Sending Secret Messages with Synchronized Chaotic Systems

Kevin Phan

May 12, 2023

Abstract

This paper introduces a synchronized chaotic system based on the Lorenz system. We will see how they can be applied to the field of communications as synchronized chaotic system can be used to send secret messages. Lastly, we see how resistant this method of encryption is to noise when transmitting the signal.

Contents

1 Introduction

Chaotic systems are known for their sensitivity to initial conditions. Two trajectories that start close together can diverge from each other. Despite this, Pecora and Carroll (1990) discovered that a pair of chaotic systems can synchronize with each other, so that the trajectories are eventually the same in time [PC90].

Cuomo, Oppenheim, and Strogatz studied a pair of dynamical systems based on the Lorenz system and use it to encrypt messages in the field of communications [CO93; COS93b; COS93a]. In particular, they have shown that the pair of dynamical systems do synchronize and synchronization is exponential, built an algorithm to send secret messages, and how noise can affect the quality of transmission.

In this paper, we followed in their footsteps by showing the properties of the synchronized dynamical system and report the same findings that they found. However, a numerical algorithm is implemented rather than using circuits which allow for better reproducibility.

2 Theory of Synchronized Chaotic Systems

Two dynamical systems are synchronized when the two dynamical systems' trajectories are eventually identical as time $t \to \infty$. A definition of synchronization is given by He and Vaidya [HV92].

Definition 2.1. *Let* $\dot{\mathbf{x}} = f(t, \mathbf{x})$ *and* $\dot{\mathbf{y}} = g(t, \mathbf{y})$ *be two dynamical systems, where* t *is time and* $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$*. Let* $\mathbf{x}(t; t_0, \mathbf{x}_0)$ *and* $\mathbf{y}(t; t_0, \mathbf{y}_0)$ *be solutions to the dynamical systems respectively. We say that the two dynamical systems synchronize if there exists a subset of* $\mathbb{R}^n$*, denoted* $D(t_0)$*, such that* $\mathbf{x}_0, \mathbf{y}_0 \in D(t_0)$ *implies*

$$||\mathbf{x}(t; t_0, \mathbf{x}_0) - \mathbf{y}(t; t_0, \mathbf{y}_0)|| \to 0 \text{ as } t \to +\infty.$$

If the region of synchronization $D(t_0) = \mathbb{R}^n$*, we say that the synchronization is global. Otherwise, the synchronization is local.*

Note synchronization does not depend on the initial conditions of the dynamical systems.

One example of a synchronized system is given by Cuomo and Oppenheim which was used to send secret messages:

$$\begin{aligned} \dot{x_T} &= \sigma(y_T - x_T), \\ \dot{y_T} &= rx_T - y_T - 20(x_T z_T), \\ \dot{z_T} &= 5x_T y_T - bz_T, \end{aligned} \tag{1}$$

which is the transmitter's dynamical system and

$$\begin{aligned} \dot{x_R} &= \sigma(y_R - x_R), \\ \dot{y_R} &= rx_T - y_R - 20(x_T z_R), \\ \dot{z_R} &= 5x_T y_R - bz_R, \end{aligned} \tag{2}$$

which is the receiver's dynamical system [CO93]. Notice that the only state variable of the transmitter's dynamical system that appears in the receiver's dynamical system is x_T. This means that only information that the receiver need to know to reconstruct the trajectory of the transmitter's dynamical system is data about x_T. Furthermore, this pair of dynamical system is the same as the Lorenz system after doing a change of variables. Hence, this pair of chaotic system is also chaotic.

Cuomo and Oppenheim proved that the synchronization occurs using a Lyapunov function to show that the error asymptotically approaches the point $\mathbf{0} \in \mathbb{R}^3$ [CO93].

Theorem 2.1. *The pair of dynamical systems given by equations 1 and 2 are globally synchronized.*

Proof. Let $e_x = x_T - y_T$, $e_y = y_T - y_R$, and $e_z = z_T - z_R$. This gives us the dynamical system

$$\begin{aligned} \dot{e_x} &= \sigma(e_y - e_x), \\ \dot{e_y} &= -e_y - 20 e_z x_T, \\ \dot{e_z} &= 5 e_y x_t - b e_z, \end{aligned} \tag{3}$$

which describes the error between each component of the trajectories given by transmitter and receiver's dynamical system. Let $\mathbf{e} = (e_x, e_y, e_z)^T$. To show synchronization, it is sufficient to show that for equation 3, the fixed point $\mathbf{0}$ is asymptotically stable. By inspection, $\mathbf{0}$ is a fixed point of equation 3 and $V(\mathbf{e}) > 0$ for all $\mathbf{e} \neq 0$.

To show that it is asymptotically stable, we use a Lyapunov function. Let $V(\mathbf{e}) = \frac{1}{2}\left(\frac{1}{\sigma}e_x^2 + e_y^2 + 4e_z^2\right)$. By inspection, we see that $V(\mathbf{0}) = 0$ and $V(\mathbf{e}) > 0$ for all $\mathbf{e} \neq 0$.

Taking the time derivative of V and substituting for e_x, e_y, e_z using equation 3, we get

$$\begin{aligned}
\dot{V} &= \frac{1}{\sigma}e_x\dot{e_x} + e_y\dot{e_y} + 8\dot{e_z} \\
&= \frac{1}{\sigma}e_x(\sigma e_y - \sigma e_x) + e_y(-e_y - 20x_Te_z) + 4e_z(5x_Te_y - be_z) \\
&= -e_x^2 + e_xe_y - e_y^2 - 4be_z^2 \\
&= -\left(e_x - \frac{1}{2}e_y\right)^2 - \frac{3}{4}e_y^2 - 4be_z^2,
\end{aligned}$$

where the last step is completing the square. Thus, for all $\mathbf{e} \neq \mathbf{0}$, $\dot{V} < 0$. As such, V is a Lyapunov function, so all trajectories of V flow toward the fixed point $\mathbf{0}$. This means that the error goes to 0 which prove that the pair of dynamical systems given by equations 1 and 2 are globally synchronized. $\square$

However, the definition of synchronization does not tell us how fast the pair of dynamical systems will synchronize. Fortunately, Cuomo, Oppenheim, and Strogatz (1993) proved that error converge exponentially by studying the error dynamics [COS93b].[1]

Theorem 2.2. *The error dynamics of equations 1 and 2 given by equation 3 converge to* $\mathbf{0}$ *exponentially.*

Proof. Consider the function $V(e_y, e_z) = \frac{1}{2}e_y^2 + 2e_z^2$. We wish to show that $\dot{V} \leq -kV$ where $k < \min\{2, 2b\}$. Taking the time derivative and substituting for e_y, e_z using equation 3, we get

$$\begin{aligned}
\dot{V} &= e_y\dot{e_y} + 4e_z\dot{e_z} \\
&= e_y(-e_y - 20e_zx_T) + 4e_z(5e_yx_T - be_z) \\
&= -(e_y^2 + 4be_z^2).
\end{aligned}$$

We see that $-(e_y^2 + 4be_z^2) \leq -k\left(\frac{1}{2}e_y^2 + 2e_z^2\right)$ where $k < \min\{2, 2b\}$.

[1] This is also given as Exercise 9.1 in Strogatz's Nonlinear Dynamics and Chaos [Str19].

Next, we establish that $e_2, e_3 = O(e^{-t})$. Integrating $\dot{V} = -kV$ with respect to t, we get $V(t) \leq V_0 e^{-kt}$ where V_0 is the initial condition of V. From this, we establish the inequalities

$$\frac{1}{2}e_y^2 \leq V(t) \leq V_0 e^{-kt}$$

and

$$2e_z^2 \leq V(t) \leq V_0 e^{-kt}.$$

Solving for e_y in the first inequality, we get

$$e_y \leq \sqrt{2V_0}e^{-\frac{kt}{2}}.$$

Simiarly, solving for e_z in the second inequality, we get

$$e_z \leq \sqrt{\frac{V_0}{2}}e^{-\frac{kt}{2}}.$$

This show that $e_y, e_z = O(e^{-\frac{kt}{2}})$.

Lastly, we show that $e_1 = O(e^{-t})$. From equation 3, $\dot{e_x} = \sigma(e_y - e_x)$. This can be rewritten as $\dot{e_1} + \sigma e_1 = \sigma e_2$. Since $e_y \leq \sqrt{2V_0}e^{-\frac{kt}{2}}$, we have

$$\dot{e_1} + \sigma e_1 \leq \sqrt{2V_0}e^{-\frac{kt}{2}}.$$

Multiplying by the integrating factor $e^{\sigma t}$, we get

$$(e_1 e^{\sigma t})' \leq \sqrt{2V_0}e^{\left(\sigma - \frac{k}{2}\right)t}$$

Integrating and solving for e_1, we get

$$e_1 \leq \frac{\sqrt{2V_0}}{\sigma - \frac{k}{2}}e^{-\frac{kt}{2}}$$

This established that $e_1 = O(e^{-\frac{kt}{2}})$. Therefore, we proved that the error dynamics given by equation 3 converge to $\mathbf{0}$ exponentially. $\square$

Furthermore, we give a numerical example of synchronization and the error going to zero for the x-component of the dynamical system given by equations 1 and 2 with parameters $\sigma = 16$, $r = 45.6$, and $b = 4$. The initial conditions of the transmitter's dynamical system and receiver's dynamical system is $(2.2, 1.3, 2.0)$ and $(10.2, 7.3, 6.0)$ respectively. From the plot, the dynamical systems synchronize at $t \approx 2$ and the error goes to 0 and remains at 0 for $t > 2$.

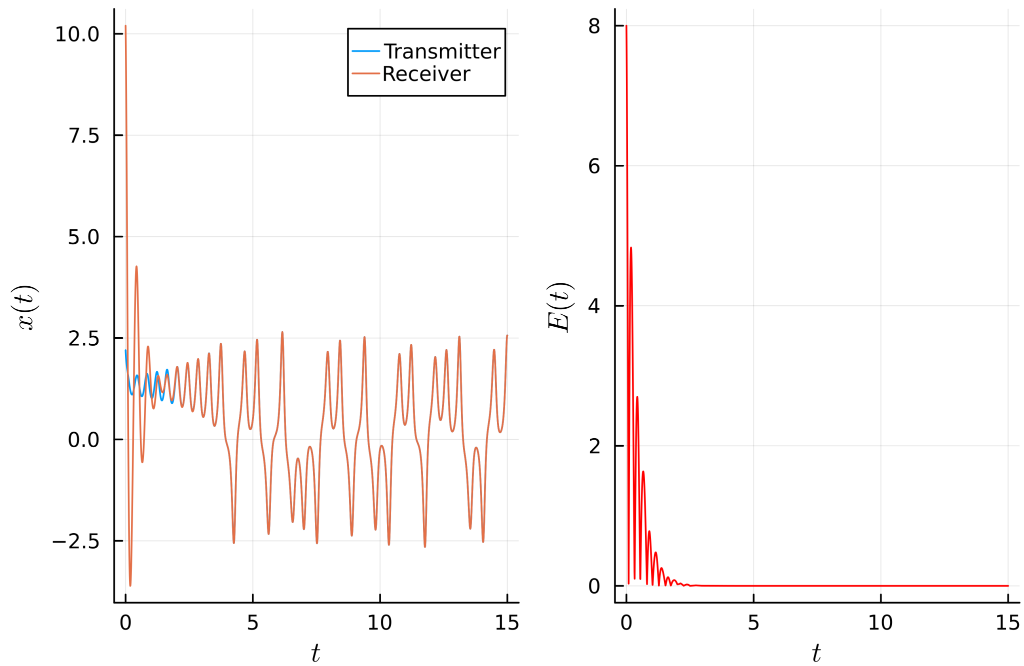

Figure 1: Plot of the x-component of both the transmitter and receiver's dynamical systems. The error $E(t) = |x_T - x_R|$ exponentially decrease to 0.

3 Applications to Communication and Numerical Experiments

We explore how synchronized chaotic systems can be used to encrypt messages.

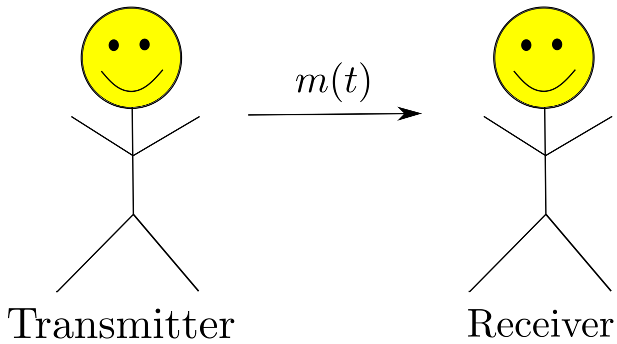

Figure 2: The transmitter want to send a message $m(t)$ to the receiver and want no one else to be able to read it.

Consider two people: Transmitter and Receiver. Transmitter want to send a message $m(t)$ to Receiver. However, the message should not be able to be read by anyone, but the Receiver. Cuomo and Oppenheim show that one way of approaching this problem is by using synchronized chaotic system [CO93]. The core idea is to send the sum of the message $m(t)$ and the trajectory of the transmitter's dynamical system, use the receiver's dynamical system to reproduce the actual trajectory of the transmitter's dynamical system, and use this to directly compute $m(t)$. In their paper, they create a circuit implementation that capture the same behavior as the pair of dynamical systems in equations 1 and 2. Compared to their paper, we will use the same algorithm by Cuomo and Oppenheim, but implement the algorithm numerically.

3.1 Algorithm Implementation

Let $m(t)$ be the message the transmitter want to send to the receiver. The numerical algorithm is given below.

1. Create the encrypted message $\widetilde{m}(t) = x_T(t) + m(t)$ where $||m(t)|| \ll ||x_T(t)||$.

2. Send the encrypted message $\widetilde{m}(t)$ to the receiver.

3. Use the receiver's dynamical system to hopefully reproduce $x_R(t) \approx x_T(t)$.

4. Compute $\widetilde{m}(t) - x_R(t) \approx x_T(t) + m(t) - x_T(t) = m(t)$.

The first step is to create an encrypted message $\widetilde{m}(t) = x_T(t) + m(t)$ where the magnitude of $m(t)$ is much smaller than the magnitude of $x_T(t)$. This encrypts the message $m(t)$ because $x_T(t)$ serve as a mask to hide the message $m(t)$. Note that $m(t)$ can be made as small as we like by multiplying by $0 < \varepsilon < 1$. The receiver can multiply by $\frac{1}{\varepsilon}$ to get $m(t)$ back when the receiver recovers the scaled version of $m(t)$.

The second step is to send the encrypted message $\widetilde{m}(t)$ to the receiver and the third step is to use $\widetilde{m}(t)$ to reproduce $x_T(t)$. Note that in this case, $m(t)$ is noise as the receiver's dynamical system try to synchronize with $\widetilde{m}(t)$. The receiver's dynamical system is

$$\begin{aligned}
\dot{x_R} &= \sigma(y_R - x_R),\\
\dot{y_R} &= r\widetilde{m} - y_R - 20(\widetilde{m}z_R),\\
\dot{z_R} &= 5\widetilde{m}y_R - bz_R,
\end{aligned}$$

where x_R is replaced by $\widetilde{m}$ except for the equation for $\dot{x_R}$. Also, notice that the receiver's dynamical system will not perfectly recover $x_T(t)$ because of the noise $m(t)$.

The last step is to compute the message $m(t)$ which is what the transmitter want to send. In step 3, the receiver's dynamical systems hopefully reproduce $x_R(t) \approx x_T(t)$. Thus, $\widetilde{m}(t) - x_R(t) \approx (x_T(t) + m(t)) - x_T(t) = m(t)$.

In contrast to a circuit implementation of the algorithm, one concern is numerical errors. The tolerance of the differential equation solver should be set to sufficiently low values such that the digits representing $m(t)$ are not truncated or rounded when finding the solution to both dynamical systems. For this reason, we set the relative and absolute tolerance to 10^{-11}.

3.2 Transmitting a Message

In order to transmit a message, we can convert an audio file to a waveform. For instance, the `wav` library and `Wav.jl` package are both capable of reading audio files and writing them into waveforms in Python and Julia respectively. Then, a linear interpolation can be done on the signal to create the message $m(t)$. After transmitting them to the receiver, the receiver can convert the waveforms into audio files to listen to them.

We use the transformation above to transmit the audio file `taunt.wav`.[2]

[2] The audio file came from an introductory programming class taught at UIUC: `https://www2.cs.uic.edu/~i101/SoundFiles/`.

The parameters are the same as before which are $\sigma = 16$, $r = 45.6$, and $b = 4$ and the initial conditions are the same for both systems which is $(2.2, 1.3, 2.0)$. The plot of the waveforms and error between the two waveforms are shown below.

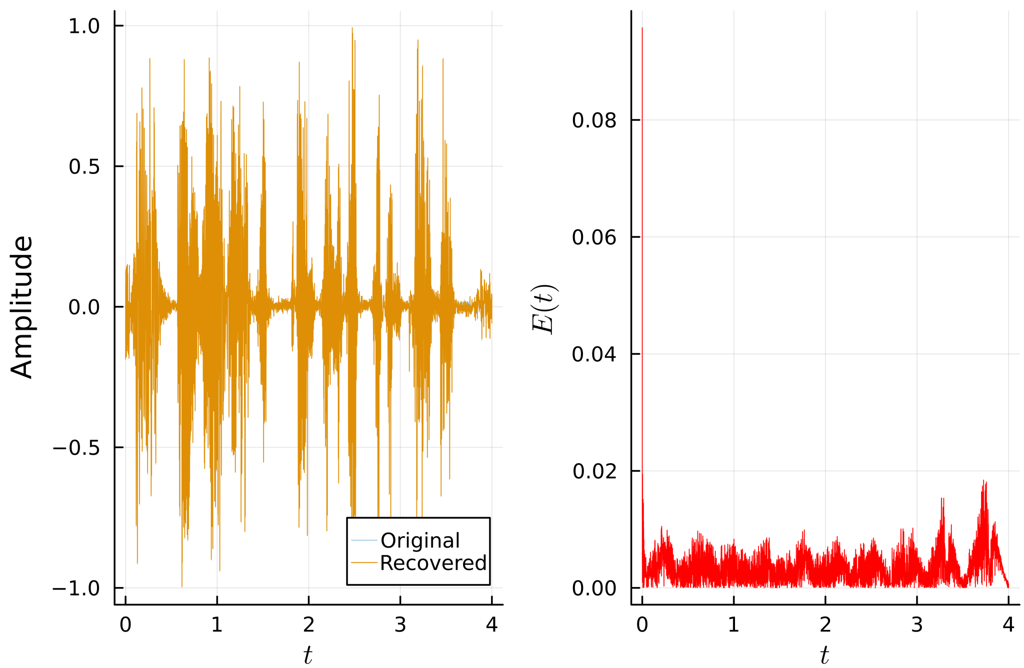

Figure 3: Plot of both waveforms and the absolute error between the two waveforms.

Notice that the error is not completely zero due to the "noise" that is $m(t)$. Despite this, the audio file produced from this is listenable and one can hear the message that is being sent.

3.3 Testing Algorithm Against Noise

In non-idealized situations, there will always be noise that is transmitted along with the signal that we want to send. Cuomo, Oppenheim, and Strogatz (1993) studied how robust the algorithm is to recovering the message in the presence of noise and why speech can still be recovered in presence of noise [COS93a]. Similar to Cuomo, Oppenheim, and Strogatz, we explore how Gaussian noise affect the quality of the recovered message in the context of the numerical algorithm.

Instead of sending the message $\tilde{m}(t) = x_T(t) + m(t)$, we send the message

$$\tilde{m}(t) = x_T(t) + m(t) + N(0, \sigma^2)$$

where $N(0, \sigma^2)$ is Gaussian noise with variance σ^2.

We test it for various standard deviations σ: $0, 0.5, 1, 2$ and determine how well the algorithm withstand against noise by plotting the error between the original message and the recovered message.

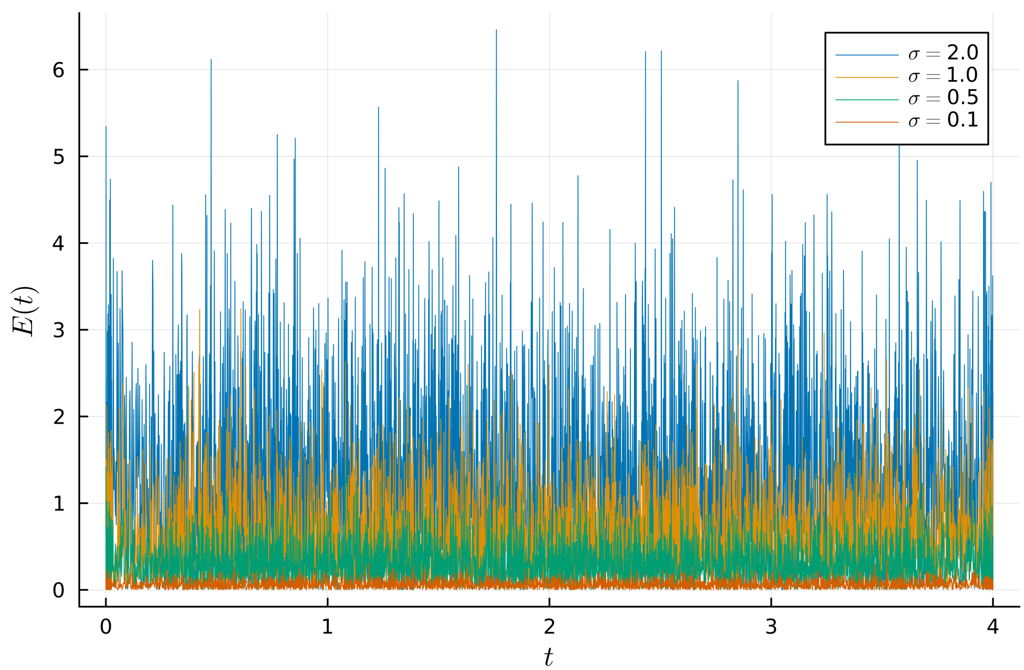

Figure 4: A plot of the absolute error between the original message and the recovered message for various values of σ.

Recall that the magnitude of a waveform is 1. As such, we might expect some distortion of the audio for $\sigma = 0.5$ or greater. However, the result was that the original message remains in the audio file, but the message is masked by static noise. As σ increases, the volume of the static noise increase which eventually drown out the original message as in the case of $\sigma = 2$. This points that the algorithm is susceptible to noise and require a near perfect transmission of the encrypted message $\widetilde{m}(t)$ to recover the message $m(t)$.

4 Conclusion

In this work, we showed that the pair of dynamical systems synchronize and the rate of convergence is exponential. Then, we show how this can be applied in the field of communications to send a secret message. This was done by a numerical algorithm which can suffer from a potential lack of numerical accuracy. This was resolved by enforcing a smaller tolerance when finding the solution to the dynamical system. We also detail how an audio message can be sent by first converting it into a waveform and doing a linear interpolation to create a function that can be passed on as the message. Lastly, we tested the algorithm against noise and learned that a near-perfect transmission is required to transmit a message that can be heard. Surprisingly, the message remains, but the audio file is corrupted by static noise.

References

[PC90] Louis M. Pecora and Thomas L. Carroll. "Synchronization in chaotic systems". In: *Phys. Rev. Lett.* 64 (8 Feb. 1990), pp. 821–824. DOI: 10.1103/PhysRevLett.64.821. URL: https://link.aps.org/doi/10.1103/PhysRevLett.64.821.

[HV92] Rong He and P. G. Vaidya. "Analysis and synthesis of synchronous periodic and chaotic systems". In: *Phys. Rev. A (3)* 46.12 (1992), pp. 7387–7392. ISSN: 1050-2947. DOI: 10.1103/PhysRevA.46.7387. URL: https://doi.org/10.1103/PhysRevA.46.7387.

[COS93a] K.M. Cuomo, A.V. Oppenheim, and S.H. Strogatz. "Robustness and Signal Recovery in a Synchronized Chaotic System". In: *International Journal of Bifurcation and Chaos* 03.06 (1993), pp. 1629–1638. DOI: 10.1142/S021812749300129X. URL: https://doi.org/10.1142/S021812749300129X.

[COS93b] K.M. Cuomo, A.V. Oppenheim, and S.H. Strogatz. "Synchronization of Lorenz-based chaotic circuits with applications to communications". In: *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing* 40.10 (1993), pp. 626–633. DOI: 10.1109/82.246163.

[CO93] Kevin M. Cuomo and Alan V. Oppenheim. "Circuit implementation of synchronized chaos with applications to communications". In: *Phys. Rev. Lett.* 71 (1 July 1993), pp. 65–68. DOI: 10.1103/PhysRevLett.71.65. URL: https://link.aps.org/doi/10.1103/PhysRevLett.71.65.

[Str19] S. Strogatz. *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering.* Chapman & Hall book. CRC Press, 2019. ISBN: 9780367092061.