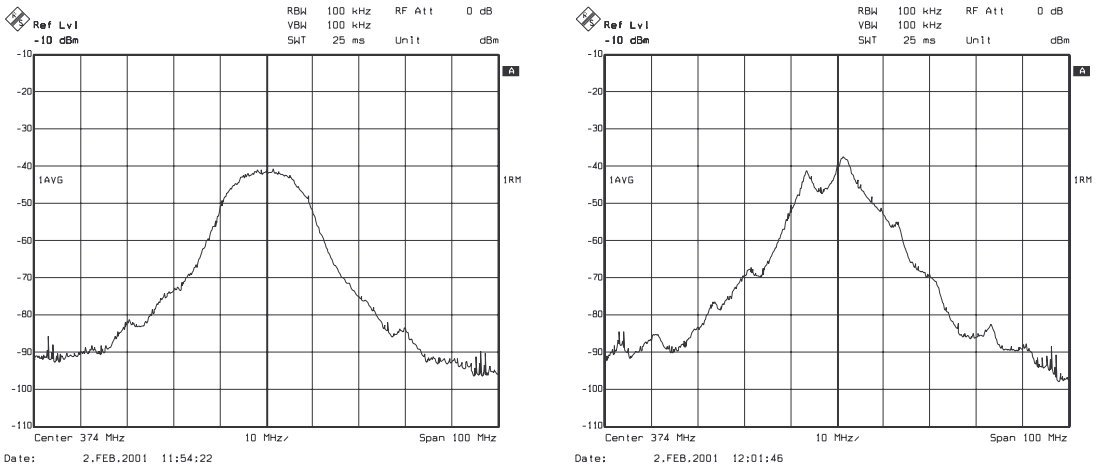
[1] K. Krol, L. Azzinnari, E. Korpela, M. Talonen, V.Porra, "An Experimental FM-DCSK Chaos Radio System", *Proc. ECCTD '01*, Espoo, Finland, Aug. 2001.

[2] G. Kolumbán, M. P. Kennedy and L. O. Chua, "The role of synchronization in digital communication using chaos — Part II: Chaotic Modulation and chaotic synchronization", *IEEE Trans. Circuits Syst. I*, vol. 45, pp. 1129-1140, Nov. 1998.

[3] G. Kolumbán and B. Frigyik, "Robust chaotic communications without synchronization", *Proc. ECCTD '99*, Stresa, Italy, vol. I, pp. 445-448, Sep. 1999.

[4] E. Ott, "*Chaos in Dynamical Systems*", Cambridge, UK, Cambridge Univ. Press 1993.

[5] M. Delgado-Restituto and A. Rodríguez-Vázquez, "Piecewise affine Markow maps for Chaos Generation in chaotic Communication", *Proc. ECCTD '99* Stresa, Italy, vol. I, pp. 453-458, Sep. 1999.



(a) Bernoulli shift generator

(b) T ent generator

Figure 5: Measured IF spectra of an FM-DCSK test radio system using Bernoulli shift and "tent" mapping

[6] A. J. Viterbi, "*CDMA: Principles of Spr ead Sp ectrum Communication*", A ddison-Wesley, 1995.