DOI: 10.13656/j.cnki.gxkx.1999.04.010
广西科学 Guangxi Sciences 1999, 6 (4): 272~277

非线性系统流的耦合同步*
Synchronization in Nonlinear Systems Coupled with Flow

王旭明　　陈光旨　　覃团发**
Wang Xuming　Chen Guangzhi　Qin Tuanfa
(广西大学物理系　南宁市西乡塘路 10号　530004)
(Dept. of Phy. Guangxi Univ., 10 Xixiangtanglu, Nanning, Guangxi, 530004, China)

摘要　基于一些自然系统混沌同步的考虑,提出了流的耦合同步法。在 Lorenz系统中数值实验验证了我们的方法,实现了全部分量、部分分量和单个分量上流的对称耦合的混沌同步。
关键词　流的对称耦合　耦合强度　混沌同步
中图法分类号　O 545

Abstract　A method of chaotic synchronization in nonlinear systems coupled with flow is proposed, which based on considering the possible synchronizing approach in some natural systems. We show this method in Lorenz system, and achieve chaotic synchronization via symmetric coupling with flow respectively in all components, in partial components and in a single component.
Key words　symmetric coupling with flow, coupling strength, chaotic synchronization

混沌同步指两系统的混沌轨道在长时间下趋于相同,表现为相空间中两系统对应量的零相位锁定。近来,学者们拓广了混沌同步的概念,出现了一些新成果[1,2],发现两个系统由一定的函数关系所支配。由此看来混沌同步仍然是一个引人注目的领域,理论和实验研究均在蓬勃开展。特别是混沌同步通讯在电路系统中的一系列成果[3~5],使该领域的研究热潮更见高涨。

变量零相位锁定的同步,就理论方法而言不外乎3种:一是变量替换耦合,包括文献[6, 7]方法和APD[5]方法;二是反馈耦全同步[8,9];三是参数耦合同步,包括参数调节法和自适应控制调节法[10]。其中反馈耦合和参数调节法在一些系统中就其实质来说是等价的。上述3种方法的共同特点是以一系统为目标,通过系统的自动调节或外加的强迫使另一系统的轨道向目标系统的轨道收敛。然而,诸如生态系统、神经系统、生命体组织等自然系统的同步,并不存在目标系统,而是不同的系统向一个预先未知的共同状态发展。同步的方式可能是通过不断交换信息流的作用,系统向共同的目标调整。

此文中,我们以系统中某种流的输入输出代表信息的交换,在 Lorenz系统中数值研究全部分量、部分分量以及单个分量上流的对称耦合的混沌同步,并对有关的现象和问题进行分析讨论。

1　流的对称耦合同步原理

考虑两连续流系统

$$\begin{cases} \dfrac{dx}{dt} = F(X,P), \\ \dfrac{dy}{dt} = F(y,P), \end{cases} \tag{1}$$

其中 F为矢量场,$X=\{x_1,x_2,\cdots,x_n\}$, $Y=\{y_1,y_2,\cdots,y_n\}$分别代表两系统的变量矢量。$P=\{p_1,p_2,\cdots,p_k\}$是系统的参数矢量。如果两系统间不断地相互输入流,则耦合后

$$\begin{cases} \dfrac{dX}{dt} = F(X,P) + \varepsilon U(X,Y), \\ \dfrac{dY}{dt} = F(Y,P) + \varepsilon' W(X,Y), \end{cases} \tag{2}$$

其中 U和 W是两系统分别向对方输入的流的函数形式(矢量式)。一般来说,系统间互换流的方式与两个系统的分布有关,依据具体的分布,U和 W的函数形式可以是任意的。式中 ε和 ε'为耦合的系数矩阵,代表耦合的强弱,对于 n维系统

$$\varepsilon = \begin{Bmatrix} X_{11} & X_{12} & \cdots & X_{1n} \\ X_{21} & X_{22} & \cdots & X_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ X_{n1} & X_{n2} & \cdots & X_{nn} \end{Bmatrix},$$

1999-02-01收稿,1999-07-16修回。
* 广西自然科学基金资助项目(9912005)。
** 广西大学计算机与信息工程学院,南宁市西乡塘路 10号,530004(College of Comp.& Info. Eng., Guangxi Univ., 10 Xixiangtanglu, Nanning, Guangxi, 530004, China)。

$$E' = \begin{Bmatrix} X'_{11} & X'_{12} & \cdots & X'_{1n} \\ X'_{21} & X'_{22} & \cdots & X'_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ X'_{n1} & X'_{n2} & \cdots & X'_{nn} \end{Bmatrix}. \quad (3)$$

若无反馈无驱动(替换)作用的互输入流能使两系统精确同步,对流的一些要求和限制是必须和自然的。首先,$U(X,Y)$ 和 $W(X,Y)$ 必须是对称的,即 $W(X,Y) = U(Y,X)$,注意这里的矢量 X、Y 在函数关系中的位置对两系统恰好是互换的,此所谓流的对称耦合。要不然,方程(2)中的两系统形式不同,就不可能精确同步。其次,E 和 E' 相等。否则,E 和 E' 的元相当于耦合而成的两个系统的参数,参数不同,则系统亦不可能精确同步。

我们对流的耦合作简化,即令

$$\begin{cases} X'_{ij} = 0, \\ X'_{ij} = 0, \end{cases} \quad i \neq j \quad (4)$$

于是方程(2)的分量式表示为

$$\begin{cases} \dfrac{dx_i}{dt} = f_i(x_1, x_2, \cdots, x_n) \\ \qquad + X_{ii}u_i(x_1, x_2, \cdots, x_n; y_1, y_2, \cdots, y_n), \\ \dfrac{dy_i}{dt} = f_i(y_1, y_2, \cdots, y_n) \\ \qquad + X_{ii}u_i(y_1, y_2, \cdots, y_n; x_1, x_2, \cdots, x_n), \end{cases} \quad (5)$$

其中 $i = 1, 2\cdots, n$,X_{ii} 简记为 X_i,u_i 为 U 第 i 个分量。

现将方程(5)中两系统的对应变量相减,并令 $e_i = x_i - y_i$,其结果的矩阵形式为

$$\frac{d}{dt}\begin{Bmatrix} e_4 \\ e_2 \\ \vdots \\ e_n \end{Bmatrix} = (A_{ij})\begin{Bmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{Bmatrix}, \quad (6)$$

式中 (A_{ij}) 表示矩阵,其元为 a_{ij},一般来讲此元无统一表式,须从两系统之差中整理出来,我们将在第四节的数值实验中作具体说明。设方程(6)的本征值为 λ,则本征值方程为

$$\det\begin{Bmatrix} a_{11} - \lambda & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} - \lambda & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} - \lambda \end{Bmatrix} = 0, \quad (7)$$

由此可解得 $\lambda = \{\lambda_1, \lambda_2, \cdots, \lambda_n\}$,方程(6)的解的一般表达式便为

$$e_i = \exp(\lambda_i t), \quad i = 1, 2, \cdots, n \quad (8)$$

当 λ_i 的实部全部小于零时,对任意的 i 就有 $\lim_{t\to\infty} e = 0$,此即长时间下 $x_i = y_i$,相空间中 x_i 和 y_i 被锁定在零相位上而同步。

2 耦合强度的确定方法

对于数值模拟实验,应当有一个合适的耦合强度 X_i,以确保两系统的同步。从前边的讨论中可知,在 $\lambda_i < 0$ 的条件下 X_i 才是合理的取值。但是通过求解本征值方程(7)来确定耦合强度对高维系统是相当繁复的。一条简捷的途径利用 Routh-Hurwitz 的线性化稳定性判据。显然,方程(6)关于 e_i 的线性化方程和原方程形式相同,有相同的本征值方程,可将其改写为如下标准形式

$$a_0\lambda^n + a_1\lambda^{n-1} + a_2\lambda^{n-2} + \cdots + a_n = 0, \quad (9)$$

Routh-Hurwitz 判据是

$$\triangle_i > 0 \quad (a_0 > 0), \quad i = 1, 2, \cdots, n, \quad (10)$$

$\triangle_i$ 为 Routh-Hurwitz 行列式,此条件是 λ_i 有负的实部的充分必要条件,因而能确保 e_i 向零收敛。这条判据较之直接求解本征值简便多了。但在某些情况下凭此确定耦合强度仍然是困难的。我们对三维系统寻找另一种更简洁判据。(9)式在三维情形为

$$\lambda^3 + a_1\lambda^2 + a_2\lambda + a_3 = 0, \quad (11)$$

设方程(11)可写为能被分解的形式

$$(\lambda + b_1)(\lambda^2 + b_2\lambda + b_3) = 0, \quad (12)$$

其解为

$$\begin{cases} \lambda_1 = -b_1, \\ \lambda_2 = \dfrac{-b_2 - \sqrt{b_2^2 - 4b_3}}{2}, \\ \lambda_3 = \dfrac{-b_2 + \sqrt{b_2^2 - 4b_3}}{2}, \end{cases} \quad (13)$$

满足同步要求的 λ_i $(i = 1, 2, 3)$ 规定了

(a) $b_1 > 0$;

(b) λ_2, λ_3 是实数还是复数,均应有 $b_2 > 0$;

(c) 若 λ_2, λ_3 是实数,则 $b_3 > 0$;

(d) 若 λ_2, λ_3 是复数,则 $b_3 < 0$;

将方程(12)展开为方程(11)的形式并与之比较得

$$\begin{cases} a_1 = b_1 + b_2, \\ a_2 = b_1b_2 + b_3, \\ a_3 = b_1b_3. \end{cases} \quad (14)$$

同步的结果是系统 $\{e_1, e_2, e_3\}$ 收缩到不动点 $\{0, 0, 0\}$,根据线性化稳定性理论,λ_i 全部为实数,那么 $\lambda_i < 0$ 的判据应为

$$a_i > 0, \quad i = 1, 2, 3 \quad (15)$$

此条件能够充分保证 e_i 向零收敛。由此确定耦合强度更快捷一些。

3 数值实验

我们以 Lorenz系统

$$\begin{cases} \dfrac{dx_1}{dt} = \sigma(x_2 - x_1), \\ \dfrac{dx_2}{dt} = x_1(R - x_3) - x_2, \\ \dfrac{dx_3}{dt} = x_1x_2 - bx_3, \end{cases} \tag{16}$$

$$\begin{cases} \dfrac{dy_1}{dt} = \sigma(y_2 - y_1), \\ \dfrac{dy_2}{dt} = y_1(R - y_3) - y_2, \\ \dfrac{dy_3}{dt} = y_1y_2 - by_3, \end{cases} \tag{17}$$

为例进行数值模拟。这是一个典型的耗散连续流系统,当参数 σ, R, b 取一定的值时系统呈现混沌运动。

流的耦合形式是灵活的,本节我们分 3种情况讨论。

3.1 全部分量上的对称耦合

假设一三维系统的全部分量上都有对方系统的流的输入与之耦合。流的函数表示取最简单的形式

$$\begin{cases} \dfrac{dx_i}{dt} = f(x_1, x_2, x_3) + \varepsilon_i y_i, \\ \dfrac{dy_i}{dt} = f(y_1, y_2, y_3) + \varepsilon_i x_i, \end{cases} \quad i = 1, 2, 3 \tag{18}$$

那么,与此类似的耦合在两个 Lorenz系统中分别为

$$\begin{cases} \dfrac{dx_1}{dt} = \sigma(x_2 - x_1) + \varepsilon_1 y_1, \\ \dfrac{dx_2}{dt} = x_1(R - x_3) - x_2 + \varepsilon_2 y_2, \\ \dfrac{dx_3}{dt} = x_1x_2 - bx_3 + \varepsilon_3 y_3, \end{cases} \tag{19}$$

$$\begin{cases} \dfrac{dy_1}{dt} = \sigma(y_2 - y_1) + \varepsilon_1 x_1, \\ \dfrac{dy_2}{dt} = y_1(R - y_3) - y_2 + \varepsilon_2 x_2, \\ \dfrac{dy_3}{dt} = y_1y_2 - by_3 + \varepsilon_3 x_3, \end{cases} \tag{20}$$

为简单考虑,令 $\varepsilon_1 = \varepsilon_2 = \varepsilon_3 = \varepsilon$,方程 (19), (20) 并整理成方程 (6) 的形式

$$\frac{d}{dt}\begin{Bmatrix} e_1 \\ e_2 \\ e_3 \end{Bmatrix} = \begin{Bmatrix} -(\sigma + \varepsilon) & \sigma & 0 \\ R - y_3 & -(1 + \varepsilon) & -x_1 \\ y_2 & x_1 & -(b + \varepsilon) \end{Bmatrix} \begin{Bmatrix} e_1 \\ e_2 \\ e_3 \end{Bmatrix}, \tag{21}$$

在整理过程中,我们从每一个对应相减的项中提出某一 e_i 来。(21) 的本征值方程为

$$\lambda^3 + (1 + b + \sigma + 3\varepsilon)\lambda^2 + [(1 + \varepsilon)(b + \varepsilon) + (\sigma + \varepsilon)(1 + b + 2\varepsilon) + x_1^2 - \sigma(R - y_3)]\lambda + (1 + \varepsilon)(b + \varepsilon)(\sigma + \varepsilon) - \sigma(b + \varepsilon)(R - y_3) + (\sigma + \varepsilon)X_1^2 = 0, \tag{22}$$

令式中 λ 的常数项为 C。由条件 (15) 得不等式

$$\begin{cases} 1 + b + \sigma + 3\varepsilon > 0, \\ (1 + \varepsilon)(b + \varepsilon) + (\sigma + \varepsilon)(1 + b + 2\varepsilon) \\ \quad + x_1^2 - \sigma(R - y_3) > 0, \\ C > 0. \end{cases} \tag{23}$$

取混沌态的参数 $\sigma = 16.0, R = 45.92, b = 4.0$,由 (23) 的第一式容易求得 $\varepsilon > -7$;第三式因包含 X 的立方项难以直接求解,第二式可写为 $(X - X_1)(X - X_2) > 0$,假设 $X_1 > X_2$,则 $X > X_1$ 或 $X > X_2$,我们只取

$$X > X_1, \tag{24}$$

用求根公式得

$$X_1 = [-(1 + b + \sigma) + \sqrt{\triangle}]/3, \tag{25}$$

其中 $\triangle = (1 + b + \sigma)^2 + 3[\sigma(R - b - 1) - b - \sigma y_3 - x_1^2]$,如果在 (25) 中用一个比之较大的数 a 取代 $-(1 + b + \sigma)$ 的位置,就能满足 (23) 的第一式和 (24),同时考虑 (23) 中的 $C > 0$,耦合强度便为

$$\varepsilon = \begin{cases} (a + \sqrt{\triangle})/3 & (C > 0 \text{且} \triangle > 0), \\ 0 & \text{其他}. \end{cases} \tag{26}$$

这种作法的实质是当同步条件不满足时,暂停系统间的互输入。理论上讲,按照 (26) 式,只要 $a > -21$,同步条件 (23) 就能满足。但是存在两个问题: 耦合强度不能太大,否则会使系统轨道跑出吸引域,轨道发散,系统遭到破坏。另外,$C > 0$ 和 $\triangle > 0$ 的条件很强,虽然根据混沌运动的遍历性,总有一段时间内条件能够满足,但因系统对初值的敏感依赖性,短暂的互输入间歇,系统间的差别就被迅速放大,由于我们无法知道在条件得到满足的时间内系统能否同步,所以 (26) 不能保证一定能够实现同步。为解决这两个问题,我们采取如下措施,当 $C > 0, \triangle > 0$ 不能满足时,令 $\varepsilon = e$ (e 为一常数) 以维持系统间的互输入。为防止轨道发散,即使在 (26) 不为零的条件得到满足的情况下,当其值超过某值 X_0 (此时轨道发散) 时,亦令 $\varepsilon = e$。因此耦合强度可修改为

$$\varepsilon = \begin{cases} (a + \sqrt{\triangle})/3 & (C > 0, \triangle > 0, (a + \sqrt{\triangle})/3 < X_0), \\ e & \text{其他}. \end{cases} \tag{27}$$

数值实验表明,$X_0 = 4.0$ 时轨道发散。图 1是 $a = 3.5, e = 0.9$ 时初值为 {0.4, 2.5, 1.0} 和 {-2.0, -

4. 22, 2. 0}的两系统之差随时间的变化过程. 同步的暂态时间较长,其原因是流的耦合并不像反馈耦合和参数调节等能给系统施加很大的强迫作用,而是靠流一点点的调节,系统才相互接近,最后得以同步.

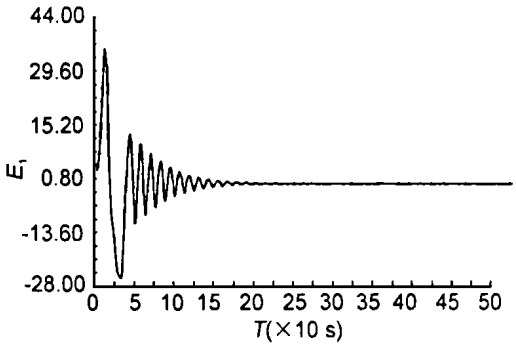

图 1 Lorenz系统全部分量上均有流的耦合时 $e_1 = x_1 - y_1$ 的时间序列,系统缓慢同步.

Fig. 1 $e_1 = x_1 - y_1$ as time progresses is shown, Lorenz systems achieve chaotic synchronization via coupling with flow in all components

3. 2 部分分量上的对称耦合

现在考虑部分分量上流的耦合,在这种情况下,由于耦合在各个分量上的不对称即系统中的耦合分量受对方系统的直接作用,而未耦合分量只是间接地受其影响,若耦合较弱,耦合使两系统接近的作用不足以压制未耦合分量比较"自由"的发展所导致两系统的分离. 只有耦合足够强,部分分量上流的耦合才能使系统同步. 为说明流的取法的灵活性,我们取如下耦合

$$\begin{cases} \dfrac{dx_1}{dt} = \varepsilon(x_2 - x_1) + \chi y_1 y_2, \\ \dfrac{dx_2}{dt} = x_1(R - x_3) - x_2 + \chi y_2 y_3, \\ \dfrac{dx_3}{dt} = x_1 x_2 - b x_3, \end{cases} \tag{28}$$

$$\begin{cases} \dfrac{dx_1}{dt} = \varepsilon(y_2 - y_1) + \chi x_1 x_2, \\ \dfrac{dx_2}{dt} = y_1(R - y_3) - y_2 + \chi x_2 x_3, \\ \dfrac{dx_3}{dt} = y_1 y_2 - b y_3. \end{cases} \tag{29}$$

两系统相减,求得对应系统的 Jacobian矩阵的本征值方程为

$$\lambda^3 + [(1 + b + \varepsilon + \chi(y_2 + x_1 y_3)]\lambda^2 + [(\varepsilon - \chi x_1)(y_2 - R) + (\varepsilon + \chi y_2) \times (1 + x_1 + y_2 + b) + \chi x_1 x_2 + (\chi x_2 - \varepsilon)(R - y_3) + b(1 + x_1 + y_3)]\lambda + b(\varepsilon - \chi y_2) \times (1 + x_1 + \chi y_3) + \chi x_1 x_2(\varepsilon + \chi y_2) + b(\varepsilon - \chi x_1)(y_2 - R) + (\varepsilon - \chi x_1)\chi x_2 y_2 = 0, \tag{30}$$

为方便起见,令方程 (30) 的一次项系数和常数项分别为 C_1 和 C_2,根据条件 (15),同步条件为

$$\begin{cases} \chi(y_2 + x_1 y_3) + 1 + b + \varepsilon > 0, \\ C_1 > 0, \\ C_2 > 0, \end{cases} \tag{31}$$

同 3. 1节关于耦合强度的讨论一样,在 $C_1 > 0$及 $C_2 > 0$的情况下,同时考虑避免轨道发散和维持系统间的相互输入,取

$$\varepsilon = \begin{cases} \dfrac{C - \varepsilon - b - 1}{y_2 - x_1 y_3} \\ \qquad (C_1 > 0, C_2 > 0, \dfrac{C - \varepsilon - b - 1}{y_2 - x_1 y_3} < \chi_0), \\ e \qquad \text{其他}, \end{cases} \tag{32}$$

其中 C为某个正数. 这种耦合在 $\chi_0 = 0.18$时就使系统跑出吸引域,我们取 $e = 0.08$,图 2是 $C = 2.0$时,系统 (28) 和系统 (29) 的同步过程. 如果把方程 (28) 和方程 (29) 的耦合由变量相乘改为变量相加,同步也容易实现,只是要求维持系统间相互输入的耦合强度比较大. 原因是耦合的变量部分比前者的作用较弱,因而耦合强度就要大一些. 基于这种事实,只要耦合足够强,单个分量上的耦合也能使系统同步.

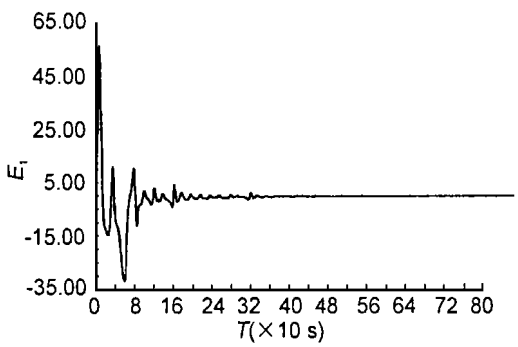

图 2 Lorenz系统两个分量上有流的耦合时 $e_1 = x_1 - y_1$ 的时间序列,系统缓慢同步.

Fig. 2 $e_1 = x_1 - y_1$ as time progresses is shown, Lorenz systems achieve chaotic synchronization via coupling with flow in two components

3. 3 单个分量上流的对称耦合

考虑如下单分量上流的耦合

$$\begin{cases} \dfrac{dx_1}{dt} = \varepsilon(x_2 - x_1) + \chi(y_1 + y_2 + y_3), \\ \dfrac{dx_2}{dt} = x_1(R - x_3) - x_2, \\ \dfrac{dx_3}{dt} = x_1 x_2 - b x_3, \end{cases} \tag{33}$$

$$\begin{cases} \dfrac{dy_1}{dt} = e(y_2 - y_1) + X(x_1 + x_2 + x_3), \\ \dfrac{dy_2}{dt} = y_1(R - y_3) - y_2, \\ \dfrac{dy_3}{dt} = y_1 y_2 - b y_3, \end{cases} \tag{34}$$

同前面的讨论一样,求(33)与(34)相减而成的系统的 Jacobian矩阵的本征值方程,从而得到耦合强度

$$\varepsilon = \begin{cases} q = \dfrac{C - e(1 + 2b + x_1 x_2 + y_3 - R) - b - x_1 x_2}{1 + 2b + R + x_1 x_2 + y_2 - y_3} \\ \qquad (C_1 > 0, q < X_0), \\ e \qquad \text{其他}, \end{cases} \tag{35}$$

$C_1 = (e + X)(b + x_1 x_2) + (e - X)(y_3 - R)b + (e - X)x_1 y_2 + X(R - y_3)x_1 + Xy_2$,$C$为某个正数,$X_0$最大为4.0 图3是$e = 3.4, C = 1.2$时,系统(33)和(34)的同步过程。从以上的讨论和数值计算来看,只有通过增大耦合强度,使其他两分量被间接地约束起来,才能有效扼制系统轨道的相互分离。

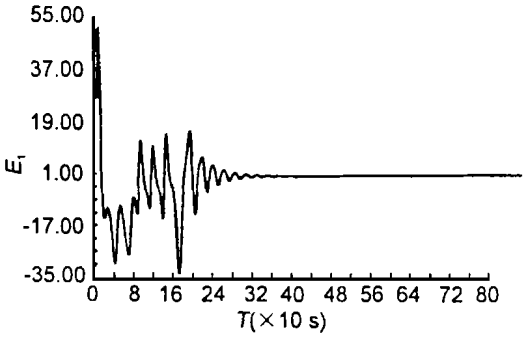

图 3 Lorenz系统单个分量上有流的耦合时 $e_1 = x_1 - y_1$的时间序列,系统缓慢同步。

Fig. 3 $e_1 = x_1 - y_1$ as time progresses is shown, Lorenz systems achieve chaotic synchronization via coupling with flow in single components

本节的数值实验说明,系统间互输入的函数形式是灵活多样的。但有两点需要说明:一、系统间的互输入改变了原系统,对于全部分量上的耦合,由于耦合作用在各分量上的对称性,小流输入就可使系统同步,所以同步后或者说新的系统的吸引子仍保留了原系统吸引子的轮廓;而部分变量上的耦合,因其作用在各变量上的不对称,必须依靠强流输入才能使系统同步,从而大大改变了原系统,新的吸引子的形状与原吸引子的大不一样(图4)。此法如用于实验系统需注意这点。二、流的输入强度要受到一定的限制,过大的耦合要么会使轨道发散,要么会改变系统的混沌运动。我们对系统(19)计算加了耦合的条件 Lyapunov指数以说明这一点。取耦合强度(27)中的 e分别为0.09和1.50时,Lyapunov指数分别为(1.97, 0.0, -32.19)和(0.0, -2.15, -28.21)可见后一种情况下,吸引子为极限环,系统作准周期运动系统(33)的 Lyapunov指数为(0.70, 0.0, -29.30),当 e再大一些时,吸引子就可能为极限环。做数值实验时要特别注意这一点。等系统完全同步后,撤消系统间的相互输入就能恢复 Lorenz吸引子,因为耦合后的吸引子还在 Lorenz吸引域内。

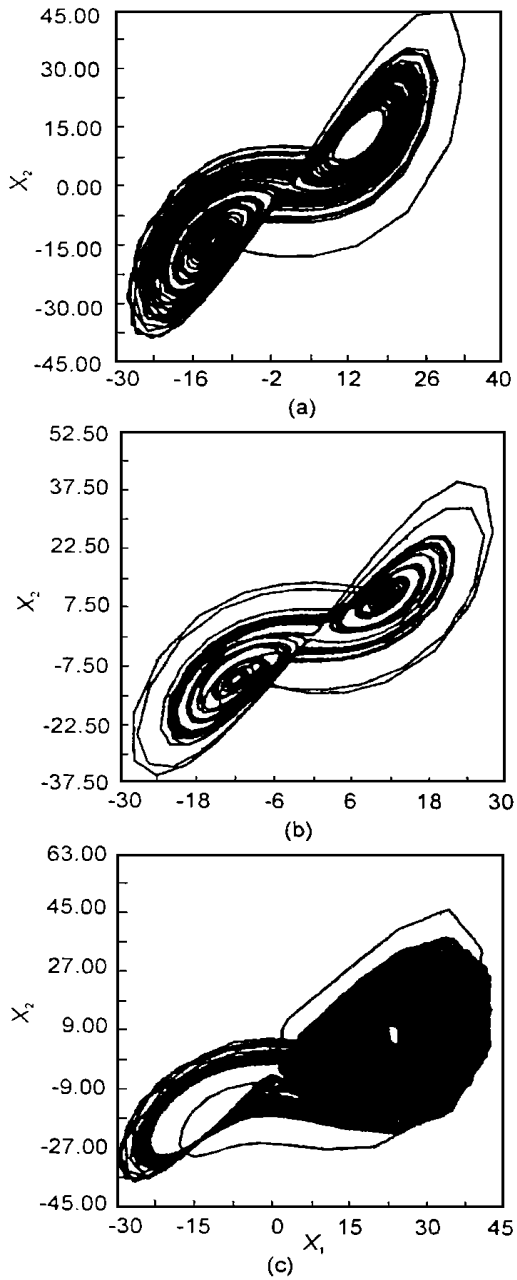

图 4 Lorenz系统的吸引子

Fig. 4 Lorenz systems

(a)无耦合 No coupled; (b)全部分量上有耦合 Coupled in all components; (c)单个分量上有耦合 Coupled in single component.

4 结语

本文考虑了一些自然系统中混沌同步的一种可能方式: 系统间连续不断地互相输入流,靠流的作用把不同的系统逐渐调整到相同的混沌态并在此后保持有相同的混沌轨道. 同步要求流的耦合对两系统必须是对称的,否则耦合后的两个系统完全不同,就无所谓同步. 我们还对三维系统的对应变量之差的收敛提出了新的判据. 在 Lorenz系统中进行了数值模拟,结果表明,全部分量上流的对称耦合在其强度较弱时就可同步,对于部分分量上流的对称耦合,由于存在耦合在各分量之间不对称的问题,强耦合才能使系统同步. 这种耦合同步方法对模拟生态系统等一些自然系统的混沌同步是一种尝试,也可用于一些人工系统.

参考文献

1 Henry, Abarbanel D I, Nikolai F. Phys Rev, 1996, E53: 4528.

2 Pecarev L, Parlitz U, Generalized synchronization, predictability and equivalence of unidirectionally coupled dynamical. Phys Rev Lett, 1996, 76: 1816.

3 Hayes S, Grebogi C, E Ott. Communicating with chaos. Phys Rev Lett, 1993, 70: 3031.

4 Perez G, Cerderra H A. Extracting messages masked by chaos. Phys Rev Lett, 1995, 74: 1970.

5 Kocarev L, Parlitz U. General approach for chaotic synchronization. with applications to communication. Phys Rev Lett, 1995, 74: 5028.

6 Pecora L M, Carroll T L. Synchronization in chaotic systems. Phys Rev Lett, 1990, 64: 821.

7 Pecora L M, Carroll T L. Driving systems with chaotic signals. Phys Rev, 1991, A44: 2374.

8 Pyrgas K. Predictable chaos in slightly perturbed unpredictable chaotic systems. Phys Lett, 1993, A181: 203.

9 Sugawarn T, Tachikawa M, Tsnkamoto T. Observation of synchronization in laser chaos. Phys Rev Lett, 1994, 72: 3502.

10 Jolly K John, Amritkar R E. Synchronization of unstable orbits using adaptive control. Phys Rev, 1994, E49: 4843.

(责任编辑: 黎贞崇)

(上接第 261页 Continue from page 261)

子是困难的. 现有各种破译方法对 $P_4^{(4)}$ 是无效的. 因此破译加密钥是不可能的.

分析密值抗破译强度, P^H 是已知的, 容易分解 $P^H \cdot m_{ij}$ 得到信息值 m_{ij}. 要保护 $P^H \cdot m_{ij}$, 取决于 T_2 元素的全部组合数量不被穷举. 由于 T_2 随机矩阵元素可以不断通过内部变换获得, 根据 $C_{200}^{25} = 2.5 \times 10^{30}$, 可使 T_2 元素达到 200个以上, 通过 (120回合以上) 环指方法, 每次选择 25个累加到密值中. 这一方案基本满足日常民用安全水平需要. 如果要求更高, 可以做到 C_{200}^{50} 要求或增加 T_2 元素.

5 结语

通过以上分析, 看到基于 PDX体制理论的 $P_n^{(r)}$ 公钥不但具有高抗击强度的多态变异功能系统, 而且还有独特的引入外部参数手段和优良的等概率构造性能, 为背包型公钥推向应用提供了新的方法.

参考文献

1 Chor B, Rivest R. A knapsack-type public key cryptosystem based on arithmetic in finite fields, IEEE Trans, Inform Theory, 1988, I T- 34, (5): 901~ 909.

2 邵祖华. 子集和组的求解与真分式背包体制的攻破: 密码学新进展, 北京: 科学出版社, 1994. 7~ 15.

3 Peter J, Smith, L U C. Public-key encryption-a secure alternative to RSA. Dr. Dobb's Journal, January 1993: 90 ~ 92.

4 彭宏祥等. P钥原型及抗击 SHORT V ECTOR破译算法研究. 广西大学学报 (自然科学版), 1996, 21 (3): 224 ~ 229.

5 彭典祥等. PDX有限机公钥密码体制. 广西大学学报 (自然科学版), 1995, 20 (3): 295~ 301.

(责任编辑: 黎贞崇)