PH567 - Nonlinear Dynamics Course Project

Entrainment and Communication with Dissipative Pseudorandom Dynamics

Jason Gomez, Devansh Satra, Harsh Pujare, Soham Sawant, Arjunn Pradeep

Abstract

This project explores the novel approach of utilizing dissipative pseudorandom dynamics for signal modulation and communication. By extending the principles of Linear Feedback Shift Registers (LFSRs) into their analog counterparts, Analog Feedback Shift Registers (AFSRs), we achieve optimal pseudorandom noise generation with nonlinear dissipative entrainment properties. These systems allow for efficient message encoding and retrieval through synchronization mechanisms that overcome the limitations of conventional pseudorandom modulation. By developing both discrete and continuous-time dynamical models, we demonstrate the practical applications of these systems in communication protocols that combine the robustness of chaotic designs with the simplicity of digital spread-spectrum techniques. Our findings are inspired by and build upon the work of Gershenfeld and Grinstein in their seminal paper on this subject[1].

1 Introduction

Almost all communications and measurement systems benefit from modifying signals to make them appear to be as random as possible. We introduce a new class of discrete and continuous-time dynamical systems with dissipative pseudorandom (statistically random but generated using deterministic functions using a repetitive process with a very large repeat cycle $\sim 10^{20}$) dynamics. These new dynamical systems will provide an interesting environment to explore nonlinear entrainment (in simpler words the frequency locking of two oscillating dynamical systems), and for practical communications applications combine the best features of digital spread-spectrum and chaotic designs.

A common method for introducing randomness is to modify the message of interest, $m(t)$, by a deterministic pseudorandom noise signal, $x(t)$. Modulation strategies include transmitting the product $T(t) = x(t)m(t)$, "masking" the signal $T(t) = x(t) + m(t)$, or a combination of both . A receiver with an identical copy of the noise source can generate an output, $y(t)$, identical to $x(t)$, and hence recover $m(t)$ from the received $T(t)$.

However the receiver doesn't know the correct initial conditions, therefore, recovery of the message is quite difficult. A more convenient synchronization method is suggested by the observation that two chaotic dynamical systems can entrain (or "lock"), so that their states become identical.

2 Linear Feedback Shift Registers (LFSRs)

We use digital LFSRs to produce the pseudorandom noise. They consist of a single binary variable x_n updated in discrete values according to the equation

$$x_n = \sum_{i=1}^{N} a_i x_{n-i} \pmod 2 \tag{1}$$

We choose a_i to be either zero or one such that its Z transform is not factorisable which implies that the period has the maximum possible value $2^N - 1$. For many values of a given order N just two non zeroes a_i's are needed so as to make the periodicity of the LFSR sequence to be maximal. For instance, if the update rate is set to be 1 GHz, and we take N's exceeding 90 we get the period on a time scale that exceeds the age of the Universe.

LFSRs produce deterministic signals with optimal pseudorandom properties, such as a flat power spectrum (Spectral flatness quantifies how much a signal resembles a pure frequency wave as opposed to being noise-like. High flatness implies the energy distribution of the noise signal is uniform.) within one repeat cycle. However this noise is cryptographically weak, as it is possible to predict the sequence from a short prefix of the sequence using the Berlekamp-Massey algorithm.

Moreover LSFRs cannot entrain due to their digital nature (although they can be entrained when epsilon = 1 in Equation 6) so we convert it to AFSRs

3 Analog Feedback Shift Registers (AFSRs)

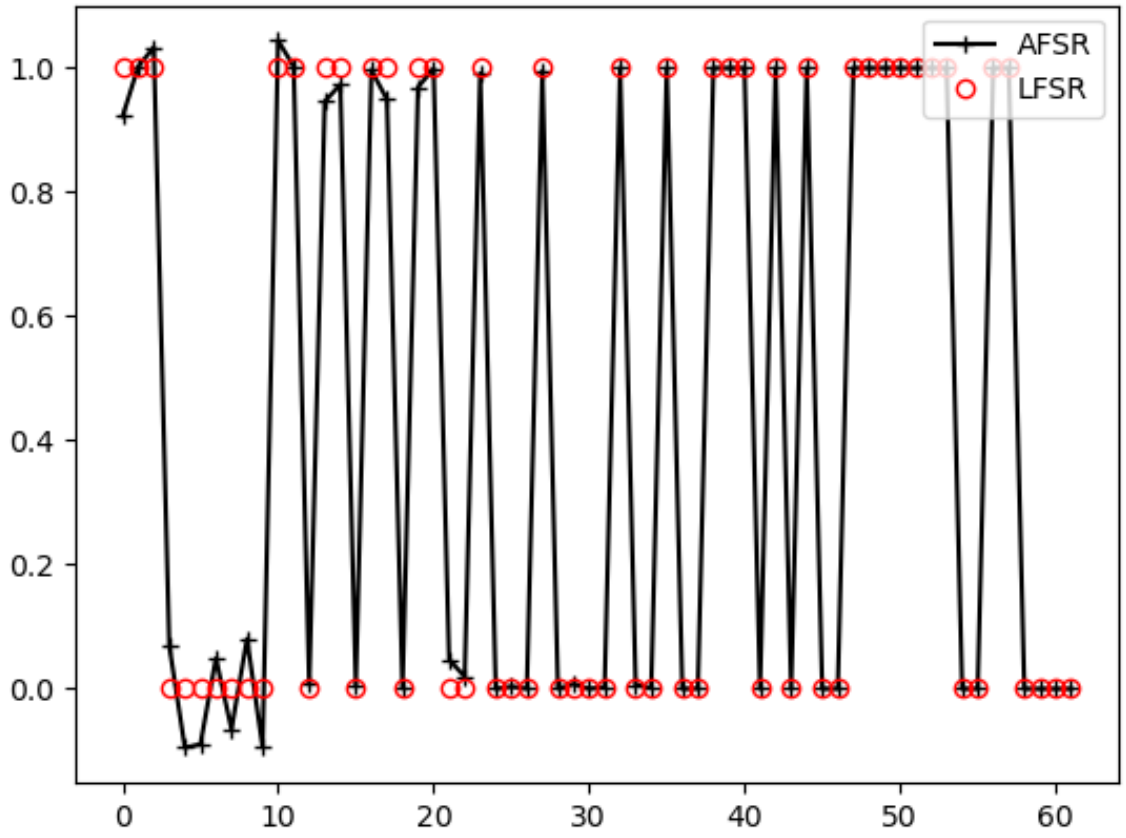
AFSRs are designed in such a way that it has fixed points at integral values and unstable fixed points in between these integral values. To achieve this, we replace the (mod 2) function with a continuous function that is equal to it and has a slope of magnitude less than one for integer arguments because if the slope is greater than 1 then the attractors (integral points) become unstable.

We need the AFSR to have stable attractors (have an attracting basin around those points) at -1 and 1 since unstable attractors would lead to outputs diverging from -1 and 1 in the vicinity of these integer values. We can achieve this using the relation

$$x_n = \frac{1}{2}\left[1 - \cos\left(\pi \sum_{i=1}^{N} a_i x_{n-i}\right)\right] \tag{2}$$

where the a_i's are selected as in the LFSR.

In a N-dimensional hyperspace the LFSR values comprise the corners of a N-dimensional Hypercube. The AFSRs approach a limit cycle of period $2^N - 1$ on the corners corresponding to the LFSR with the same a_i. Thus after some time the AFSR will converge to the LFSR pseudorandom noise. For an illustration of the above, see the below image. An advantage of Equation (2) is that it can take continuous variables as inputs which can be used in optical systems to and permits the AFSR to run at very high frequencies.



4 Encryption and Decryption using Entrainment of AFSRs

Consider the system:

$$x_n = -\cos\left(\pi \sum_{i=1}^{N} a_i \frac{1 + x_{n-i}}{2}\right) \tag{3}$$

$$T_n = x_n(1 + \mu m_n) \tag{4}$$

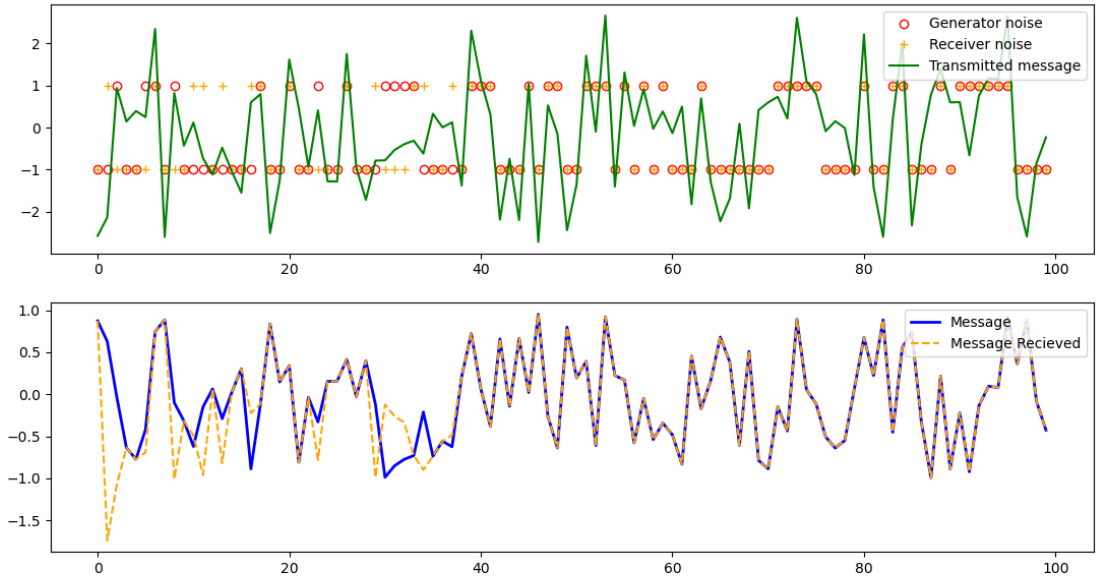
$$y'_n = -\cos\left(\pi \sum_{i=1}^{N} a_i \frac{1 + y_{n-i}}{2}\right) \tag{5}$$

$$y_n = \begin{cases} y'_n & \text{if } ||T_n| - 1| > \delta \\ (1-\epsilon)y'_n + \epsilon \ \text{sgn}(T_n) & \text{otherwise} \end{cases} \tag{6}$$

Equation (3) is the noise generated by the receiver,the AFSR equation has been modified to make the fixed points ± 1 rather than 0 and 1. The transmitted signal T_n in Equation(4) is generated by modulating the message m_n with the noise x_n . The receiver has an identical noise equation to that of x_n but with a different initial condition.

To overcome this the noise of the receiver y_n updates by taking a piece of the transmitted message $\epsilon \text{sgn}(T_n)$ according to Equation (6) whenever the absolute value of the transmitted signal T_n is in

a δ range within ± 1. Whenever it is not we move on to the next iteration and repeat the process until we get the desired result. Choosing δ such that $0 < \delta < 2 - \mu$ guarantees that $\text{sgn}(T_n) = x_n$, so this tries to lock y_n with x_n. Knowing T_n and x_n the receiver can deduce the message m_n using Equation 4.



5 Small modulation approximation

If we take μ to be small enough, then Equation (6) can be reduced to

$$y_n = (1 - \epsilon)y'_n + \epsilon T_n \tag{7}$$

The $(1-\epsilon)y'_n$ term is the autonomous dynamics and the ϵT_n is responsible for the locking. ϵ therefore controls the tradeoff between time required for locking and accuracy of the retrieval (which can be neglected once locking has occurred by taking $\text{sgn}(y_n)$ rather than y_n)
When $\epsilon = 0$ the incoming signal does not influence the receiver, so there can be no synchronization. If $\epsilon = 1$, the receiver has no dynamics of its own, which decreases quality of message retrieval.

6 AFSR's with Continuous Time Dynamics

So far we have been discussing equations related to discrete time dynamics. It is more desirable for the AFSR to produce a noise with continuous time dynamics. To do this we consider the following system

$$\dot{x} = \epsilon_1(x - x^3) + A\theta(z(t) - z_c)\cos\left(\pi\frac{1 + x(t - 1/2)}{2}\right)$$

$$\left[1-\cos\left(\pi\sum_{i=2}^{N}a_i\frac{1+x[t-(2i-1)/2]}{2}\right)\right] \tag{8}$$

This equation produces a continuous noise signal whose values are close to ± 1 except for the transition points which may occur at integer values of time. The first term is a stable attractor with fixed points at ± 1 and an unstable fixed point at 0. This drives the function to the values ± 1. $\theta(z - z_c)$ is a function that takes the value 1 when $z > zc$ and 0 otherwise. If we take z_c to be a value slightly less than 1, then the noise is allowed to reach the stable fixed points for non integral values of t.

The product of the (cos) and $(1 - \cos)$ factors in this term is -2 if a $1 \to -1$ transition is needed, 2 for a $-1 \to 1$ transition, and 0 otherwise (when no transition is needed). The coefficient A is chosen to ensure that the net change in x produced by a kick has magnitude 2, i.e., for infinitesimal kick durations, $A \to \pi/\arccos(z)$. The receivers signal y_n can be generated in a similar fashion to Equation (8) by multiplying it with a forcing term $\epsilon_2[T(t) - y(t)]$ which kicks the y_n onto the x_n. We also need to replace the θ function by $\theta(|dT(t)/dt| - d_c)$ which mimics the use of δ in Equation (6).

7 Modifications and Improvements

Equation (6) can be improved to

$$y_n = \begin{cases} y'_n & \text{if } |T_n| < 1 - \delta \\ (1-\epsilon)y'_n + \epsilon \ \mathrm{sgn}(T_n) & \text{otherwise} \end{cases} \tag{9}$$

This decreases the locking time by 100 times in some cases (only tested for $\mu = 1.8, \delta = 0.2, \epsilon = 1$, decreased the average amount of time for locking from 7000 to 70, tested for 10000 cases)

8 Conclusion and Future Scope

This paper comes up with equations through which we can recover the continuous time message from our transmitted signal easily. Using equations similar to Equation (8) (with an additional term which locks $y(t)$ onto $x(t)$ and a change of inputs to the θ function which generates transitions in synchrony with those of $x(t)$ only when the derivative of the received signal exceeds a threshold) it recovers our message embedded in the noise.

In summary, they have introduced a new class of dynamical systems with dissipative pseudoran dom dynamics. They provide an interesting environment to explore non-linear entrainment, and can be practically applied in communications applications, combining the best features of digital spread-spectrum and chaotic designs.

Currently the author has been granted a patent for his invention. It is a system that modulates a pseudo-random noise with an analog message signal and includes, in a receiver that demodulates the modulated signal, an "analog" generalization of a linear feedback shift register. The analog feedback shift register (AFSR), which is both non-linear and dissipative, directly uses samples of the received signal to synchronize to that signal. The AFSR is thus coupled to the transmitter through

the received signal. The system is non-chaotic and uses non-correlated (i.e., "ideal") pseudo-random noise to modulate a message. Synchronization of the transmitter and receiver in this nonlinear and dissipative system is possible because of the coupling.
Link to code : https://bit.ly/3E6y0nF

References

[1] N. Gershenfeld and G. Grinstein. Entrainment and communication with dissipative pseudorandom dynamics. *Phys. Rev. Lett.*, 74:5024–5027, Jun 1995. doi: 10.1103/PhysRevLett.74.5024. URL https://link.aps.org/doi/10.1103/PhysRevLett.74.5024.