Entrainment and Communication with Dissipative Pseudorandom Dynamics

N. Gershenfeld

Physics and Media Group, Massachusetts Institute of Technology Media Lab, Cambridge, Massachusetts 02139

G. Grinstein

IBM Research Division, T.J. Watson Research Center, Yorktown Heights, New York 10598

(Received 21 November 1994)

We introduce a new class of dynamical systems, analog generalizations of linear feedback shift registers, that can be designed with any number of degrees of freedom, generate optimal pseudorandom noise, and exhibit nonlinear dissipative entrainment which can be used to decode signals in communication and measurement applications.

PACS numbers: 05.45.+b, 43.72.+q

Almost all communications and measurement systems benefit from modifying signals to make them appear to be as random as possible; the benefits can include lower peak power, greater channel sharing, higher resolution timing measurements, better satisfaction of channel coding constraints, lower probability of unintended reception, and improved resistance to interference, eavesdropping, and jamming [1]. A common method for introducing randomness is to modify the message of interest, $m(t)$, by a deterministic pseudorandom [2] noise signal, $x(t)$. Modulation strategies include transmitting the product $T(t) = x(t)m(t)$ (thereby convolving or “spreading” the power spectrum), “masking” the signal $T(t) = x(t) + m(t)$, or a combination $T(t) = x(t)[1 + m(t)]$ [3]. 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 $T(t)$. In practice, however, one does not know the correct initial condition to apply at the receiver, so $y(t)$ and $x(t)$ will differ. Recovery of the message therefore typically requires a cumbersome search, acquisition, and tracking strategy for synchronizing $y(t)$ with $x(t)$ [1].

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, if they are suitably coupled (for example, by a forcing term proportional to the difference between one or more of the corresponding variables of the two systems) [4]. A chaotic receiving system locked onto a transmitter in this way can then recover a message that is modulated onto the coupling term [5]. In such a communications application, the dynamical systems serve two purposes: the positive Lyapunov exponent(s) produces noise by amplifying small fluctuations, and the dissipation produces the lower-dimensional attractor needed for entrainment [6]. Although this idea is appealingly simple, most chaotic systems produce “noise” that is far from random. A filter can be used to flatten the power spectrum of a chaotic system, but this will not remove the higher order correlations [7].

In this paper we introduce a new class of dissipative nonlinear dynamical systems that generate ideal pseudorandom noise and can recover even large messages through simple entrainment. These systems, which work in either discrete or continuous time, are analog generalizations of digital linear feedback shift registers (LFSR’s), commonly employed as pseudorandom noise generators in conventional spread-spectrum applications [1]. We briefly review some familiar aspects of LFSR’s before describing the analog generalization. LFSR’s produce deterministic signals with optimal pseudorandom properties, such as a flat power spectrum within one repeat cycle. They consist of a single binary variable $x_n$ updated in discrete time $n$ by

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

(1)

The coefficients $a_i$ are either 0 or 1 (with $a_N = 1$), and are chosen so that the $z$ transform of Eq. (1) does not factor, which implies that the repeat time of the sequence $x_n$ has its maximum possible value, $2^N - 1$ (one state is missing because the state of all zeros is a fixed point). Such irreducible polynomials [on the Galois field GF(2)] producing maximal sequences can be found by applying Euclid’s algorithm [1]. Convenient tabulations exist of maximal polynomials with the minimum number of nonzero $a_i$’s (“taps”) needed for a given order $N$; for many values of $N$ just two taps are needed [1]. The periodicity of an LFSR sequence can readily be made so long as to be undetectable: if the update rate is 1 GHz, then $N$’s that exceed $\sim 90$ yield repeat times longer than the age of the universe. A spread-spectrum scheme based on pseudorandom noise from an LFSR is cryptographically weak [8], but has all of the desirable attributes described in the introduction.

The state space of an LFSR comprises the corners of an $N$-dimensional hypercube (one axis for each time delay), and a maximal sequence visits each corner once in a cycle. Because they are digital, LFSR’s cannot entrain. To produce an analog version capable of entrainment, we replace the mod2 function in Eq. (1) by a continuous function that is equal to it for integer arguments, has a slope of magnitude less than one in the vicinity of
these integer values, and necessarily then has unstable fixed points between the integer values. This makes the maximal sequence of the LFSR a stable attractor. An example is the trigonometric function

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

where the \( a_i \)'s are selected just as in the LFSR, although the function need not be symmetrical or even strictly periodic. We call this an analog feedback shift register (AFSR). It has an attracting basin around the limit cycle of period \( 2^N - 1 \) on the corners of the hypercube corresponding to the LFSR with the same \( a_i \)'s. Starting from arbitrary initial conditions that lie in this basin, an AFSR will therefore produce, in the long-time limit, ideal pseudorandom noise governed by the well-developed theory of LFSR design. This is illustrated for \( N = 12 \) by Fig. 1, which shows an LFSR sequence generated by \( x_n = x_{n-1} + x_{n-4} + x_{n-6} + x_{n-12} \mod 2 \), with an initial condition of all 1's, and the relaxation onto this limit cycle by a corresponding AFSR with an initial state of all 1's perturbed by random numbers chosen from a uniform distribution on the interval \((-0.1, 0.1)\).

AFSR's are a particular example of the general result that digital functions always admit analog generalizations [9]. Conventional spread-spectrum systems usually have an analog front end to convert received signals to digital symbols; an AFSR can be viewed as merging the front end detector with the LFSR. Another advantage of Eq. (2) is that it can be implemented by a physical system with continuous variables. For example, for a two-tap AFSR an optical system can represent \( x_n \) by the phase of the light, the time delays can be implemented by two appropriately spaced beam splitters, and the AFSR function realized by coherently summing the delayed beams and using the intensity to drive an optical phase shifter (similar to the use of a photorefractive material to build an optical phase-locked loop [10]). This may permit AFSR's to run at very high frequencies.

We now explain how the global entrainment properties of AFSR's can be used to code and recover messages. Consider the following system:

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

\[ T_n = x_n (1 + \mu m_n), \tag{4} \]

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

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

The transmitted signal \( T_n \) is generated by modulating the message \( m_n \) with a pseudorandom signal \( x_n \) generated at the transmitter by an AFSR (or the corresponding LFSR); \( \mu > 0 \) is the magnitude of the modulation, while \( |m_n| \) is taken to be \( < 1 \). Unlike in Eq. (2), \( x_n \) in (3) has been scaled so that the fixed points lie symmetrically at \(-1\) and \(1\) rather than at \(0\) and \(1\). The receiver, \( y_n \), updates its state by combining an AFSR rule identical to that of the transmitter with a piece, \( \epsilon \text{sgn}(T_n) \), of the transmitted signal (where \( 0 \leq \epsilon \leq 1 \)). Note that \( \text{sgn}(T_n) \) is fed in to the receiver only when the message is small, i.e., \( \|T_n\| - 1 \leq \delta \). If the parameters \( \delta \) and \( \mu \) are chosen to satisfy \( 0 < \delta \leq 2 - \mu \), then this condition guarantees that \( \text{sgn}(T_n) = x_n \), so feeding \( \epsilon \text{sgn}(T_n) \) tends correctly to lock \( y_n \) with \( x_n \). If \( \|T_n\| - 1 > \delta \), then \( y_n \) is allowed to free-run: \( y_n = y'_n \). For \( \epsilon \) sufficiently large, the kicks from this sporadic coupling can lock the receiver onto the transmitter, i.e., make \( y_n = x_n \), even though the modulation is large enough to give \( T_n \) and \( x_n \) opposite signs and hence make this locking impossible to achieve through simple inspection. Knowing \( T_n \) and \( x_n \), one can immediately deduce \( m_n \). The locked state is a stable attractor achieved for a broad set of initial conditions of the receiver [11]. To illustrate, Fig. 2 shows the state of the transmitter \( x_n \) (circles) and receiver \( y_n \) (pluses) recovered by Eq. (6) from a transmitted signal incorporating a message uniformly randomly distributed between \(-1\) and \(1\), with \( \mu = 1.8 \), \( \delta = 0.2 \), and \( \epsilon = 1 \). This use of irregular perturbations to produce locking is similar to the use of occasional feedback in controlling chaos [12,13].

If one restricts \( \mu \) to be sufficiently small, approximate message retrieval can be achieved by replacing Eq. (6) with a simpler receiver equation that is always applied, similar to those used for entrainment in chaotic systems:

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

Here the term \( \epsilon T_n \) is responsible for the approximate entrainment of \( y_n \) to \( x_n \), and hence the approximate recovery
perturbed by the message, enabling it to produce a better estimate of the transmitter's state $x_n$ and hence of the message. While the recovery error can be reduced by adding a similar forcing term to the transmitter \cite{5(b)}, the sensitivity of the receiver to channel noise will still depend on the coupling strength. Figure 3 shows the error $y'_n - x_n$ as a function of $\epsilon$ for short times, the dependence on $\epsilon$ of the time to lock, and the variance of the error after locking (all for $\mu = 0.01$). The functional dependence of the locking time on the register length and signal strength is currently being investigated. The approximate linear dependence of the asymptotic error on $\epsilon$ for small $\epsilon$ can be understood by recognizing that, if the error in the receiver's state is $\Delta = \sum_{i=1}^{N} (x_{n-i} - y_{n-i})$, then $|y'_n| \sim ||\Delta|| = |\Delta| = \pi^2 \Delta^2 / 8$. One iteration of the AFSR function thus reduces the error in the new value $y'_n$ from $O(\Delta)$ to $O(\Delta^2)$, and so to first order in $\Delta$ the error in $y_n$ is just equal to the amount of the message coupled in, which is proportional to $\epsilon$. Instead of keeping $\epsilon$ constant, it is also possible to start with $\epsilon$ large to lock quickly and then decrease it to reduce the error.

Equations (3) and (5) are discrete-time maps, requiring the transmitter and receiver clocks to be synchronized. This timing recovery can be done with a phased-lock loop, but it is also possible to generalize the AFSR map to continuous-time dynamics. Beyond the obvious relevance for applications, the construction of continuous-time systems with the desirable noise characteristics of the AFSR's is of theoretical interest. We now describe how to accomplish this task.

Consider the following delay-differential equation:

$$
\frac{dx}{dt} = \epsilon_1 (x - x^3) + A \theta(z(t) - z_c) \cos\left(\frac{\pi \cdot 1 + x(t - 1/2)}{2}\right) \left[1 - \cos\left(\frac{\pi \cdot \sum_{i=2}^{N} a_i \cdot 1 + x(t - (2i - 1)/2)}{2}\right)\right], \tag{8}
$$

where $\epsilon_1(>0)$, $z_c(<1)$, and $A$ are positive parameters, and $z(t) = \cos(2\pi t)$ is a forcing function with unit period. Equation (8) produces a continuous pseudorandom noise signal $x(t)$ with $x(t) \approx \pm 1$, except for $t$'s very close to integer
values, where transitions between +1 and −1 may occur, mirroring the sign changes of the discrete-time AFSPR with the same set of \(a_i\)'s. The first term drives \(x(t)\) toward fixed points at ±1, with a speed governed by \(\epsilon_1\). Since \(\theta(z - z_c) = 1\) for \(z > z_c\) (and equals 0 for \(z < z_c\)), choosing \(z_c\) just slightly less than 1 makes the second term apply kicks that produce the transitions. The product of the cos and \(1 - \cos\) factors in this term is \(-2\) if a \(1 \rightarrow -1\) transition is needed, \(2\) for a \(-1 \rightarrow 1\) transition, and \(0\) otherwise (when no transition is needed) \([15]\). The coefficient \(A\) is chosen to ensure that the net change in \(x\) produced by a kick has magnitude \(2\); for \(z_c \rightarrow 1\), i.e., for infinitesimal kick durations, \(A \rightarrow \pi/\arccos(z_c)\). If the sharp transitions need to be band limited, an inertial term can be added.

A continuous-time message \(m(t)\) can be recovered from the transmitted signal \(T(t) = x(t)[1 + \mu m(t)]\) through an equation similar to (8) for the receiver variable \(y(t)\). This equation differs from (8) only through the addition of a forcing term \(\epsilon_2[T(t) - y(t)]\) which tends to lock \(y(t)\) onto \(x(t)\), and through the replacement of \(\theta(z(t) - z_c)\) by \(\theta(dt(t)/dt - d_c)\), which generates transitions in synchrony with those of \(x(t)\) (i.e., only when the magnitude of the derivative of the received signal exceeds a parameter \(d_c\)). Figure 4 shows the receiver \(y(t)\) locking onto \(x(t)\) in the simplest case where \(m(t) = 0\), for \(d_c = 1.0, \epsilon_1 = 0.5, \epsilon_2 = 1.0, \text{ and } A = 4.7\).

In summary, we have introduced a new class of discrete and continuous-time dynamical systems with dissipative pseudorandom dynamics. They provide an interesting environment to explore nonlinear entrainment, and for practical communications applications combine the best features of digital spread-spectrum and chaotic designs.

We are pleased to acknowledge valuable input from Scott Kirkpatrick, Paul Horowitz, Charles Tresser, and Patrick Worfolk. N.G. is grateful for support from IBM and Hewlett-Packard.

[3] This description of modulation schemes omits the possible extra step of modulation and demodulation by a communications carrier. See Ref. [1].
[11] With regard to local stability, it is easily shown that the locked state is superstable; i.e., the appropriate Lyapunov exponent is \(-\infty\).
[14] This is a trivial kind of synchronization, similar to a self-synchronizing spread-spectrum configuration; see Ref. [1].
[15] One can also satisfy this logical relationship with products instead of sums of lags.