Physical Review Letters **74**, p. 5024 (1995)

Entrainment and Communication with Dissipative Pseudorandom Dynamics

N. Gershenfeld

Physics and Media Group, MIT Media Lab, Cambridge, MA 02139

G. Grinstein

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

(August 3, 1995)

Abstract

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 pseudo-random noise, and exhibit nonlinear dissipative entrainment which can be used to decode signals in communication and measurement applications.

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 pseudo-random [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 doesn't 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 system serves 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 pseudo-random 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 pseudo-random 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 pseudo-random 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

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

The coefficients a_i are either 0 or 1 (with $a_N = 1$), and are chosen so that the z-transform of equation (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 non-zero 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 ~ 90 yield repeat times longer than the age of the universe. A spread-spectrum scheme based on pseudo-random 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 can not entrain. To produce an analog version capable of entrainment, we replace the *mod* 2 function in equation (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

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

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 pseudo-random noise governed by the well-developed theory of LFSR design. This is illustrated for N=12 by Figure 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 equation (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 photo-refractive 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:

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

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

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

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

The transmitted signal T_n is generated by modulating the message m_n with a pseudo-random signal x_n generated at the transmitter by an AFSR (or the corresponding LFSR); μ (> 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, $\epsilon \, sgn(T_n)$, of the transmitted signal (where $0 \leq \epsilon \leq 1$). Note that $sgn(T_n)$ is fed in to the receiver only when the message is small, i.e., $||T_n| - 1| \leq \delta$. If the parameters δ and μ are chosen to satisfy $0 < \delta \leq 2 - \mu$, then this condition guarantees that $sgn(T_n) = x_n$, so feeding $sgn(T_n)$ 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 ϵ 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, Figure (2) shows the state of the transmitter x_n (circles) and receiver y_n (pluses) recovered by equation (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 μ 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:

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

Here the term ϵT_n is responsible for the approximate entrainment of y_n to x_n, and hence the approximate recovery of m_n. The coupling strength ϵ controls a trade-off between the time required for entrainment and the accuracy of the retrieval. When $\epsilon = 0$ the incoming signal does not influence the receiver, so there can be no synchronization. If $\epsilon = 1$, the receiver has no autonomous dynamics, and so the incoming signal simply passes through it [14]. As ϵ is decreased from 1, the receiver takes progressively longer to lock onto the signal, but its internal state is less 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 [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 ϵ for short times, the dependence on ϵ 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 ϵ for small ϵ 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 $||y'_n| - 1| = || - \cos(\pi \sum_i a_i(1 + y_{n-i})/2)| - 1| \approx \pi^2\Delta^2/8$. 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 Δ the error in y_n is just equal to the amount of the message coupled in, which is proportional to ϵ. Instead of keeping ϵ constant, it is also possible to start with ϵ 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:

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

where ϵ_1 (> 0), z_c (< 1), and A are positive parameters, and $z(t) = cos(2\pi t)$ is a forcing function with unit period. Eq. (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 AFSR with the same set of a_i's. The first term drives $x(t)$ toward fixed points at ± 1, with a speed governed by ϵ_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 $d_c = 1.0$, $\epsilon_1 = 0.5$, $\epsilon_2 = 1.0$, and $A = 4.7$.

In summary, we have introduced a new class of discrete and continuous time dynamical systems with dissipative pseudo-random 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. NG is grateful for support from IBM and Hewlett–Packard.

REFERENCES

[1] M.K. Simon et. al., *Spread Spectrum Communications Handbook* (McGraw-Hill, New York, 1994).

[2] Pseudo-random noise is a deterministic signal whose properties mimic those of random noise. See ref. [1] for a precise definition.

[3] This description of modulation schemes omits the possible extra step of modulation and demodulation by a communications carrier. See ref. [1].

[4] L.M. Pecora and T.L. Carroll, Phys. Rev. Lett. **64**, 821 (1990); C. Tresser and P. Worfolk, preprint.

[5] e.g., (a) K.M. Cuomo and A.V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993); (b) C.H. Wu and L. O. Chua, Int. J. of Bif. and Chaos **3**, 1619 (1993).

[6] R. Temam, *Infinite-Dimensional Dynamical Systems in Mechanics and Physics*, Vol. 68 of *Applied Mathematical Sciences* (Springer-Verlag, New York, 1988).

[7] T. Sauer, J.A. Yorke, and M. Casdagli, J. Stat. Phys. **65**, 579 (1991).

[8] For secure cryptographic systems see, for example, *Contemporary Cryptology: The Science of Information Integrity*, edited by G.J. Simmons (IEEE Press, Piscataway, 1992).

[9] T. Toffoli, Math. Systems Theory **14**, 13 (1981).

[10] F. Davidson and C.T. Field, IEEE Phot. Tech. Lett. **5**, 1238 (1993).

[11] With regard to *local* stability, it is easily shown that the locked state is superstable; i.e., the appropriate Lyapunov exponent is $-\infty$.

[12] E. Ott, C. Grebogi, and J.A. Yorke, Phys. Rev. Lett. **64**, 1196 (1990)

[13] R. Roy *et. al.* , Phys. Rev. Lett. **68**, 1259 (1992).

[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.

FIGURES

FIG. 1. A 12-tap LFSR register sequence (circles), and the relaxation to this sequence of a corresponding AFSR (pluses) which starts with the same initial conditions perturbed by random numbers uniformly distributed between -0.1 and 0.1.

FIG. 2. The transmitted signal T_n (solid), transmitter state x_n (circles), and receiver state y_n (pluses), from Eqs. (3–6) with m_n uniformly randomly distributed between -1 and 1, $\mu = 1.8$, $\delta = 0.2$, and $\epsilon = 1$, showing locking with μ large enough to give x_n and T_n different signs.

FIG. 3. A LFSR coupled to an AFSR by equations (3–5, 7). The left plot shows the time dependence of the error $y'_n - x_n$ as a function of the coupling constant ϵ, the middle plot shows the time to lock for an ensemble of 100 random initial conditions (the solid line connects the average locking times), and the right plot shows the standard deviation of the error after locking.

FIG. 4. A continuous time AFSR (solid line) with a random initial condition, locking onto the signal from a transmitter (dashed line), for $m(t) = 0, d_c = 1.0, \epsilon_1 = 0.5, \epsilon_2 = 1.0$, and $A = 4.7$.

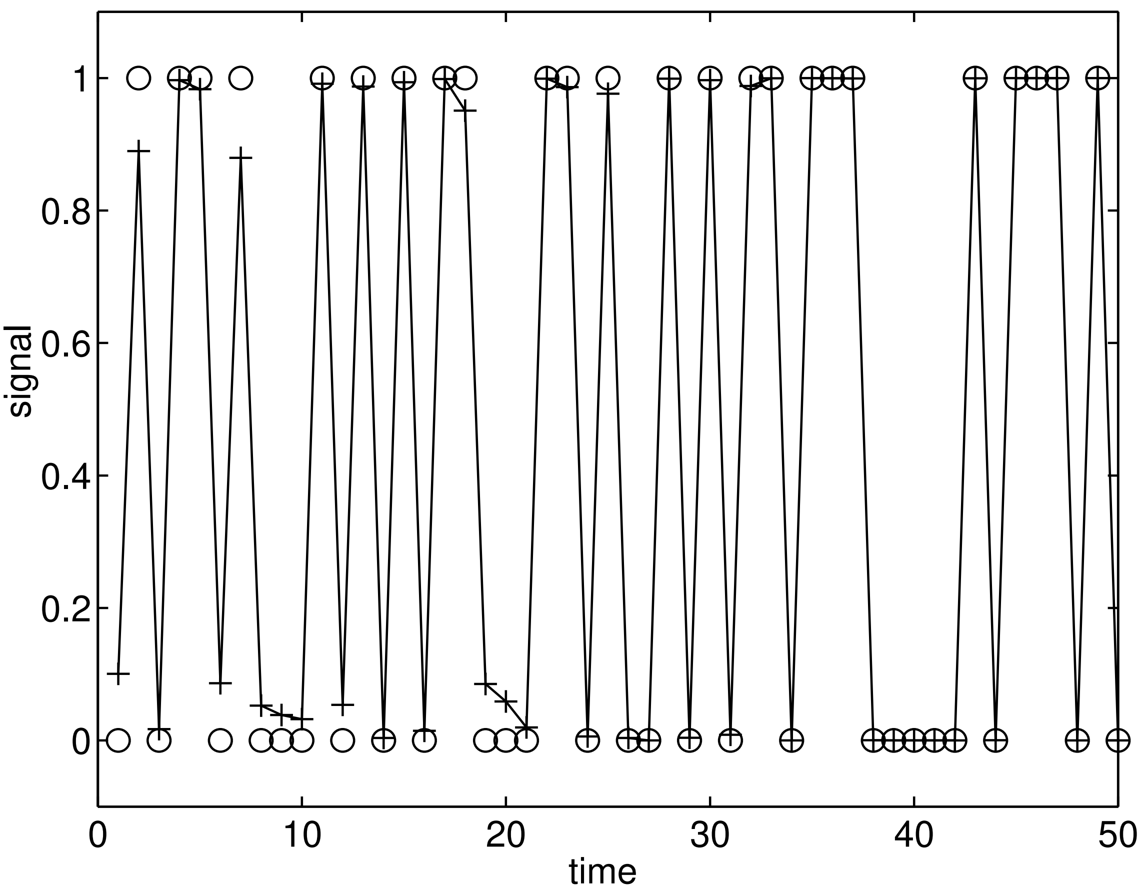


Figure 1

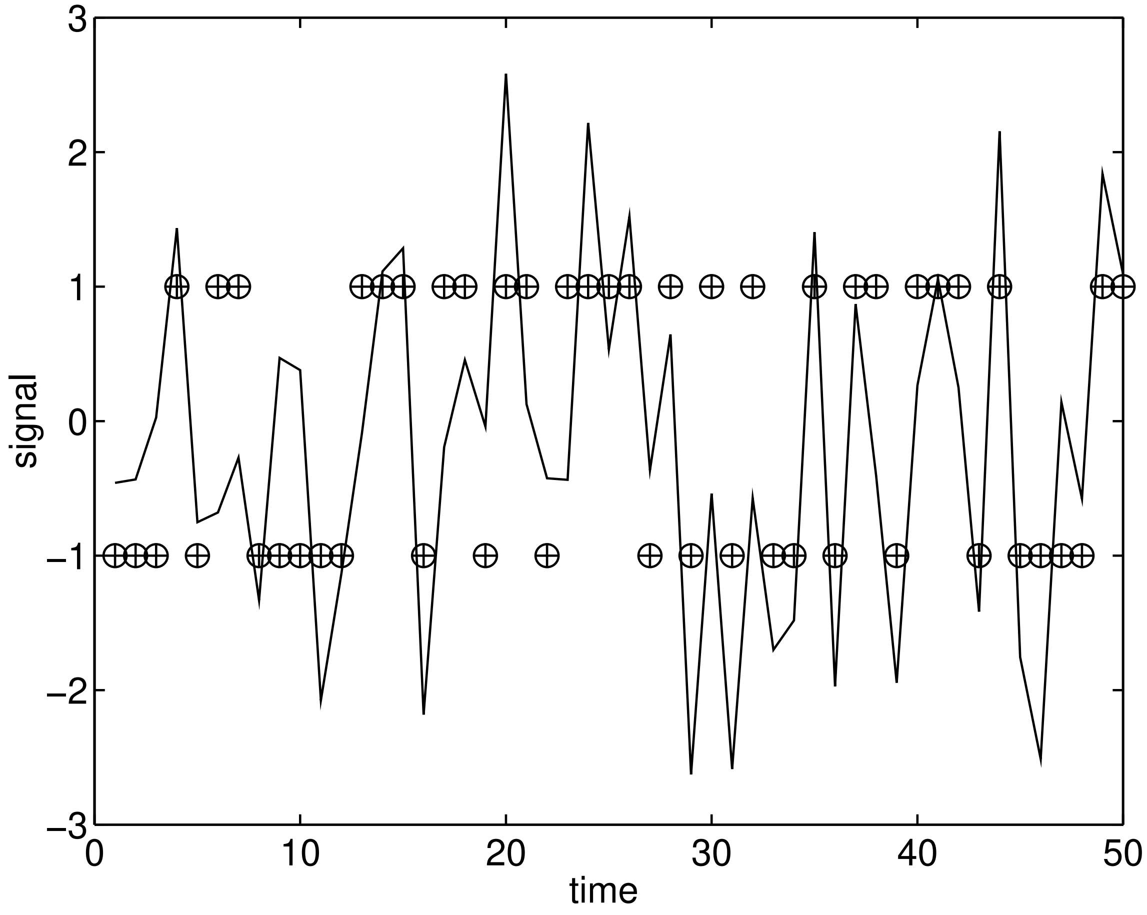
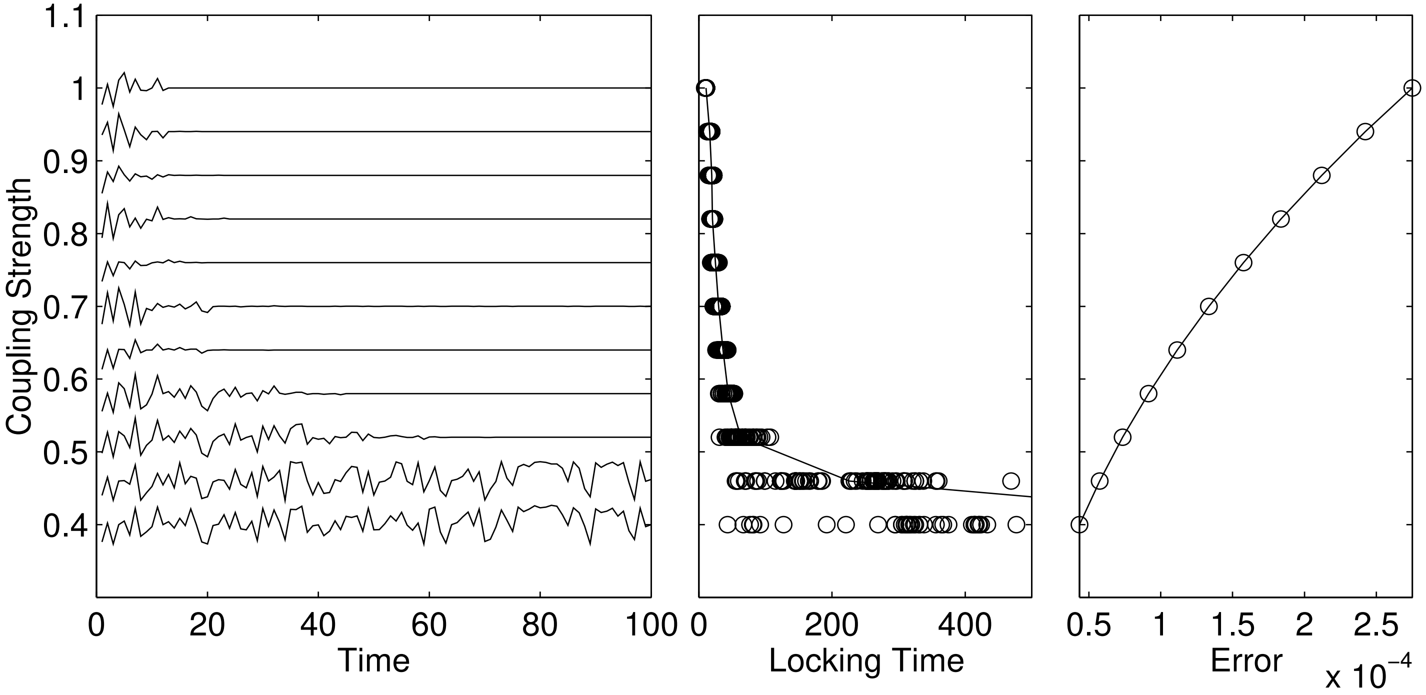


Figure 2

Figure 3



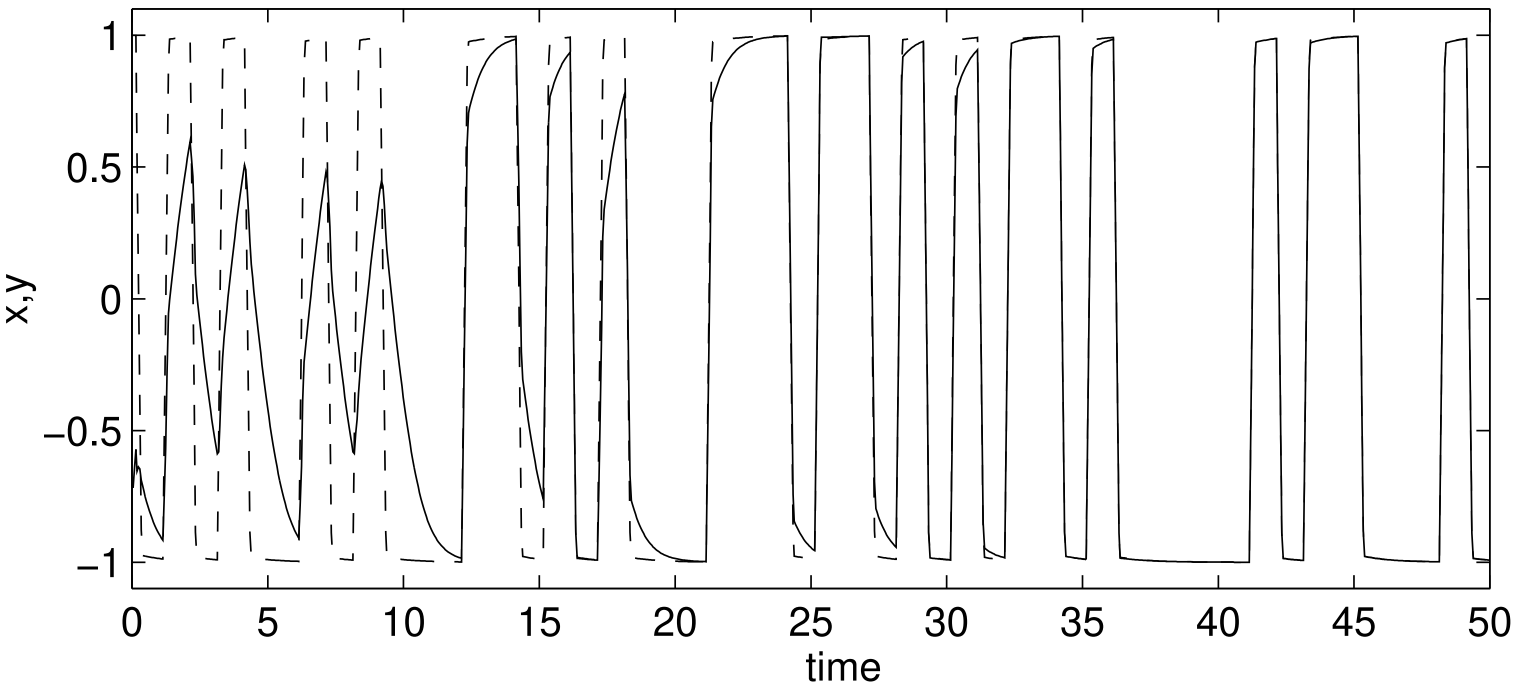


Figure 4