A statistical perspective on the dynamics of bivariate chaotic maps for communications modelling

Conference or Workshop Item

A Statistical Perspective on the Dynamics of Bivariate Chaotic Maps for Communications Modelling

Rachel M Hilliam† and Anthony J Lawrance†

†*School of Mathematics and Statistics, The University of Birmingham, Birmingham, B15 2TT, England*
`rmh@for.mat.bham.ac.uk & A.J.Lawrance@bham.ac.uk`

Abstract— Statistical and dynamical properties of bivariate (two-dimensional) maps, are less understood than their univariate counterparts. This paper will give a synthesis of extended results with exemplifications by the contrasting bivariate logistic and Arnold cat maps. The use of synchronization from bivariate maps in communication modelling is also described.

I. Issues Concerning Bivariate Maps

The dynamical and statistical properties of many univariate chaotic maps are well understood and have been the basis of several chaos-based communications models over recent years. Associated research has also produced important statistical results and clarified several statistical issues concerning independence and non-linear dependence of their chaotic sequences [1, 2]. A comprehensive review of the use of chaos in telecommunications is given by [3]. More sophisticated chaos-based communication systems involve *bivariate chaotic maps* for which less is known. There are more complex issues of stability, pre-image regional structure, synchronization, dynamic behaviour and joint statistical behaviour, which deserve further understanding. In the past, continuous chaotic flows, rather than discrete maps, have mainly been investigated. Current experimental communication implementations of bivariate maps involving synchronization appear to have outreached their theoretical foundations in many instances. It is the purpose of this paper to address these issues by theoretical synthesization and exploration of two contrasting bivariate chaotic maps; the focus will be on their dynamical and statistical behaviour and their relevance to embryonic communication systems. These maps are the *bivariate logistic map* and a *bivariate Arnold cat map.* For the latter there is surprising independence, not obtainable with one-dimensional maps, both in the individual sequences and between them.

II. Mathematical Basis of Bivariate Maps

A general bivariate map will be taken in the form

$$\{x_t, y_t\} = \{\tau_x(x_{t-1}, y_{t-1}), \tau_y(x_{t-1}, y_{t-1})\}, \quad (1)$$

for $t = 1, 2, \ldots$ using a function $\tau = (\tau_x, \tau_y)$ over a region A.

Perhaps the most fundamental aspect of any map is its *fixed points.* As in one dimension, the existence of fixed points, satisfying $\tau(x, y) = (x, y)$, is relevant to the dynamical behaviour; secondly, the behaviour at these points is determined by eigen analysis of the Jacobian of the map at these points.

The *chaotic aspect*, as in one dimension, is concerned with the idea of divergence after close initial conditions, and is now determined by a *Lyapunov exponent matrix* and its eigen values. The component-wise divergence at time t, $\Delta(x_t, y_t)$, of a process started from two nearby points (x_0, y_0) and (x_0', y_0'), where $\Delta(x_0, y_0) = (x_0 - x_0', y_0 - y_0')$ is

$$\Delta(x_t, y_t) \approx DT^t(x_0, y_0)\Delta(x_0, y_0), \quad t = 0, 1, \ldots \quad (2)$$

where $DT^t = \prod_{i=1}^{t} DT(x_i, y_i)$ and $DT(x, y)$ is the Jacobian of the map at the point (x, y). As $t \to \infty$, it may be shown that $\Delta(x_t, y_t) \approx \exp(\lambda t)\Delta(x_0, y_0)$ where λ is obtained from the largest eigenvalue $q(t, x, y)$ of $DT^t(x, y)$ as $\lambda = lim_{t\to\infty} \frac{1}{t}[\log|q(t, x, y)|]$. When $DT(x, y)$ is constant in (x, y), λ is simply the log of the absolute value of the largest eigenvalue of DT. This does not necessarily mean that if the sequence is divergent the individual components will also be divergent, since the directions of convergence or divergence lie along the eigenvectors and not the $x-$ and y-axes. A consequence is that chaotic bivariate maps can be used to transmit messages using synchronisation, since a chaotic bivariate map can be non-divergent in the x and y directions whilst the (x, y) sequence is divergent. *Conditional Lyapunov exponents* of the map, to be considered in Section VII, are central to determining synchronization.

A crucial aspect of a bivariate map is its pre-image structure. Most simply a map can have unique pre-image structure $g = (g_x, g_y)$, such that $\{x_{t-1}, y_{t-1}\} = \{g_x(x_t, y_t), g_y(x_t, y_t)\} \quad t = 0, 1, \ldots$ although often it may be more complicated with multiple pre-images. The multiple pre-image structure of bivariate maps is governed by *pre-image curves, PIC*, determined by the determinant of the Jacobian of the map being zero.

Applying the map to all positions on these curves then gives the *critical curves, CC*, of the map. The PIC and CC curves enable the pre-image regional structure to be determined, identifying the number and multiplicity of pre-images at any position and in particular on regional boundaries. That the number of pre-images of a point usually depends on its position is also true for one-dimensional maps with 'curtailed' branches, but not so for the standard one-dimensional maps.

Statistical aspects of bivariate maps begin with a bivariate invariant distribution, satisfying a Perron-Frobenius type equation, but usually mathematically intractable for interesting non-invertible bivariate maps such as the bivariate logistic map of Section III. It follows that their dependency structure which includes joint dependencies is similarly intractable. Recourse to numerical simulation is thus inevitable, but can produce illuminating results. There can be analytical tractability for invertible maps as shown for the bivariate Arnold cat map in Section IV.

III. Bivariate Logistic Maps - Dynamical Properties

The *bivariate logistic map* in [4] couples two standard logistic maps, with $0 \leq c \leq 1$, in the form

$$\{x_t, y_t\} = \begin{array}{l} \{(1-c)x_{t-1} + 4cy_{t-1}(1-y_{t-1}) \,, \\ (1-c)y_{t-1} + 4cx_{t-1}(1-x_{t-1})\} \end{array} \tag{3}$$

for $0 \leq x, y \leq 1$. This map is not uniquely invertible since (x_{t-1}, y_{t-1}) cannot be solved uniquely in terms of (x_t, y_t). There are four fixed points of the bivariate logistic map, at $P_1 = (0,0)$, $P_2 = (\frac{3}{4}, \frac{3}{4})$, $P_3 = (\frac{5-\sqrt{5}}{8}, \frac{5+\sqrt{5}}{8})$ and $P_4 = (\frac{5+\sqrt{5}}{8}, \frac{5-\sqrt{5}}{8})$. The nature of these fixed points, determined by the eigen analysis, changes as c increases, undergoing a series of period doubling and hopf bifurcations. From (3)

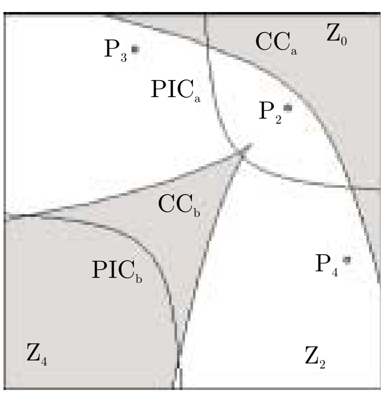

Figure 1: Critical and pre-image curves with $c = 0.5$

each point under the bivariate logistic map has 2 or 4 pre-images and thereby implies regions of the map's domain Z_2 and Z_4 respectively; the remaining region Z_0 is not visited by the map, and therefore has no preimages (see Figure 1). The boundaries of these regions are defined by the critical curves which are themselves determined by the pre-image curves given by the equilateral hyperbola $(x-1/2)(y-1/2) = \frac{(1-c)^2}{64c^2}$. The critical curves follow from substituting this hyperbola into the map (4). In Figure 1 the critical curve CC_a defines the boundary of Z_0 and Z_2 and therefore possesses only one pre-image (as two coincident pre-images) located on PIC_a. The boundary between Z_2 and Z_4 is defined by the curve CC_b. Taking the pre-image function for points on this curve will produce two coincident pre-images given by the curve PIC_b and two further distinct pre-images, which will give *excess pre-image curves*, denoted by PIC_{be1} and PIC_{be2} in Figure 2. The four grey shaded regions bounded

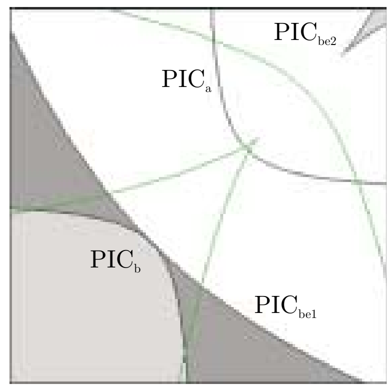

Figure 2: Excess pre-image curves with $c = 0.5$

by the curves PIC_b, PIC_{be1} and PIC_{be2} separate the plane into the regions of the four pre-images of a point in Z_4. A point in Z_2 will have two pre-images one in each of the regions above and below the curve PIC_a.

Theoretical results on divergence behaviour can be calculated for individual points, however bifurcation and invariant behaviour is complex. Tracing the bivariate sequences individually from nearby starting points indicates that the individual sequences also possess divergence behaviour for particular values of c.

IV. Arnold Cat Maps - Dynamical Aspects

The Arnold cat map [8] is one case of a relatively small number of simple uniquely invertible maps, the simplicity being largely due to the strong linearity in the structure. It is given by

$$\{x_t, y_t\} = \{(x_{t-1}+y_{t-1}), (x_{t-1}+2y_{t-1})\} \bmod (1) \tag{4}$$

and is defined on the unit square. The map takes different but linear forms over four regions $A_i, i = 1, \ldots, 4$ defined by the lines $x + 2y = 1, x + y =$

1 and $x+2y=2$. The only fixed point is $(0,0)$ and the Jacobian matrix is the constant matrix $(1,1;1,2)$ with largest eigenvalue $(3+\sqrt{5})/2$, giving a positive divergence coefficient of 0.418 and chaotic characteristics. Clearly from (4), the unique pre-image of (x_t, y_t) is given by $\{x_{t-1}, y_{t-1}\} = \{(2x_t - y_t), (y_t - x_t)\}$ mod (1) and this takes different mathematical forms over four regions delineated by $x-2y=0, x-y=0$ and $2x-y=1$, a complication for calculation.

V. Bivariate Maps - Statistical Properties

The statistical aspects of bivariate maps are considerably more complicated to obtain than those of univariate maps. A distinction must be drawn between maps with a unique pre-image and maps with multiple pre-images. For a bivariate statistical model, suppose the process starts with the random variable (X_0, Y_0), having a bivariate invariant distribution and continues via the recursion (1) to create the sequence of random variables $(X_0, Y_0), (X_1, Y_1), \ldots$.

The bivariate invariant distribution function satisfies the equation

$$\begin{aligned} P\{(X,Y) \le (x,y)\} &= P\{\tau^{-1}(X,Y) \le (x,y)\} \\ &= P\{g_x(X,Y) \le x, g_y(X,Y) \le y\} \qquad (5) \end{aligned}$$

when there is a unique pre-image. For maps with $k(\ge 1)$ pre-images of each point, let $g_{xi}(x,y)$, $g_{yi}(x,y)$ be solutions to the equation $\tau\{g_{xi}(x,y), g_{yi}(x,y)\} = (x,y)$ for $i = 1,2,\ldots,k$; then $\{g_{xi}(x,y), g_{yi}(x,y)\}$, $i = 1,2,\ldots,k$ are the k multiple pre-image functions. Thus (5) can be written

$$\begin{aligned} &P(X \le x, Y \le y) = \\ &\quad \sum_{i=1}^{k} P(g_{xi}(X,Y) < x, g_{yi}(X,Y) < y). \qquad (6) \end{aligned}$$

This leads to a bivariate generalization of the Perron-Frobenius operator for the invariant density for $f(x,y)$ of (X,Y), as

$$Pf(x,y) = \sum_{i=1}^{k} f\{g_i(x,y)\} \left| \frac{\partial g_i(x,y)}{\partial x \partial y} \right|, \qquad (7)$$

with the invariant equation being $f(x,y) = Pf(x,y)$.

The invariant bivariate density does not, of course, describe the joint lag-one auto-distributions of (X_0, X_1) and (Y_0, Y_1). The auto-distributions are defined in terms of $(X_0, \tau_x(X_0, Y_0))$ and $(Y_0, \tau_y(X_0, Y_0))$ so depending on the joint invariant distribution of (X_0, Y_0); by stationarity these also apply to (X_t, X_{t+1}) and (Y_t, Y_{t+1}).

For joint moments, Kohda's results [5] for univariate maps with a constant number of multiple pre-images can be extended in the bivariate sense. Then the joint moment $E[a(X_t, Y_t) b(X_{t+1}, Y_{t+1})]$, for functions $a(x,y)$, $b(x,y)$, can be related to the invariant joint density by the equation

$$\begin{aligned} &E[a(X_t, Y_t) b(X_{t+1}, Y_{t+1})] = \\ &\quad \int_A b(x,y) P\{a(x,y) f(x,y)\}\, dx\, dy. \qquad (8) \end{aligned}$$

It is also convenient to extend Khoda's *equidistributivity* result in a bivariate sense, and assume

$$k^{-1} f(x,y) = f\{g_i(x,y)\} \left| \frac{\partial g_i(x,y)}{\partial x \partial y} \right|, \qquad (9)$$

for $i = 1,2,\ldots,k$ over the region A; this allows explicit representation of (8) as

$$\begin{aligned} &E[a(X_t, Y_t) b(X_{t+1}, Y_{t+1})] = \qquad (10) \\ &\quad \int_A b(x,y) \left[\frac{1}{k} \sum_{i=1}^{k} a\{g_i(x,y)\} \right] f(x,y)\, dx\, dy, \end{aligned}$$

exactly parallel to Kohda's univariate map result. The theory can be further extended to higher lags to produce the recursive relation

$$\begin{aligned} &E[a(X_t, Y_t) b(X_{t+s}, Y_{t+s})] = \qquad (11) \\ &\quad E\left[\frac{1}{k} \sum_{i=1}^{k} a\{g_i(X_t, Y_t)\} b(X_{t+s-1}, Y_{t+s-1}) \right]. \end{aligned}$$

The results (10) and (11) are rather more complicated when the number of preimages depends on regions of the map, as for the bivariate logistic map. With k_j pre-images over region A_j and $A = \bigcup_{j=1}^{n} A_j$, equidistributivity is defined over each A_j as in (9) but with k_j replacing k. The integral in (10) is thus replaced by a sum of integrals over A_j with k_j replacing k in the integrand of the j^{th} integral. A result similar to (11) holds in principle, but will be quite complicated. The previous results apply most readily when there is a common mathematical formula $\tau(x,y)$ for all positions. Sometimes, however, as with the invertible Arnold cat map, the map takes different forms $\tau_j(x,y)$ over sub-region B_j of A, say, $j = 1,2,\cdots,n$. The joint expectation (10) for $k=1$ then needs to be calculated as $\sum_{j=1}^{n} \int_{B_j} b\{\tau_j(x,y)\}\, a(x,y) f(x,y)\, dx\, dy$.

VI. Statistical Behaviour of Bivariate Logistic and Arnold Cat Maps

As mentioned in Section II, the bivariate logistic map is intractable as far as explicit results for its joint invariant distribution and invariant behaviour are concerned. A thorough numerical study is beyond this brief format; behaviour is controlled by the value of c, with $c=1$ implying a pair of non-related logistic maps. For $0 < c \le 1$ a variety of joint invariant distributions are evident, often indicating significant concentrations and periodic-like behaviour.

There is no evidence of independence. In contrast, the Arnold cat map (6) can be shown to have a bivariate mean-centred independent uniform invariant distribution over the unit square; thus each X_t and Y_t are independent. It cannot be the case that (X_t, Y_t) is independent of (X_{t-1}, Y_{t-1}); this could be checked by evaluating the probability $P(X_t < x_1, Y_t < y_1, X_{t-1} < x_0, Y_{t-1} < y_0)$. With less effort it can be verified that (X_t, X_{t-1}) are independent, as also are (X_t, Y_{t-1}) and (Y_t, X_{t-1}). From calculations of lagged correlations and quadratic correlations and simulation evidence, it seems that the $\{X_t\}$ and $\{Y_t\}$ sequences are individually independent and independent of each other. The conclusions are that the generation of univariate sequences with chaotic characteristics and statistical independence can be achieved by the use of bivariate Arnold cat maps. Such statistical behaviour cannot be achieved from univariate maps because of the direct functional dependence of successive values.

VII. Embryonic Chaos-communications Implementations of Bivariate Maps

The communications motivation for the study of bivariate maps comes from the need for secure systems. When a message is encrypted using a chaotic map it is necessary to simultaneously know the resulting chaotic sequence at both the transmitting and receiving stations. This is possible using a discrete bivariate chaotic system (1) and the idea of synchronization. The fact that two chaotic systems can synchronize if one of them is driven by at least one component of the first system was initially observed by Pecora and Carroll [7] and has been widely exploited in the continuous case; however there is far less literature concerning the use of this property in relation to discrete maps. In the discrete bivariate case, the chaotic signal x_t is generated by (1) started with (x_0, y_0) and sent down the line to the receiver, where there exists an identical copy of the bivariate map, generating (x_t^R, y_t^R) in the following way. The receiver system uses x_0 together with some arbitrarily chosen y_0^R to give x_1^R and y_1^R; on the next iteration of the map, the system transmitted x_1 and the newly made y_1^R are used to produce x_2^R and y_2^R, and so on. Thus the transmitter drives the receiver system according to the equation $(x_t^R, y_t^R) = \tau(x_{t-1}, y_{t-1}^R)$.

For the receiver and transmitter to synchronise $\Delta y_t = y_t^R - y_t \rightarrow 0$. First order approximation gives $|\Delta y_t| \approx \left|\frac{\partial \tau_y}{\partial y}(x_{t-1}, y_{t-1})\right| |\Delta y_{t-1}|$ leading to $\log|\Delta y_t| \approx t\left[1/t \sum_{i=1}^{t} \log|\partial\tau_y(x_i, y_i)\partial y|\right] + \log|\Delta y_0|$. The average term can be replaced with the ensemble expectation and so y^R will synchronize with y if the *conditional Lyapunov exponent*

$$\lambda_y = E\left(\log\left|\frac{\partial \tau_y(X,Y)}{\partial y}(x,y)\right|\right) \tag{12}$$

satisfies the condition $\lambda_y < 0$. The received system generating y_t^R is used to produce a *cascaded* $x_t^C = \tau_x(x_{t-1}^C, y_{t-1}^R)$. If the other conditional Lyapunov exponent $\lambda_x < 0$, (x_t^C, y_t^R) jointly synchronises with (x_t, y_t). That is the transmitter and receiver systems are synchronised by the transmission by one of the two variables, x_t.

Once synchronized, a message bit can be transmitted, with one of the binary values leaving the system as it is and synchronized, and the other binary value modifying the transmitted chaotic signal and causing loss of synchronization. In this way, detection of synchronization or otherwise decodes the transmitted bit. Noise needs to be allowed for in the transmission channel so disturbing the ideal situation of perfectly accurate decoding. Recent work has however suggested that suitable transformations can be made to the transmitted x_t variable before the noise corrupts the signal. Back-transforming the combined received signal and noise in an appropriate way, ensures that the invariant distribution of the sequence at the receiver matches the invariant distribution at the transmitter. By this approach, not only is the effect of noise reduced, but calculation for modulation techniques which involve correlation detection will be based on the correct invariant distribution.

References

[1] T Kohda, A Tsuneda & AJ Lawrance, "Correlational properties of Chebyshev chaotic sequences", *J. Time Series Analysis*, vol.21, 2, pp.181–192, 2000.

[2] AJ Lawrance & N Balakrishna, "Statistical aspects of chaotic maps with negative dependency in a communications setting", *J. Royal Stat. Society Series B*, vol.63, to appear, 2001.

[3] MP Kennedy, R Rovatti & G Setti, *Chaotic Electronics in Telecommunications*, CRC Press, London, 2000.

[4] L Gardini, R Abraham, RJ Recard & D Fournier-Pranaret, "A double logistic map", *J. Bif. Chaos.*, vol.4, 1, pp145-176, 1994.

[5] T Kohda & A Tsuneda "Explicit evaluations of correlation functions of Chebyshev binary and bit sequences based on Perron-Frobenius operator", *Trans Inst. Electronics, Information & Communication Engineers of Japan*, E77-A, vol.11, 1794–1800, 1994.

[6] PG Drazin *Nonlinear System*, Cambridge University Press, Cambridge, 1992.

[7] LM Percora & TL Carroll "Synchronization in chaotic systems", *Physical Review Letters*, vol.64, 8, pp.821–824, 1990.