EXPLORING THE LORENZ CHAOTIC SYSTEM TO ENCODE AND DECODE SECRET MESSAGES

ISCI 3A12 INDEPENDENT PROJECT

MICHAEL CHONG

Advised by Dr. Dmitry Pelinovsky*

CONTENTS

LIST OF FIGURES

ABSTRACT

The discovery of the Lorenz system in 1963 showed that solutions to systems of ordinary differential equations in three dimensions may have chaotic limit sets. This project explores the properties of the Lorenz system using analytical and numerical tools. We then discuss the application of chaos to private communications via synchronization of chaotic systems, and prepare a numerical simulation of a communications scheme in MATLAB. In particular, we investigate error in the imperfect recovery of the signal at the receiver system.

* *Department of Mathematics and Statistics, McMaster University, Hamilton, Canada*

1 INTRODUCTION TO CHAOS AND THE LORENZ SYSTEM

Systems of ordinary differential equations (ODEs) are equations involving functions and their derivatives, and are used to describe how systems evolve over time. The Lorenz system is a system of first-order ODEs in 3D-space, given by:

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = \rho x - y - xz \\ \dot{z} = xy - \beta z, \end{cases} \tag{1}$$

where $\sigma, \beta, \rho > 0$ are parameters. This system was discovered by Edward Lorenz in 1963 to describe convection in the atmosphere [4]. Systems with non-periodic behavior were of interest at the time to describe turbulent flow. However, the Lorenz system had unusual mathematical properties which we now describe as chaos, but were not well understood at the time. Since then, the Lorenz system has been a driving example in the study of chaos and its properties are now well-characterized.

We say a system is **chaotic** if it exhibits aperiodic behavior and sensitivity to initial conditions, meaning that there are trajectories of the system that:

1. do not settle to well-behaved limit sets (e.g. fixed points, periodic orbits, homoclinic orbits, and heteroclinic orbits), nor escape to infinity,
2. diverge exponentially fast from each other.

This definition aligns well with popular, non-mathematical notions of chaos. Lorenz himself presented the analogy of the 'butterfly effect': the idea that weather systems are so sensitive that turbulence caused by the flap of a butterfly's wings might cause a sequence of events resulting in a hurricane on the other side of the world.

For certain choices of parameters $\sigma, \beta, \rho > 0$, the Lorenz system exhibits chaotic behavior. In particular, Lorenz's original 1963 paper studied the system with $\sigma = 10$, $\beta = \frac{8}{3}$, and $\rho = 28$. Solutions of the system with these parameters trace out a butterfly wing-shaped phase portrait in 3D-space, seen in Figure 1 on the following page. A typical trajectory first enters one of two spirals, spiraling outward, and will unpredictably 'jump' to the other spiral. The trajectory will aperiodically oscillate back and forth between the two spirals for infinite time. If the trajectory starts at any arbitrarily close different initial condition, we observe similar spiraling behavior, but will jump at different times between the two spirals. This therefore satisfies both parts of the definition above, since:

1. solutions are repelled between the two unstable spirals for infinite time, and never settle onto the mentioned limit sets,
2. arbitrarily small perturbations in initial conditions result in the exponential divergence of solutions.

The remainder of this report comes in two parts. In Section 2, we discuss properties of the Lorenz system for the usual choice for parameters, and briefly explore behavior for different choices of parameters. Then, in Section 3, we discuss the surprising result of chaotic synchronization from Pecora and Caroll [5], and its application to private communications by Cuomo and Oppenheim [3].

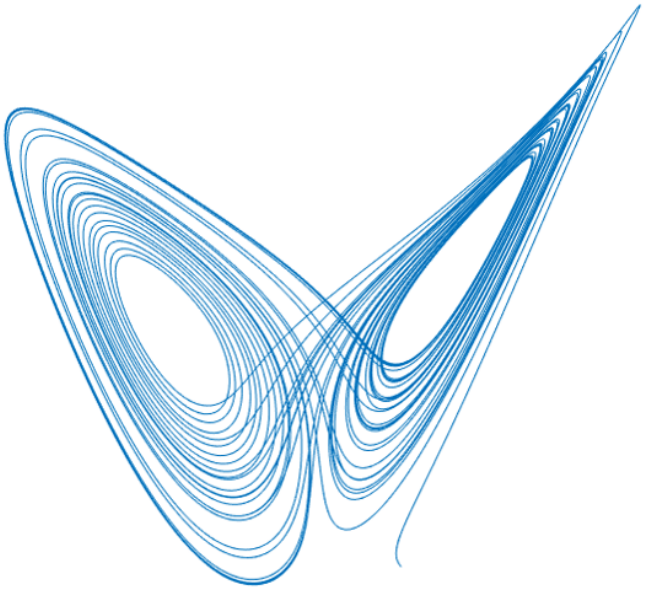


Figure 1: The famous butterfly-shaped phase portrait for the Lorenz system.

2 PROPERTIES OF THE LORENZ SYSTEM

In this section, we use analytical and numerical tools to formally characterize properties of the Lorenz system.

2.1 An Ellipsoidal Trapping Region

Using a Lyapunov function, we can show that all solutions of the system eventually enter and stay inside a bounded ellipsoidal region centered at the point $(x, y, z) = (0, 0, 2\rho)$. This region is given by

$$T = \{(x, y, z) \mid \rho x^2 + \sigma y^2 + \sigma(z - 2\rho)^2 \leqslant C\}$$

for some $C > 0$.

Proof. Let $E = \rho x^2 + \sigma y^2 + \sigma(z - 2\rho)^2$. Then taking the derivative with respect to t gives

$$\frac{dE}{dt} = 2\rho x\dot{x} + 2\sigma y\dot{y} + 2\sigma z\dot{z} - 4\sigma\rho\dot{z}$$

By substituting the Lorenz equations (1) for $\dot{x}, \dot{y}, \dot{z}$:

$$\frac{dE}{dt} = 2\rho\sigma x(y - x) + 2\sigma y(\rho x - y - xz) + 2\sigma z(xy - \beta z) - 4\sigma\rho(xy - \beta z)$$

$$\frac{dE}{dt} = -2\sigma(\rho x^2 + y^2 + \beta z^2 - 2\rho\beta z)$$

Since $\sigma > 0$, we have that $\frac{dE}{dt} < 0$ when $\rho x^2 + y^2 + \beta z^2 - 2\rho\beta z > 0$

$$\rho x^2 + y^2 + \beta z^2 - 2\rho\beta z > 0 \Leftrightarrow \rho x^2 + y^2 + \beta(z - \rho)^2 > \beta\rho^2$$

Therefore, when (x, y, z) is outside the ellipsoid $F = \{(x, y, z) \mid \rho x^2 + y^2 + \beta(z-\rho)^2 \geqslant \beta\rho^2\}$, we have $\frac{dE}{dt} \leqslant 0$. If we choose a value of C large enough such that the ellipsoid F is enclosed inside T, then T is a trapping region for the system. This is because any initial conditions outside T are also outside F. These trajectories are therefore attracted to smaller level surfaces of E, since $\frac{dE}{dt} < 0$, until they are inside F, where $\frac{dE}{dt}$ is sign-indefinite. These trajectories cannot escape outside F, and therefore do not escape T.

□

The smallest ellipsoid T for which this occurs (i.e. the minimum ellipsoidal trapping region) is achieved by obtaining the minimum value of C such that T encloses F. Here, we show that the minimum value of $C = \rho^2 \max\{4\sigma,\ \sigma(\beta+1),\ \sigma+\beta\}$.

Proof. T is centered at the point $(x, y, z) = (0, 0, 2\rho)$, and F is centered at $(x, y, z) = (0, 0, \rho)$.

First, let us analyze the z semi-axes.

For ellipsoid T:

$$x,\ y = 0 \Rightarrow z = 2\rho \pm \sqrt{C/\sigma}$$

For ellipsoid F:

$$x, y = 0 \Rightarrow z = \rho \pm \rho$$

In order for the z semi-axis of F to be contained in that of T, we require

$$2\rho - \sqrt{C/\sigma} \leqslant \rho - \rho = 0$$

$$2\rho \leqslant \sqrt{C\ \sigma}$$

$$C \geqslant 4\sigma\rho^2 \tag{2}$$

We then contain the y semi-axis in ellipsoid of F in the ellipsoid T. Since F is centered at $(0, 0, \rho)$, we find the the points at which its y semi-axis intersects T.

For ellipsoid F, the extrema of the y semi-axis are given by:

$$x = 0,\ z = \rho \Rightarrow y = \pm\sqrt{\beta}\rho$$

Substituting this value of y into the ellipsoid T:

$$x = 0,\ z = \rho,\ y = \pm\sqrt{\beta}\rho \Rightarrow \sigma\beta\rho^2 + \sigma\rho^2 \leqslant C$$

$$C \geqslant \sigma\rho^2(\beta+1) \tag{3}$$

Finally, we look at the x semi-axis of F.

The extrema are given by:

$$y = 0,\ z = \rho \Rightarrow x = \pm\sqrt{\beta\rho}$$

If we substitute these values of x in T:

$$\beta\rho^2 + \sigma\rho^2 \leqslant C$$

$$C \geqslant \rho^2(\sigma+\beta) \tag{4}$$

Therefore, in order to satisfy all three conditions (2) (3) (4), we choose $C = \rho^2 \max\{4\sigma,\ \sigma(\beta+1),\ \sigma+\beta\}$, and this is the minimum value of C for which F is contained in T. □

2.2 Exponential Divergence of Trajectories

The Lyapunov exponent of a system, denoted λ, is a measure of how quickly two nearby trajectories diverge. If $p(t)$ and $q(t)$ are two trajectories initially separated by a distance $\|\delta_0\|$, and the distance at time t, $|p(t) - q(t)|$ is given by $\|\delta(t)\|$, then the **Lyapunov exponent** is defined as λ in

$$\|\delta(t)\| \sim \|\delta_0\| e^{\lambda t} \tag{5}$$

For a system that exhibits exponential divergence of nearby trajectories, as in our previous definition of chaos, we expect $\lambda > 0$. According to past numerical experiments, λ for the Lorenz system has been found to be approximately 0.9 [7]. However, the exact value is dependent on the specific initial conditions chosen. The Lyapunov exponent is therefore usually reported as an average value of many samples of different initial conditions. Furthermore, in the Lorenz system, trajectories cannot diverge exponentially for infinite time. Since all trajectories remain in a bounded region, $\|\delta(t)\|$ must also be bounded. This result is seen in Figure 2 on the next page, where $\ln \|\delta(t)\|$ plateaus after a certain time. Therefore, for this system, we are only interested in the initial divergent behavior before saturation.

In our numerical experiment in MATLAB, we first choose two random initial conditions $p(0)$ and $q(0)$ separated by distance $\|\delta_0\|$. We then integrate solutions to the Lorenz equations (1) from these initial conditions with the usual choice of parameters $\sigma = 10, \beta = \frac{8}{3}, \rho = 28$. Since we are only interested in the initial behavior, we stop the integration at $t = 20$ which is usually before the point of saturation. To determine λ, we fit a line to the graph of $\ln \|\delta(t)\|$ and t. We take the slope of this line to be λ. Over 500 integrations we find the average Lyapunov exponent for the system $\lambda \approx 0.8993$.

Our estimate of the Lyapunov exponent therefore appears to be consistent with existing estimates. There are inevitable differences in estimates due to several reasons. For instance, as previously mentioned, there is variation in the Lyapunov exponent depending on initial conditions, and so a different estimate may be due to a different random sample of initial conditions. There may also be some small differences due to the numerical integration time steps at which $\|\delta(t)\|$ is calculated. In Figure 2 on the following page, we also observe that there are small fluctuations in $\ln \|\delta(t)\|$. Therefore, the arbitrary point at which we truncate the integration will change the fitted line and our consequent value of λ.

2.3 Unstable Periodic Orbits

In his original paper [4], Edward Lorenz presented evidence against the existence of stable limit cycles using what we call a Lorenz map. To generate a Lorenz map, we plot subsequent local maxima of the z-component of the Lorenz system. Consider the time series of $z(t)$ in the Lorenz system. Define $\{z_n\}$ to be the sequence of local maxima of $z(t)$. We then plot z_n against z_{n+1}, such that each point of the plot represents a pair of subsequent local maxima. The result of this plot from Lorenz [4] is shown in Figure 3a on page 8.

A remarkable result of this plot is that the points fall on a curve with almost no thickness. We can therefore crudely define a function $f(z_n) = z_{n+1}$. The key observation is that the magnitude of the slope of this graph,

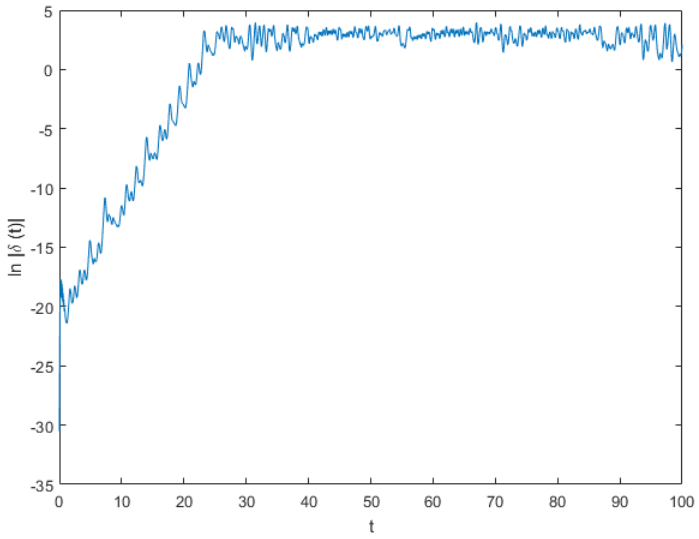


Figure 2: A plot of $\ln\|\delta(t)\|$ between two randomly selected initial conditions. The distance between any two trajectories initially increases at an exponential rate. After a finite time, $\|\delta(t)\|$ saturates as the remain in a bounded region.

$|f(z)| > 1$ for all z. This implies that any limit cycles that might exist are unstable.

To see why, consider an arbitrary closed orbit solution of the system. The sequence of maxima z_n of this solution will eventually repeat with some period p. In other words, there exists some $p \geqslant 1$ such that $z_{n+p} = z_n$. Then consider some small perturbation, ε_0 of some term of this sequence z_n. If we iterate using the Lorenz map and linearize about z_n, then the perturbation evolves to $\varepsilon_1 \approx f'(z_n)\varepsilon_0$. At the second iteration, we have $\varepsilon_2 \approx f'(z_{n+1})\varepsilon_1 \approx f'(z_{n+1})f'(z_n)\varepsilon_0$.

At the p^{th} iteration,

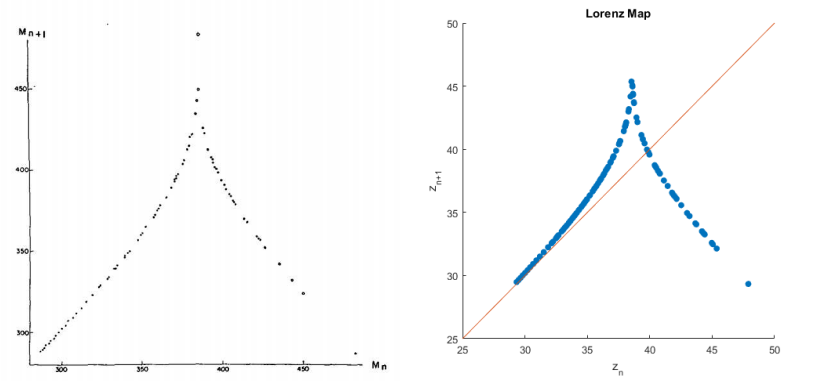
$$\varepsilon_p \approx \left(\prod_{k=1}^{p-1} f'(z_{n+k})\right)\varepsilon_0 \tag{6}$$

Since each $|f(z_i)| > 1$, it follows that that $|\varepsilon_p| > |\varepsilon_o|$, and so any closed orbit is necessarily unstable.

As Lorenz [4] notes, however, this argument is not a rigorous proof of the non-existence of stable limit cycles, since this argument only holds for the finite length of the numerical integration. However, the existence of the strange attractor was formally shown by Tucker in 1999 [8] through the use of rigorous numerics and the normal forms technique, which exceeds the scope of this project.

Here We verify Lorenz's findings using numerical integration in MATLAB. However, numerical integration methods return discrete set of coordinates $\{x(t_i), y(t_i), z(t_i)\}$ corresponding to time steps $\{t_1, ..., t_n\}$. A local maximum in the set of coordinates (i.e. a point $z(t_k)$ such that $z(t_{k-1}) < z(t_k)$ and $z(t_k) > z(t_{k+1})$) may not be a true maximum reached by the solution if the maximum is attained at some time $t' \epsilon (t_{k-1}, t_k) \cup (t_k, t_{k+1})$. To improve our estimate of the local maxima, we fit a degree-2 polynomial about the points $z(t_{k-1}), z(t_k)$, and $z(t_{k+1})$, where $z(t_k)$ is a local maximum in our set $\{z(t_i)\}$. We then take the maximum of the fitted polynomial to be a

local maximum of our solution to generate a term in our sequence $\{z_n\}$. The result of this method is shown in Figure 3b.



(a) Lorenz's original plot.

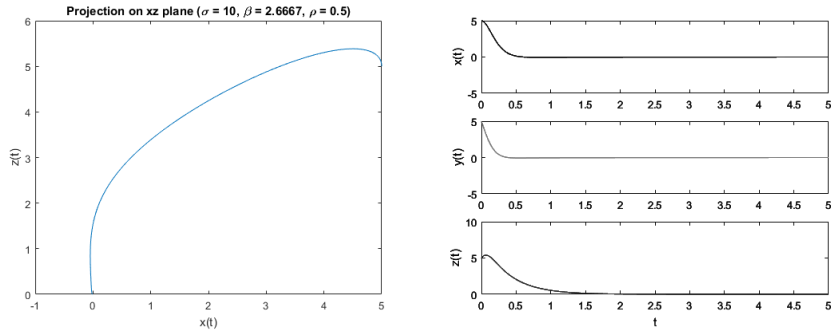
(b) Recreation of Lorenz map in MATLAB. The line $z_n = z_{n+1}$ is shown in red.

Figure 3: Lorenz maps.

2.4 Parameter Space

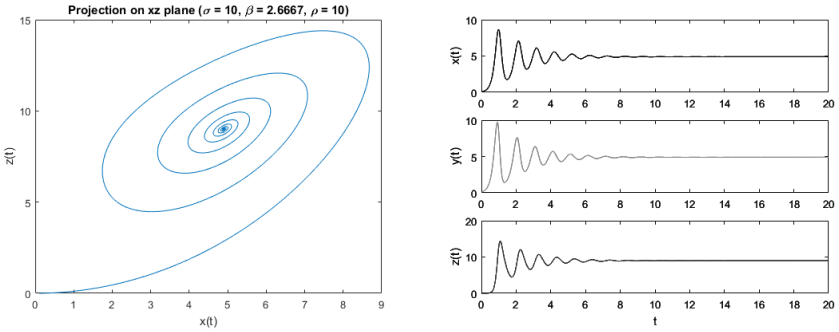
The Lorenz system takes three parameters, $\sigma, \beta, \rho > 0$, and exhibits different behavior for different choices of parameters. Typically, investigations in the parameter space of this system are done by fixing $\sigma = 10$ and $\beta = \frac{8}{3}$ and varying ρ. Different regimes are explained in the list below, and are illustrated in the numerical solutions that follow.

- For small values of ρ $(0 < \rho < 1)$, the origin is stable and attracts all initial conditions.
- At $\rho = 1$, we have a supercritical pitchfork bifurcation, and so for $1 < \rho < 24.74$, we have an unstable origin, and two stable fixed points.
- Interestingly, for $13.926 < \rho < 24.06$, we observe "transient chaos": before settling down to a fixed point, the solution initially traces out the strange attractor, jumping unpredictably between the two spirals, but eventually settles down to one of the two stable fixed points.
- For $24.06 < \rho < 24.74$, we have coexistence of the strange attractor and the stable fixed points. Therefore, depending on the initial conditions, the solution can either be chaotic or non-chaotic.
- At $\rho = 24.74$, we have a Hopf bifurcation. For $\rho > 24.74$, our fixed points become unstable and all initial conditions result in the chaotic behavior of Lorenz's strange attractor.
- For larger values of ρ, there are intervals in which there are stable periodic orbits. In particular, there are three large 'windows' of ρ in which this occurs: (99.524, 100.795), (145, 166), and (214.364, ∞). In fact, the behavior in these windows is quite complicated, and a comprehensive discussion can be found in [6].



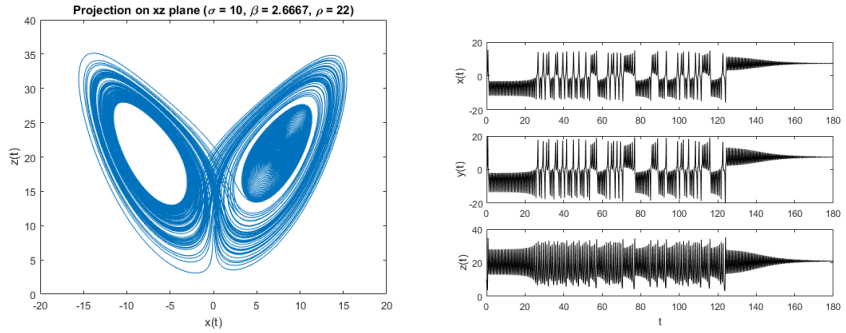
(a) Projection of solution onto the xz-plane. **(b)** Individual dynamics of x(t), y(t), and z(t).

Figure 4: The Lorenz system for $0 < \rho < 1$. The origin is globally stable and attracts all initial conditions.



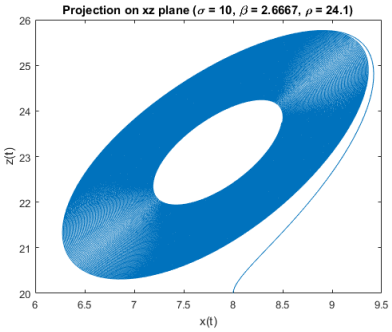
(a) Projection of solution onto the xz-plane. **(b)** Individual dynamics of x(t), y(t), and z(t).

Figure 5: The Lorenz system for $1 < \rho < 13.926$. Solutions are attracted to one of two stable fixed points.

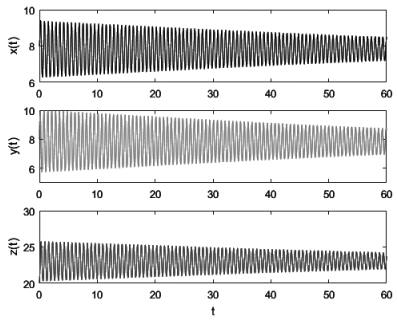


(a) Projection of solution onto the xz-plane. **(b)** Individual dynamics of x(t), y(t), and z(t).

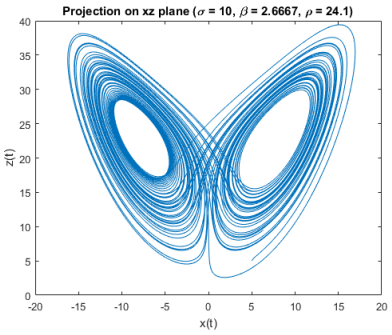
Figure 6: The Lorenz system for $13.926 < \rho < 24.06$. Solution may initially exhibit chaotic behavior, but eventually settles into a stable spiral.



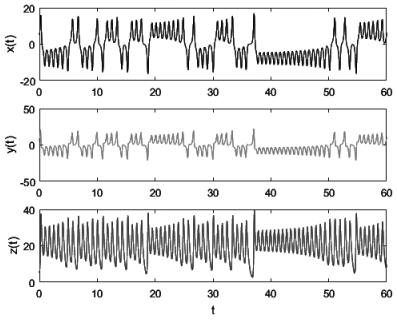
(a) Projection of a stable solution onto the xz-plane.



(b) Individual dynamics of x(t), y(t), and z(t).

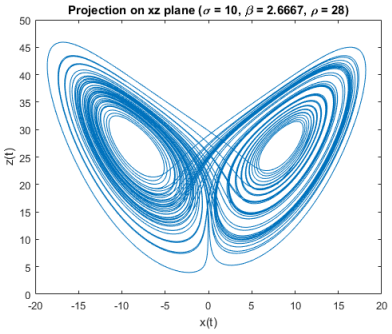


(c) Projection of a chaotic solution onto the xz-plane.

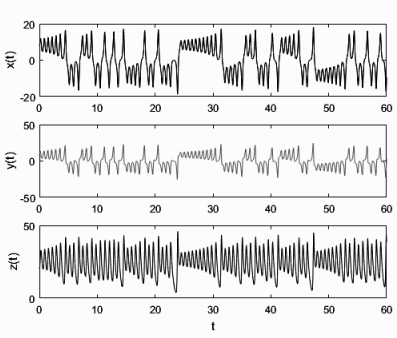


(d) Individual dynamics of x(t), y(t), and z(t).

Figure 7: Two solutions for the Lorenz system with $24.06 < \rho < 24.74$. The first solution settles onto a stable spiral, whereas the second solution exhibits is chaotic.

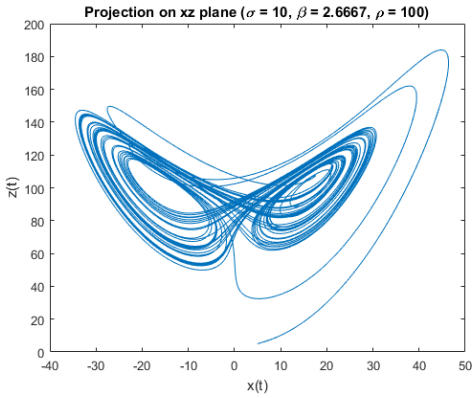


(a) Projection of solution onto the xz-plane.

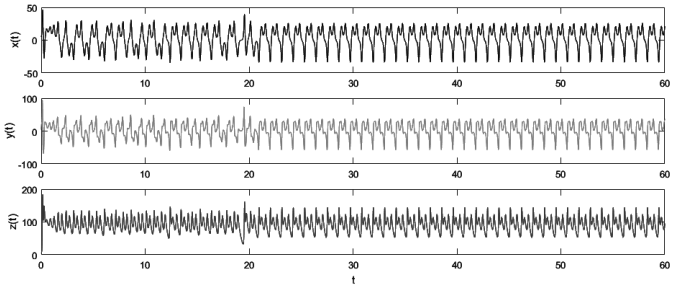


(b) Individual dynamics of x(t), y(t), and z(t).

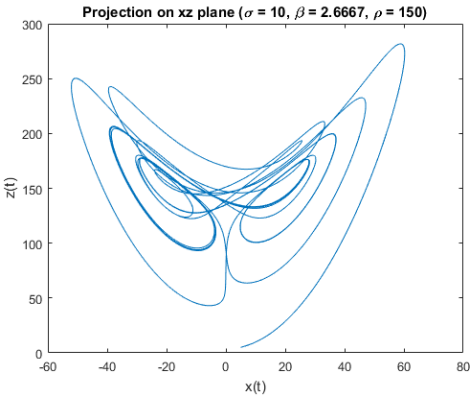
Figure 8: The Lorenz system for $24.74 < \rho < 99.524$. In particular, this is the system for $\rho = 28$, which was Lorenz's original choice of parameters. All solutions are chaotic.



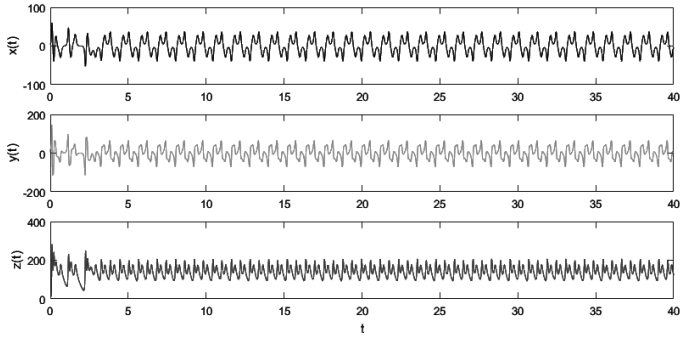
(a) Projection of solution with $\rho = 100$ onto the xz-plane.



(b) Individual dynamics of x(t), y(t), and z(t).



(c) Projection of a solution with $\rho = 150$ onto the xz-plane.



(d) Individual dynamics of x(t), y(t), and z(t).

Figure 9: The Lorenz system for large values of ρ. These are examples of solutions with stable periodic orbits.

3 APPLICATION TO COMMUNICATIONS

In this section, we use the Lorenz system as a driving example to discuss chaotic synchronization and explore its application to masking and demasking of signals.

3.1 Chaotic Synchronization

An unexpected result from Pecora and Caroll [5] was that chaotic systems that begin from two different initial conditions can be synchronized by using a continuous drive signal from one system to another. This is a counterintuitive result because as discussed in Section 1, chaotic systems are sensitive to initial conditions and one would expect that differences in initial conditions between the two systems would amplify over time.

In Pecora-Caroll synchronization, there is a sender system that generates a drive signal, and a receiver system that is dependent on the drive signal. The drive signal consists of partial dynamics of the sender system. In the case of the Lorenz system, the drive signal consists of the x-component dynamics of the sender system. A diagram of this is given in Figure 10. The full dynamics of the sender system, denoted $(x_s(t), y_s(t), z_s(t)$ behave according to the usual Lorenz equations:

$$\begin{cases} \dot{x}_s = \sigma(y_s - x_s) \\ \dot{y}_s = \rho x_s - y_s - x_s z_s \\ \dot{z}_s = x_s y_s - \beta z_s, \end{cases} \tag{7}$$

The receiver system dynamics, denoted $(x_r(t), y_r(t), z_r(t))$ are given by:

$$\begin{cases} \dot{x}_r = \sigma(y_r - x_r) \\ \dot{y}_r = \rho x_s - y_r - x_s z_r \\ \dot{z}_r = x_s y_r - \beta z_r, \end{cases} \tag{8}$$

In this setup, the y and z dynamics of the receiver system (y_r and z_r respectively), are partially driven by the x component of the sender system. The synchronization error between the two chaotic systems has been shown in [5] exponentially decay to 0 as $t \to \infty$ for any choice of initial conditions.

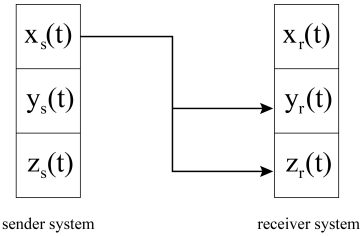


Figure 10: A schematic diagram of Pecora-Caroll synchronization for the Lorenz system. In order to synchronize the two systems, the y and z components of the receiver system (right) are dependent on the x component of the sender system (left).

3.2 Application to Private Communications

Using this principle of chaotic synchronization, Cuomo and Oppenheim [1] presented a private communications scheme that involved masking and demasking signals using chaotic noise.

Similarly to Pecora and Caroll's setup, there is a sender system and receiver system connected by a continuous drive signal. However, the drive signal from the sender system is slightly modified by adding a message component. Then, using this drive signal, the receiver synchronizes to the dynamics of the sender system. The receiver then subtracts the chaotic dynamics to recover the message component. A diagram of this is given in Figure 11. In this setup, the sender system is unchanged, and behaves according to Eq. (4). However, the receiver system behaves according to:

$$\begin{cases} \dot{x}_r = \sigma(y_r - x_r) \\ \dot{y}_r = \rho d(t) - y_r - d(t) z_r \\ \dot{z}_r = d(t) y_r - \beta z_r, \end{cases} \tag{9}$$

where $d(t) = x_s(t) + m(t)$, and $m(t)$ is a message component. The signal is recovered at the receiver system as $\hat{m}(t) = d(t) - x_r(t)$.

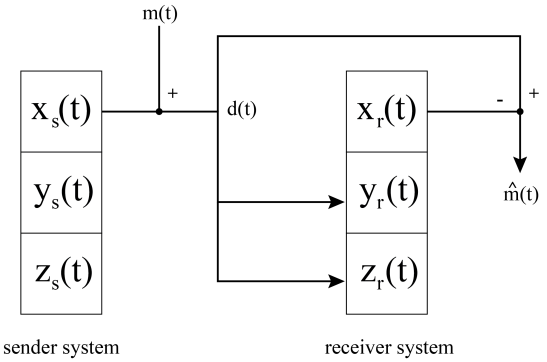


Figure 11: A schematic diagram of Cuomo and Oppenheim's communication scheme. A message component, $m(t)$, is added to $x_s(t)$ to generate $d(t)$, which partially drives the receiver dynamics. The message is then recovered by subtracting $x_r(t)$ from $d(t)$. Adapted from Cuomo and Oppenheim [1]

Cuomo and Oppenheim's original experiment implemented this scheme using two electronic circuits with scaled variables more appropriate for the electronic hardware. For our purposes, we are more interested in the mathematical scheme, rather than the electronic details.

There are a couple remarks to make about this signal masking approach. First, the masking-demasking process is imperfect. As an example, Figure 12 on the next page shows that the recovered signal $\hat{m}(t)$ is not an exact recovery of the original message $m(t)$. However, anecdotally, when $m(t)$ is some speech waveform, the message is discernible in $\hat{m}(t)$ with some additional noise. Second, the magnitude of the signal, $m(t)$, must be much lower than that of the dynamics of the Lorenz system $x(t)$ for an effective recovery. While this is analytically difficult to show, this is intuitively obvious since the $m(t)$ is effectively a perturbation to the chaotic synchronizing signal. A greater perturbation therefore results in larger error in synchronization between the sender and receiver system (in particular between $x_s(t)$ and $x_r(t)$), and a subsequent larger error in the recovered signal

$\hat{m}(t) = d(t) - x_r(t) = x_r(t) + m(t) - x_s(t)$. A question that follows is the effect of amplitude of the signal (relative to the Lorenz system amplitude) on the error of the signal masking-demasking process. We discuss this problem in Section 3.3.

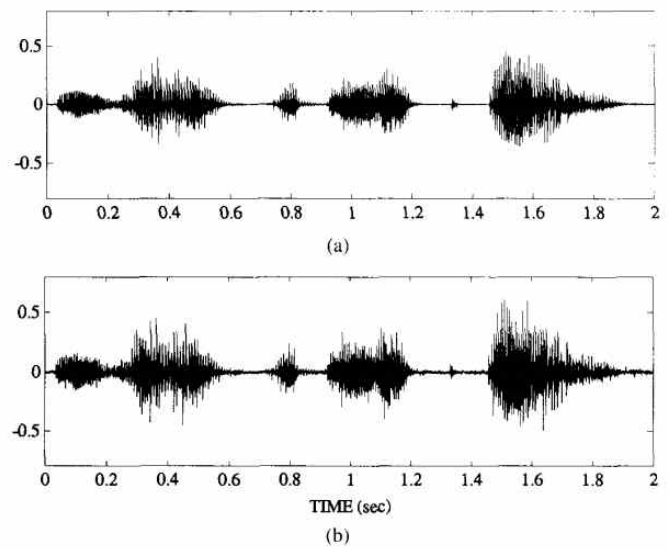


Figure 12: Speech waveform masking and recovery results from Cuomo and Oppenheim [1]. The waveform in (a) shows the original speech waveform, while (b) shows the recovered waveform.

NUMERICAL SIMULATION OF MASKING PROCESS An inherent advantage to using electronic circuits is that the signals are continuous, whereas numerically, we consider the signal and the systems in discrete time steps. For a general signal, we therefore have two main problems to consider:

1. Digital signals (in particular, audio files) are usually given as an array, with each value corresponding to the amplitude of the signal at some time step. Time steps are usually uniformly spaced according to some sample rate. Audio files may also have multiple tracks (e.g. stereo audio files have two tracks), and so to fit with the scheme, we take only mono track audio.

2. Adaptive numerical integrators in MATLAB in general do not use uniformly sized time steps.

Here we outline two approaches to numerically simulate this communications scheme in MATLAB.

Suppose the audio message $m(t)$ comes to us as an array $\{m(t_i) \mid i = 1, ..., n\}$. In our first approach, we first generate the full dynamics of the sender system at uniformly spaced time steps $\{t_1, ..., t_n\}$ determined by the audio file sample rate. This returns an array $\{x_s(t_i), y_s(t_i), z_s(t_i) | i = 1, ..., n\}$. An array for the drive signal, $d(t)$, is easily obtained by $\{d(t_i) = x_s(t_i) + m(t_i) \mid i = 1, ...n\}$. Then, we generate the corresponding receiver system array $\{x_r(t_i), y_r(t_i), z_r(t_i)\}$. Since the adaptive integration in MATLAB might require some $d(t')$, where $t_i < t' < t_{i+1}$ for some i, we use a spline interpolation about t' to estimate $d(t')$. After obtaining the receiver array, the message array is then recovered as $\hat{m}(t_i) = d(t_i) - x_r(t_i)$.

Since this method approximates $d(t)$, it is also making an approximation of $x_s(t)$. This method is sufficient to distinguish speech and music waveforms, but too imprecise to be useful for our investigation. For instance, when $m(t) = 0$ constant, and the two systems begin with identical initial conditions, we expect perfect synchronization, but this method returns non-zero error between the sender and receiver system.

In our second, more streamlined approach, we numerically integrate the sender and receiver systems simultaneously as a six-dimensional system, and return values $\{x_s(t_i), y_s(t_i), z_s(t_i), x_r(t_i), y_r(t_i), z_r(t_i) \mid i = 1, .., n\}$. Since this may also ask for some $m(t')$ with $t_i < t' < t_{i+1}$ in order to generate $d(t')$, we only interpolate to approximate $m(t')$. The message array is then recovered as $\hat{m}(t_i) = x_s(t_i) + m(t_i) - x_r(t_i)$. Results from this method is shown in Figure 13. This method does return a zero error when $m(t) = 0$ and $(x_s(0), y_s(0), z_s(0)) = (x_r(0), y_r(0), z_r(0))$.

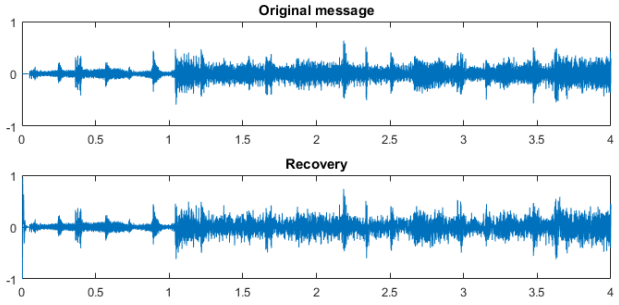


Figure 13: Results from the numerical masking/demasking process, showing the original music waveform (top) and recovered waveform (bottom).

3.3 Discussion of Error

The imperfect recovery of the original message naturally leads us to questions on how this error changes with different signals. Cuomo, Oppenheim, and Strogatz [2] discuss the robustness of this scheme using random Gaussian white noise as their message/perturbation component, which allows them to make some heuristic arguments leading to an approximate analytic model of the error.

We take a different approach in our investigation of the error. We use a regular sinusoidal function as our signal, and change the frequency and amplitude parameters of the function to observe effects on the error.

Here we investigate the sender system and receiver system as usual, given by Eq. (4) and (6), taking $m(t)$ to be $A \sin(\omega t)$, where A is our amplitude parameter and ω is our frequency parameter. We report the error, denoted in the recovery, denoted E, as the L^∞ norm of the vector:

$$\mathbf{e}(t) = (\hat{m}(t_1), ..., \hat{m}(t_n)) - (m(t_1), ..., m(t_n))$$

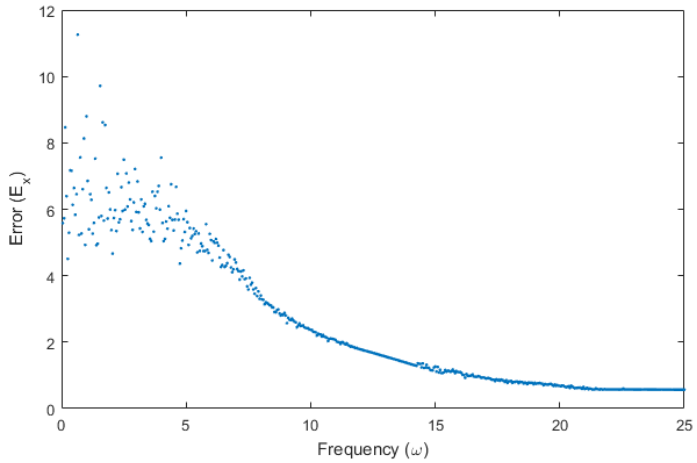
where $\hat{m}(t_i)$ is the value of the recovered signal at the i^{th} time step, and $m(t_i) = A \sin(\omega t_i)$. We use the usual choice of parameters for the Lorenz system, and integrate to $t = 100$. In our investigation of frequency, we fix the amplitude of our signal at $A = 1$, and in our investigation of amplitude, we fix the frequency of the signal at $\omega = 10$.

In general, we find that the error decreases with a higher frequency signal, and increases with larger amplitude signal, which seems to be consistent

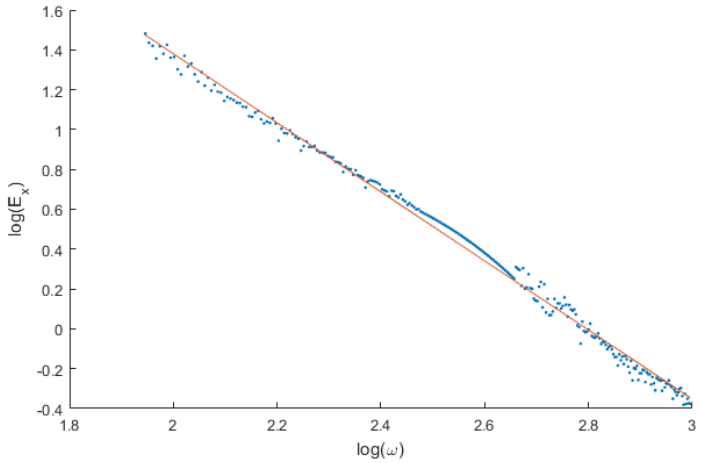
with findings from Cuomo et al. [2]. To further formalize our results, we perform a least-squares power fit on the data.

For frequency, we discard values where the data is noisy ($0 < \omega < 7$), and where the frequency of the signal is too high for our level of precision ($\omega > 20$). The result is shown in Figure 14.

For amplitude, we fit only to values where $0 < A < 2$, since this is approximately one-tenth of the magnitude of the Lorenz system dynamics, which is approximately on the order of 2×10^1. The result is shown in Figure 15 on the following page.

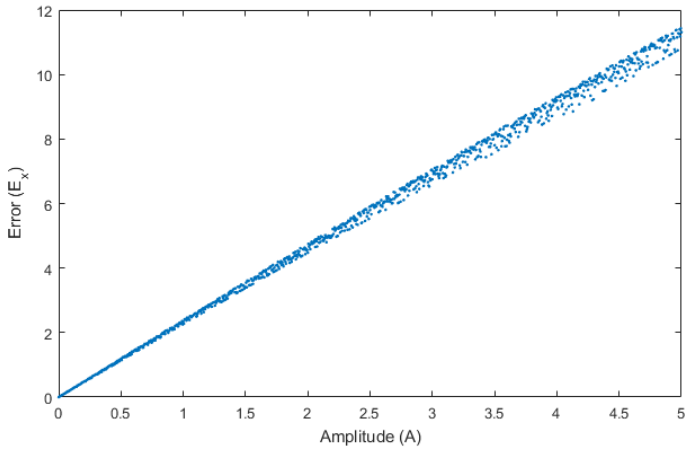


(a) Recovery error as a function of signal frequency.

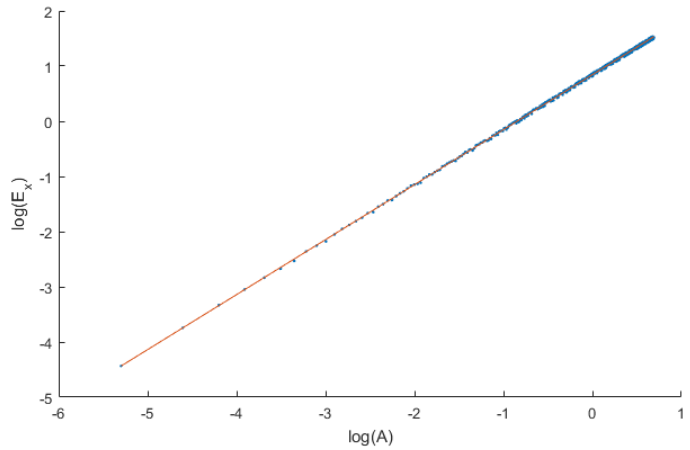


(b) Log-log plot of frequency and recovery error, with sample points shown in blue. A fitted line given by $\log E_x = -1.7332\omega + 4.8470$ is shown in red.

Figure 14: Error in signal recovery (i.e. synchronization error in the x-component) with $A = 1$ and varying ω. The corresponding least squares power fit is shown in (b).



(a) Recovery error as a function of signal amplitude.



(b) Log-log plot of amplitude and recovery error, with sample points shown in blue. A fitted line given by $\log E_x = 0.9964A + 0.8450$ is shown in red.

Figure 15: Error in signal recovery (i.e. synchronization error in the x-component) with $\omega = 1$ and varying A. The corresponding least squares power fit is shown in (b).

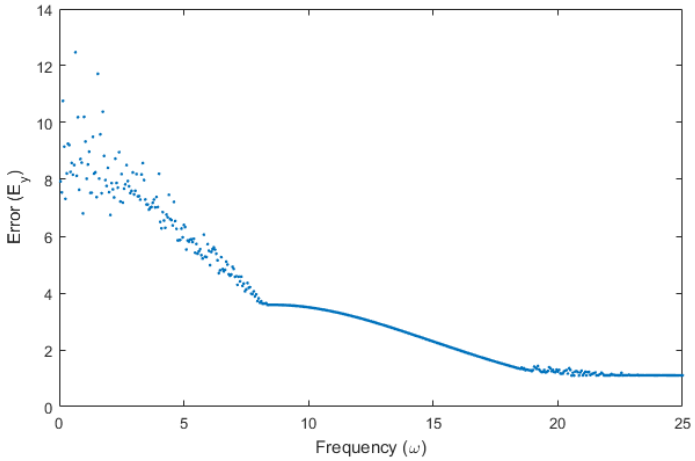
From these results, we obtain the following relationships:

$$\hat{E}_x = 129.1\,\omega^{-1.7332} \tag{10}$$

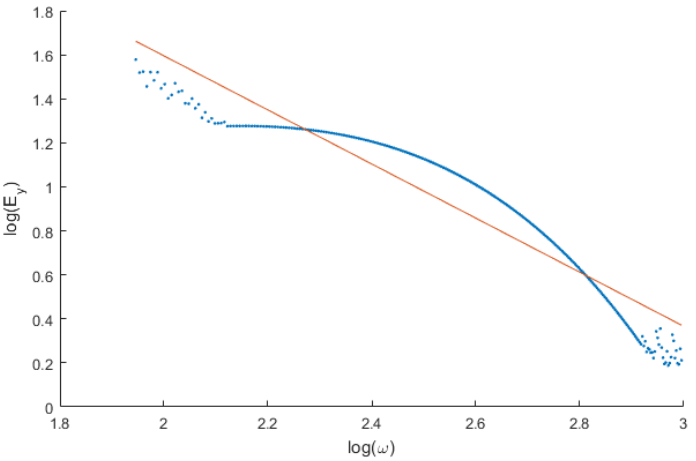
$$\hat{E}_x = 2.328\,A^{0.9964} \tag{11}$$

where $\hat{E}_x$ is our prediction of the recovery error, ω is the frequency of the signal, and A is the amplitude of the signal. The finding in (10) suggests $\hat{E}_x \sim \omega^{-2}$, which agrees with computations obtained from Laplace transforms in [2]. The law (11) suggests $\hat{E}_x \sim A$.

We also investigate the synchronization error in the y-component (Figure 16 on the next page and 17 on page 19) and z-component (Figure 18 on page 20 and 19 on page 21) below.

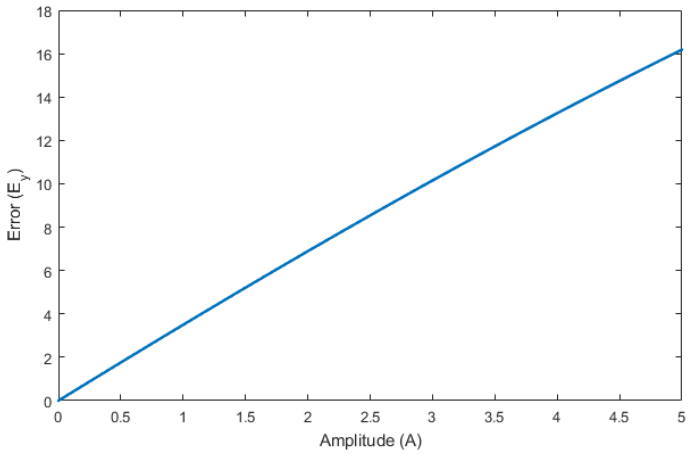


(a) Synchronization error in y as a function of signal frequency.

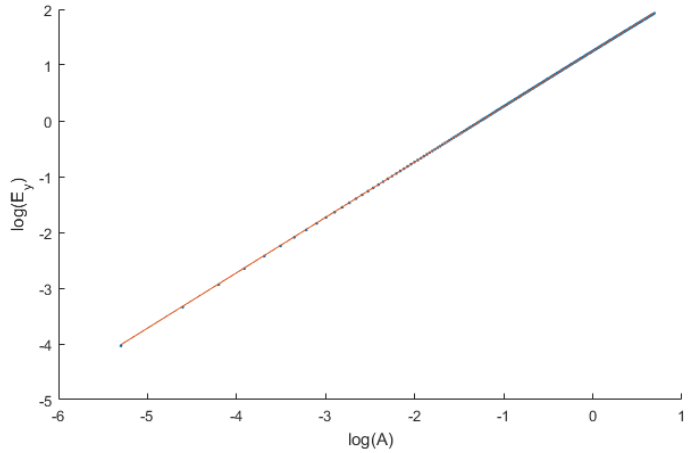


(b) Log-log plot of frequency and recovery error, with sample points shown in blue. A fitted line given by $\log E_y = -1.2292\omega + 4.0536$ is shown in red.

Figure 16: Synchronization error in the y-component with $A = 1$ and varying ω. The corresponding least squares power fit is shown in (b).

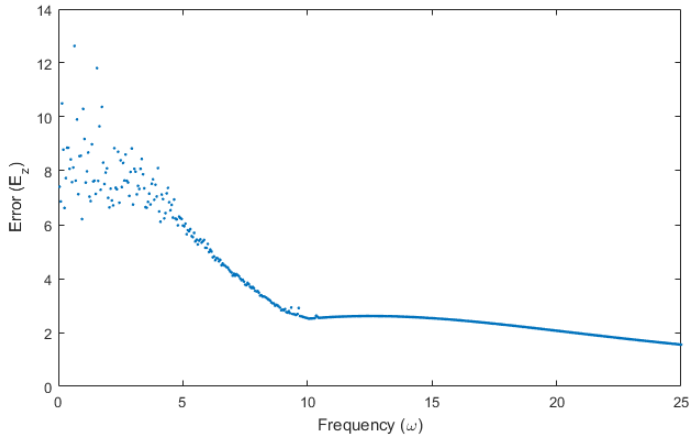


(a) Synchronization error in y as a function of signal amplitude.

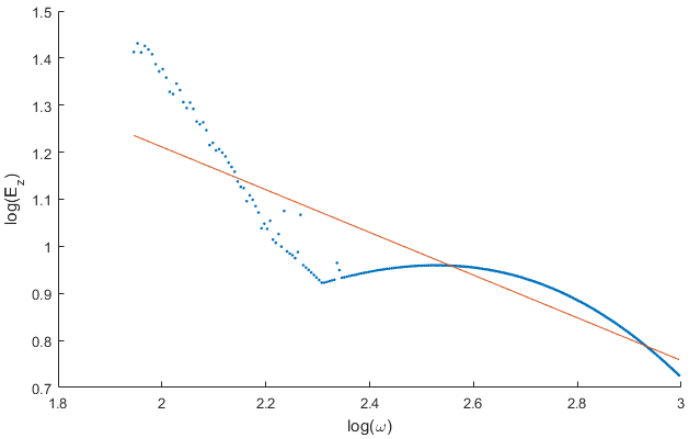


(b) Log-log plot of amplitude and synchronization error, with sample points shown in blue. A fitted line given by $\log E_y = 0.9934A + 1.2494$ is shown in red.

Figure 17: Synchronization error in the y-component with $\omega = 10$ and varying A. The corresponding least squares power fit is shown in (b).

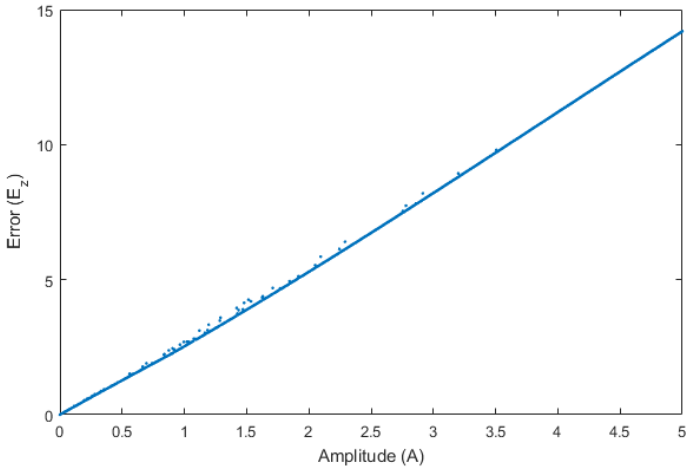


(a) Synchronization error in z as a function of signal frequency.

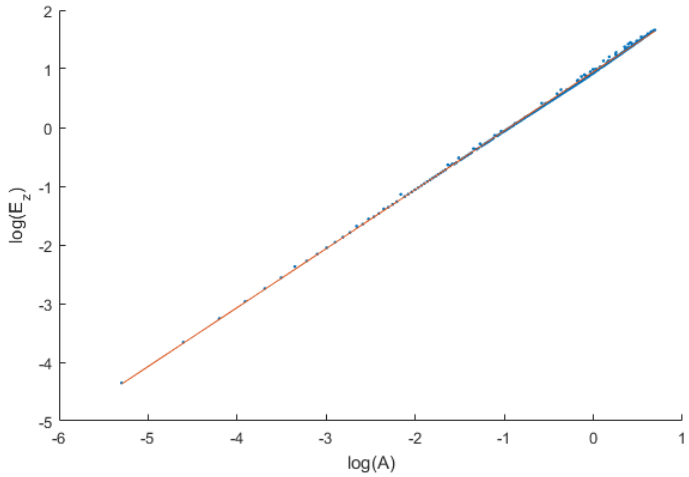


(b) Log-log plot of frequency and recovery error, with sample points shown in blue. A fitted line given by $\log E_z = -0.4538\omega + 2.1186$ is shown in red.

Figure 18: Synchronization error in the z-component with $A = 1$ and varying ω. The corresponding least squares power fit is shown in (b).



(a) Synchronization error in z as a function of signal amplitude.



(b) Log-log plot of amplitude and synchronization error, with sample points shown in blue. A fitted line given by $\log E_z = 1.0044A + 0.9495$ is shown in red.

Figure 19: Synchronization error in the z-component with $\omega = 10$ and varying A. The corresponding least squares power fit is shown in (b).

The linear relationship with signal amplitude and synchronization in the y- and z-components are consistent with the relationship in the x-component, and in agreement with results in [2]. However, the results regarding signal frequency and synchronization error are somewhat unexpected. Figure 16 on page 18 and Figure 18 on the preceding page show that E_y and E_z respectively do not decrease smoothly with ω. In particular, at approximately $\omega = 7.5$, there is a point where the curve of $E_y(\omega)$ is not smooth, and at approximately $\omega = 10$, the curve of $E_z(\omega)$ is not smooth. Furthermore, it is evident in both the log plots that there is an interval where synchronization error increases with ω. This is not consistent with the model in [2].

4 CONCLUSION AND FUTURE DIRECTIONS

There have been several developments in the literature since the introduction of Pecora-Caroll synchronization and Cuomo and Oppenheim's communication scheme. One particularly interesting area of study is observer-based synchronization, where the receiver system need not know the parameters of the transmitting system in order to synchronize dynamics. There have also been explorations into increasing the security of this communication scheme by using 'hyperchaotic' systems, which are systems that have more than one positive Lyapunov exponent. These systems exist in spaces of four dimensions or higher, and have more complex dynamics leading to greater security.

SUMMARY In this report, we discussed properties of the Lorenz system. In particular, we presented arguments for boundedness of solutions, exponential divergence of trajectories, instability of any periodic orbits, and outline different behavior regimes in the ρ parameter space of the system. We then used the Lorenz system to illustrate Pecora-Caroll synchronization between two chaotic system, and explore Cuomo and Oppenheim's approach to signal masking using chaotic synchronization. Using numerical experiments, we investigate the relationship between the error in the signal recovery and the signal frequency, and the signal amplitude. We find $\hat{E}_x \sim \omega^{-2}$ and $\hat{E}_x \sim A$ respectively, which is consistent with previous results from Cuomo et al. [2]. However, the apparent relationship between signal frequency and synchronization error in the y- and z-components does not agree with [2]. Since our method of investigation was different than that of [2], who used Gaussian white noise as a perturbing signal (as opposed to a sinusoidal function), exploring other signals may be a point of future investigation on this topic.

REFERENCES

[1] Kevin M. Cuomo and Alan V. Oppenheim, *Circuit implementation of synchronized chaos with applications to communications*, Physical Review Letters **71** (1993), no. 1, 65–68.

[2] Kevin M Cuomo, Alan V Oppenheim, and Steven H. Strogatz, *Robustness and signal recovery in a synchronized chaotic system*, International Journal of Bifurcation and Chaos **3** (1993), no. 6, 1629–1638.

[3] Kevin M. Cuomo, Alan V. Oppenheim, and Steven H. Strogatz, *Synchronization of Lorenz-based chaotic circuits with applications to communications*, IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing **40** (1993), no. 10, 626–633.

[4] Edward N. Lorenz, *Deterministic Nonperiodic Flow*, Journal of the Atmospheric Sciences **20** (1963), no. 2, 130–141.

[5] Louis M. Pecora and Thomas L. Carroll, *Synchronization in chaotic systems*, Physical Review Letters **64** (1990), no. 8, 821–824.

[6] Colin Sparrow, *The Lorenz Equations: Bifurcations, Chaos, and Strange Attractors*, Applied Mathematical Sciences, vol. 41, Springer New York, New York, NY, 1982.

[7] Steven Strogatz, *Nonlinear Dynamics and Chaos*, 2 ed., Westview Press, 1994.

[8] Warwick Tucker, *The Lorenz attractor exists*, Comptes Rendus de l'Académie des Sciences - Series I - Mathematics **328** (1999), no. 12, 1197–1202.