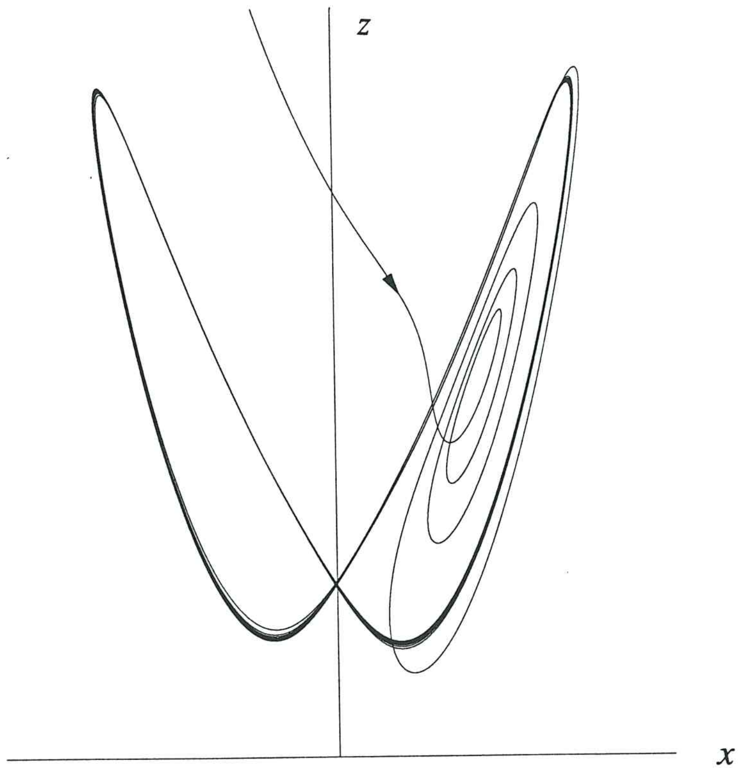


Figure 9.5.4

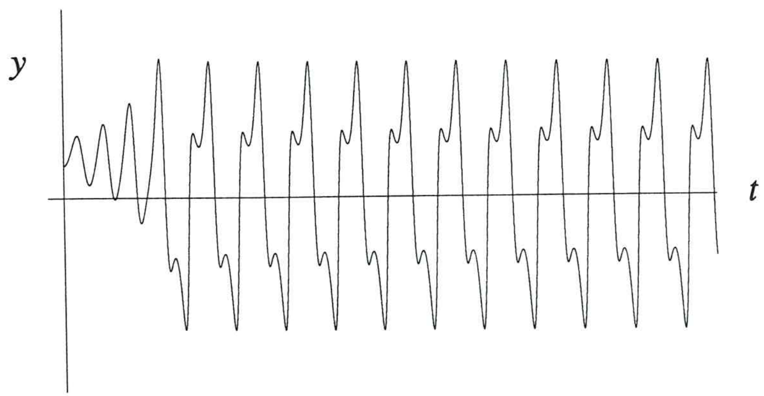


Figure 9.5.5

This solution predicts that the waterwheel should ultimately rock back and forth like a pendulum, turning once to the right, then back to the left, and so on. This is observed experimentally. ■

In the limit $r \to \infty$ one can obtain many analytical results about the Lorenz equations. For instance, Robbins (1979) used perturbation methods to characterize the limit cycle at large r. For the first steps in her calculation, see Exercise 9.5.5. For more details, see Chapter 7 in Sparrow (1982).

The story is much more complicated for r between 28 and 313. For most values of r one finds chaos, but there are also small windows of periodic behavior interspersed. The three largest windows are $99.524\ldots < r < 100.795\ldots$; $145 < r < 166$; and $r > 214.4$. The alternating pattern of chaotic and periodic regimes resembles that seen in the logistic map (Chapter 10), and so we will defer further discussion until then.

9.6 Using Chaos to Send Secret Messages

One of the most exciting recent developments in nonlinear dynamics is the realization that chaos can be *useful*. Normally one thinks of chaos as a fascinating curiosity at best, and a nuisance at worst, something to be avoided or engineered away. But since about 1990, people have found ways to exploit chaos to do some marvelous and practical things. For an introduction to this new subject, see Vohra et al. (1992).

One application involves "private communications." Suppose you want to send a secret message to a friend or business partner. Naturally you should use a code, so that even if an enemy is eavesdropping, he will have trouble making sense of the message. This is an old problem—people have been making (and breaking) codes for as long as there have been secrets worth keeping.

Kevin Cuomo and Alan Oppenheim (1992, 1993) have implemented a new approach to this problem, building on Pecora and Carroll's (1990) discovery of ***synchronized chaos***. Here's the strategy: When you transmit the message to your friend, you also "mask" it with much louder chaos. An outside listener only hears the chaos, which sounds like meaningless noise. But now suppose that your friend has a magic receiver that perfectly reproduces the chaos—then he can subtract off the chaotic mask and listen to the message!

Cuomo's Demonstration

Kevin Cuomo was a student in my course on nonlinear dynamics, and at the end of the semester he treated our class to a live demonstration of his approach. First he showed us how to make the chaotic mask, using an electronic implementation of the Lorenz equations (Figure 9.6.1). The circuit involves resistors, capacitors, operational amplifiers, and analog multiplier chips.

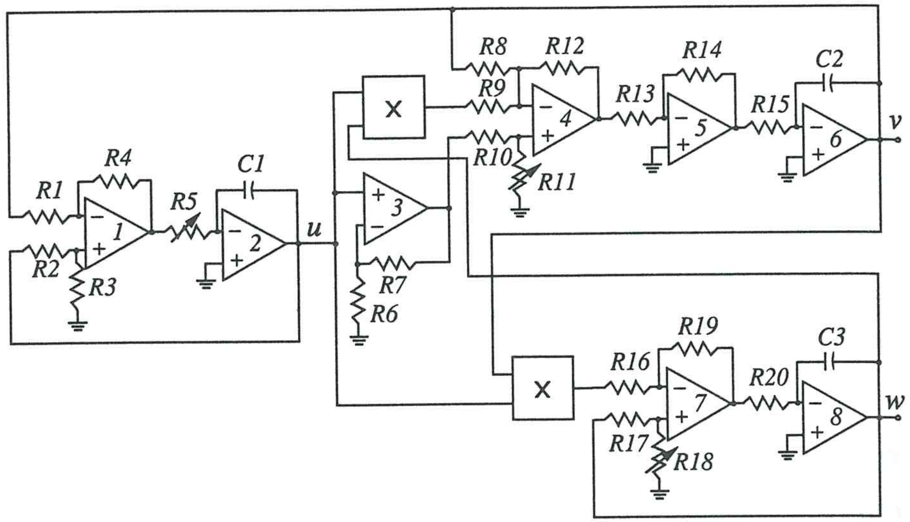
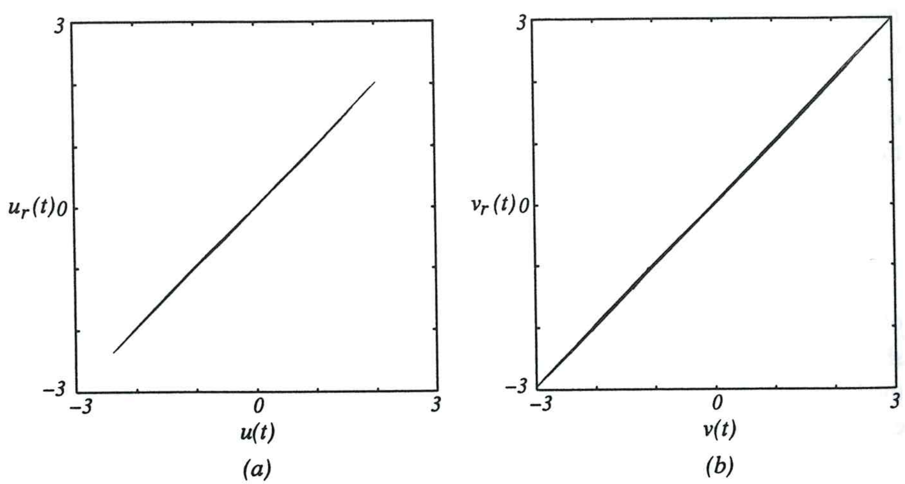


Figure 9.6.1 Cuomo and Oppenheim (1993), p. 66

The voltages u, v, w at three different points in the circuit are proportional to Lorenz's x, y, z. Thus the circuit acts like an analog computer for the Lorenz equations. Oscilloscope traces of $u(t)$ vs. $w(t)$, for example, confirmed that the circuit was following the familiar Lorenz attractor. Then, by hooking up the circuit to a loudspeaker, Cuomo enabled us to *hear* the chaos—it sounds like static on the radio.

The hard part is to make a receiver that can synchronize perfectly to the chaotic transmitter. In Cuomo's set-up, the receiver is an identical Lorenz circuit, driven in a certain clever way by the transmitter. We'll get into the details later, but for now let's content ourselves with the experimental fact that synchronized chaos does occur. Figure 9.6.2 plots the receiver variables $u_r(t)$ and $v_r(t)$ against their transmitter counterparts $u(t)$ and $v(t)$.



The 45° trace on the oscilloscope indicates that the synchronization is nearly perfect, despite the fact that both circuits are running chaotically. The synchronization is also quite stable: the data in Figure 9.6.2 reflect a time span of several minutes, whereas without the drive the circuits would decorrelate in about 1 millisecond.

Cuomo brought the house down when he showed us how to use the circuits to mask a message, which he chose to be a recording of the hit song "Emotions" by Mariah Carey. (One student, apparently with different taste in music, asked "Is that the signal or the noise?") After playing the original version of the song, Cuomo played the masked version. Listening to the hiss, one had absolutely no sense that there was a song buried underneath. Yet when this masked message was sent to the receiver, its output synchronized almost perfectly to the original chaos, and after instant electronic subtraction, we heard Mariah Carey again! The song sounded fuzzy, but easily understandable.

Figures 9.6.3 and 9.6.4 illustrate the system's performance more quantitatively. Figure 9.6.3a is a segment of speech from the sentence "He has the bluest eyes," obtained by sampling the speech waveform at a 48 kHz rate and with 16-bit resolution. This signal was then masked by much louder chaos. The power spectra in Figure 9.6.4 show that the chaos is about 20 decibels louder than the message, with coverage over its whole frequency range. Finally, the unmasked message at the receiver is shown in Figure 9.6.3b. The original speech is recovered with only a tiny amount of distortion (most visible as the increased noise on the flat parts of the record).

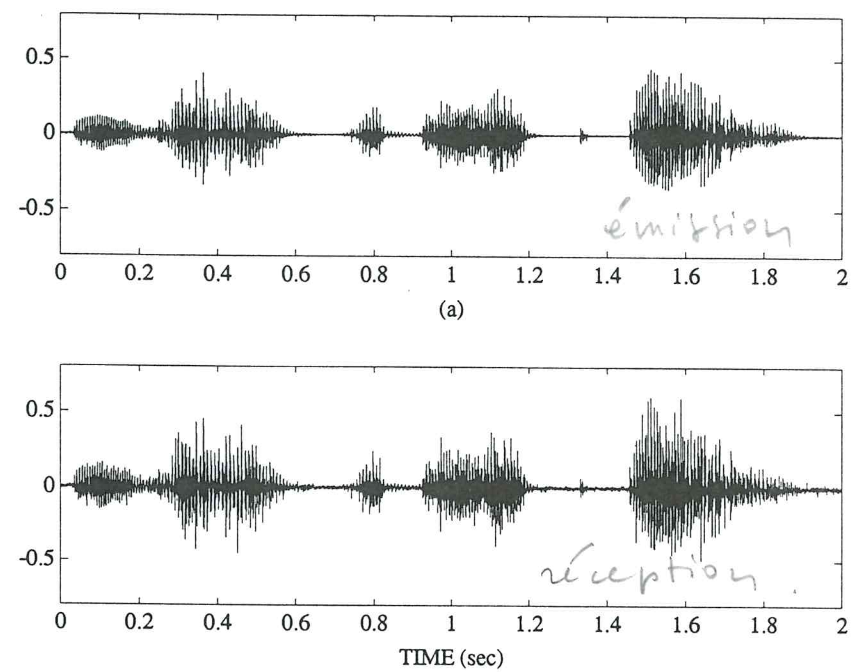


Figure 9.6.3 Cuomo and Oppenheim (1993), p. 67

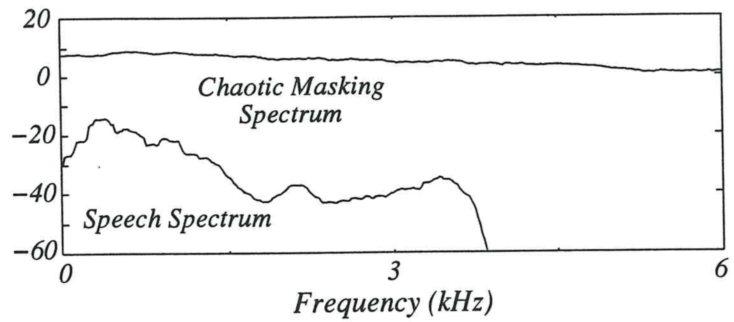


Figure 9.6.4 Cuomo and Oppenheim (1993), p. 68

Proof of Synchronization

The signal-masking method discussed above was made possible by the conceptual breakthrough of Pecora and Carroll (1990). Before their work, many people would have doubted that two chaotic systems could be made to synchronize. After all, chaotic systems are sensitive to slight changes in initial condition, so one might expect any errors between the transmitter and receiver to grow exponentially. But Pecora and Carroll (1990) found a way around these concerns. Cuomo and Oppenheim (1992, 1993) have simplified and clarified the argument; we discuss their approach now.

The receiver circuit is shown in Figure 9.6.5.

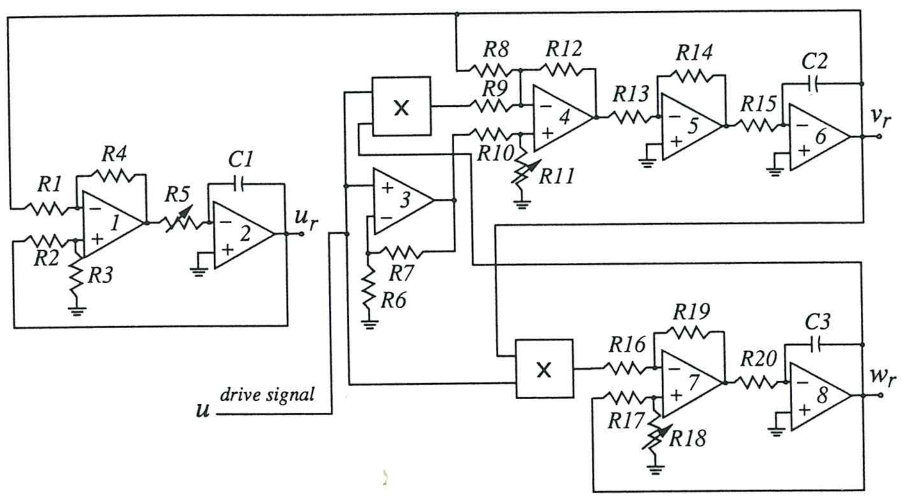


Figure 9.6.5 Courtesy of Kevin Cuomo

It is identical to the transmitter, except that the drive signal $u(t)$ replaces the receiver signal $u_r(t)$ at a crucial place in the circuit (compare Figure 9.6.1). To see what effect this has on the dynamics, we write down the governing equations for both the transmitter and the receiver. Using Kirchhoff's laws and appropriate nondimensionalizations (Cuomo and Oppenheim 1992), we get

$$\begin{aligned} \dot{u} &= \sigma(v-u) \\ \dot{v} &= ru - v - 20uw \\ \dot{w} &= 5uv - bw \end{aligned} \qquad (1)$$

as the dynamics of the transmitter. These are just the Lorenz equations, written in terms of scaled variables

$$u = \tfrac{1}{10}x, \qquad v = \tfrac{1}{10}y, \qquad w = \tfrac{1}{20}z.$$

(This scaling is irrelevant mathematically, but it keeps the variables in a more favorable range for electronic implementation, if one unit is supposed to correspond to one volt. Otherwise the wide dynamic range of the solutions exceeds typical power supply limits.)

The receiver variables evolve according to

d'après Cuomo + Oppenheim 1993

σ = 16 r = 45,6
b = 4

$$\begin{aligned} \dot{u}_r &= \sigma(v_r - u_r) \\ \dot{v}_r &= ru(t) - v_r - 20u(t)w_r \\ \dot{w}_r &= 5u(t)v_r - bw_r \end{aligned} \qquad (2)$$

where we have written $u(t)$ to emphasize that the receiver is driven by the chaotic signal $u(t)$ coming from the transmitter.

The astonishing result is that *the receiver asymptotically approaches perfect synchrony with the transmitter, starting from any initial conditions*! To be precise, let

$\mathbf{d} = (u, v, w)$ = state of the transmitter or "driver"
$\mathbf{r} = (u_r, v_r, w_r)$ = state of the receiver
$\mathbf{e} = \mathbf{d} - \mathbf{r}$ = error signal

The claim is that $\mathbf{e}(t) \to \mathbf{0}$ as $t \to \infty$, for all initial conditions.

Why is this astonishing? Because at each instant the receiver has only *partial* information about the state of the transmitter—it is driven solely by $u(t)$, yet somehow it manages to reconstruct the other two transmitter variables $v(t)$ and $w(t)$ as well.

The proof is given in the following example.

EXAMPLE 9.6.1:

By defining an appropriate Liapunov function, show that $\mathbf{e}(t) \to \mathbf{0}$ as $t \to \infty$.

Solution: First we write the equations governing the error dynamics. Subtracting (2) from (1) yields

$$\dot{e}_1 = \sigma(e_2 - e_1)$$
$$\dot{e}_2 = -e_2 - 20u(t)e_3$$
$$\dot{e}_3 = 5u(t)e_2 - be_3$$

This is a linear system for $\mathbf{e}(t)$, but it has a chaotic time-dependent coefficient $u(t)$ in two terms. The idea is to construct a Liapunov function in such a way that *the chaos cancels out*. Here's how: Multiply the second equation by e_2 and the third by $4e_3$ and add. Then

$$e_2\dot{e}_2 + 4e_3\dot{e}_3 = -e_2^2 - 20u(t)e_2e_3 + 20u(t)e_2e_3 - 4be_3^2 \qquad (3)$$
$$= -e_2^2 - 4be_3^2$$

and so the chaotic term disappears!

The left-hand side of (3) is $\frac{1}{2}\frac{d}{dt}(e_2^2 + 4e_3^2)$. This suggests the form of a Liapunov function. As in Cuomo and Oppenheim (1992), we define the function

$$E(\mathbf{e}, t) = \tfrac{1}{2}\left(\tfrac{1}{\sigma}e_1^2 + e_2^2 + 4e_3^2\right).$$

E is certainly positive definite, since it is a sum of squares (as always, we assume $\sigma > 0$). To show E is a Liapunov function, we must show it decreases along trajectories. We've already computed the time-derivative of the second two terms, so concentrate on the first term, shown in brackets below:

$$\dot{E} = \left[\tfrac{1}{\sigma}e_1\dot{e}_1\right] + e_2\dot{e}_2 + 4e_3\dot{e}_3$$
$$= -\left[e_1^2 - e_1e_2\right] - e_2^2 - 4be_3^2.$$

Now complete the square for the term in brackets:

$$\dot{E} = -\left[e_1 - \tfrac{1}{2}e_2\right]^2 + \left(\tfrac{1}{2}e_2\right)^2 - e_2^2 - 4be_3^2$$
$$= -\left[e_1 - \tfrac{1}{2}e_2\right]^2 - \tfrac{3}{4}e_2^2 - 4be_3^2.$$

Hence $\dot{E} \le 0$, with equality only if $\mathbf{e} = \mathbf{0}$. Therefore E is a Liapunov function, and so $\mathbf{e} = \mathbf{0}$ is globally asymptotically stable. ■

A stronger result is possible: one can show that $\mathbf{e}(t)$ decays *exponentially fast* (Cuomo, Oppenheim, and Strogatz 1993; see Exercise 9.6.1). This is important, because rapid synchronization is necessary for the desired application.

We should be clear about what we have and haven't proven. Example 9.6.1 shows only that the receiver will synchronize to the transmitter if the drive signal is $u(t)$. This does *not* prove that the signal-masking approach will work. For that application, the drive is a mixture $u(t) + m(t)$ where $m(t)$ is the message and $u(t) \gg m(t)$ is the mask. We have no proof that the receiver will regenerate $u(t)$ precisely. In fact, it doesn't—that's why Mariah Carey sounded a little fuzzy. So it's still something of a mathematical mystery as to why the approach works as well as it does. But the proof is in the listening!

EXERCISES FOR CHAPTER 9

9.1 A Chaotic Waterwheel

9.1.1 (Waterwheel's moment of inertia approaches a constant) For the waterwheel of Section 9.1, show that $I(t) \to$ constant as $t \to \infty$, as follows:

a) The total moment of inertia is a sum $I = I_{\text{wheel}} + I_{\text{water}}$, where I_{wheel} depends only on the apparatus itself, and not on the distribution of water around the rim. Express I_{water} in terms of $M = \int_0^{2\pi} m(\theta, t)\, d\theta$.

b) Show that M satisfies $\dot{M} = Q_{\text{total}} - KM$, where $Q_{\text{total}} = \int_0^{2\pi} Q(\theta)\, d\theta$.

c) Show that $I(t) \to$ constant as $t \to \infty$, and find the value of the constant.

9.1.2 (Behavior of higher modes) In the text, we showed that three of the waterwheel equations decoupled from all the rest. How do the remaining modes behave?

a) If $Q(\theta) = q_1 \cos\theta$, the answer is simple: show that for $n \ne 1$, all modes $a_n, b_n \to 0$ as $t \to \infty$.

b) What do you think happens for a more general $Q(\theta) = \sum_{n=0}^{\infty} q_n \cos n\theta$?

Part (b) is challenging; see how far you can get. For the state of current knowledge, see Kolar and Gumbs (1992).

9.1.3 (Deriving the Lorenz equations from the waterwheel) Find a change of variables that converts the waterwheel equations

$$\dot{a}_1 = \omega b_1 - Ka_1$$
$$\dot{b}_1 = -\omega a_1 + q_1 - Kb_1$$
$$\dot{\omega} = -\frac{v}{I}\omega + \frac{\pi g r}{I}a_1$$

into the Lorenz equations

$$\dot{x} = \sigma(y - x)$$
$$\dot{y} = rx - xz - y$$
$$\dot{z} = xy - bz$$