第 20 卷 第 4 期 电 子 科 学 学 刊 Vol.20 No.4
1998 年 7 月 JOURNAL OF ELECTRONICS July 1998

一种混沌扩频码序列设计的准则 [1]

凌 聪 孙松庚

(通信工程学院信息处理研究所 南京 210016)

摘 要 本文根据符号动力学，利用混沌系统构造了一族相互独立的 Bernoulli 序列作为扩频序列，给出了获得 q 元 Bernoulli 序列的一种设计准则——测度熵等于 $\log q$ 。

关键词 混沌，测度熵，扩频序列

中图号 TN914.4, TN914.5

1 引 言

应用混沌理论来构造扩频序列近年来已经引起了广泛的关注 [1-8] 。文献 [4-8] 利用 Logistic 映射、Chebyshev 映射等映射产生直扩序列和跳频序列，研究结果表明它们具有与传统序列相近的相关特性和多址性能。但就理论层次而言，混沌扩频序列的产生大都基于某些特定的简单映射，目前仍缺乏统一的构造和分析理论。

独立、均匀分布的随机序列 (即 Bernoulli 序列) 是扩频序列的理想模型，然而它由于其不易产生、无法实时分发等缺陷而被认为难以在实际扩频通信系统中应用 [9] 。为此，人们设计了各种确定性的伪随机序列来代替它作为扩频序列，但代数方法设计的传统扩频序列并非完美无缺。本文把混沌系统的符号序列转换为扩频序列，利用符号动力学的理论构造一族相互独立的 Bernoulli 序列作为扩频序列，混沌的确定性机制使得混沌扩频码序列尽管是随机的却可以在实践中应用 (至少理论上如此) 。

2 一种基于符号动力学的混沌扩频序列设计准则

混沌运动产生信息，刻划其信息产生速率的特征量是测度熵。以下测度熵的定义主要取自文献 [10,11] 。

设有离散混沌动力学系统 (M,μ,f) ， M 是概率空间， μ 是 M 上的归一化概率测度， f 是 M 上的保测变换，即 $\mu(M)=1$ 和对任意可测集合 $A\subseteq M$ 有 $\mu(f^{-1}A)=\mu(A)$ 。令 $E=\{E_1,E_2,\cdots,E_q\}$ 是 M 的一个有限分割：

$$\cup_{i=1}^{q}E_i=M,\qquad E_i\cap E_j=\Phi,\quad i\neq j. \tag{1}$$

根据此分割可得到双边无穷序列 $\omega=\cdots\omega_{-1}\omega_0\omega_1\omega_2\cdots$ ，其中，如果 $f^n(x)\in E_i$ ，则令 $\omega_n=i$ 。 ω 称为符号序列，以 Σ 表示符号序列空间。对 $x\in M$ 定义集合 $\Sigma_x\subseteq\Sigma$ ：

$$\Sigma_x\equiv\{\omega|x\in\cap_{n=-\infty}^{\infty}f^{-n}E_{\omega_n}\}. \tag{2}$$

显然， $\omega\in\Sigma_x$ 等价于对任意 n 有 $f^nx\in E_{\omega_n}$ 。至少对应 M 中的一个点的符号序列集合 $\Sigma_E=\cup_{x\in M}\Sigma_x$ 称为允许序列集。如果在分割 E 下，对任意符号序列 ω 交集 $\cap_{n=-\infty}^{\infty}f^{-n}E_{\omega_n}$

[1] 1997-03-31 收到， 1997-10-29 定稿
江苏省自然科学基金资助课题

只包含一个点，则称分割 E 为生成分割 (generating partition)。定义符号词为有限长符号序列 $\omega_{n_1}\cdots\omega_{n_2}$，类似地定义与符号词 $\omega_{n_1}\cdots\omega_{n_2}$ 对应的点集 $E_{\omega_{n1}\cdots\omega_{n2}}=\cap_{n=n_1}^{n_2}f^{-n}E_{\omega_n}$。分割 E 的第 N 次细分 (refinement)E^N 定义为 $E^N=\{E_{\omega_0\cdots\omega_{N-1}}\}$，它仍然是一个分割。细分 E^N 的熵是

$$H(E^N)=-\sum_{E_{\omega_0\cdots\omega_{N-1}}}\mu(E_{\omega_0\cdots\omega_{N-1}})\log\mu(E_{\omega_0\cdots\omega_{N-1}}). \tag{3}$$

若不特别强调，本文的对数都以 2 为底。映射 f 关于分割 E 的熵为

$$h(f|E)=\lim_{n\to\infty}[H(E^N)/N]. \tag{4}$$

最后，映射 f 的测度熵定义为

$$h(f)=\sup_E\{h(f|E)\}. \tag{5}$$

如果 E 是生成分割，则有 $h(f)=h(f|E)$，可避免取上确界的困难。

Pesin 指出，测度熵等于所有正 Lyapunov 指数的和 [9]

$$h(f)=\sum_{\lambda_i>0}\lambda_i, \tag{6}$$

对具有 Lyapunov 指数 $\lambda_1>0>\lambda_2$ 的二维光滑可逆映射，Young 证明了测度熵与信息维的有趣关系 [9]

$$D_1=h(f)[1/\lambda_1+1/|\lambda_2|]. \tag{7}$$

混沌系统的符号序列给出了扩频序列的一种自然的产生方法，根据测度熵的概念，我们提出以下 Bernoulli 序列的构造方法：

定理　设 $E=\{E_1,E_2,\cdots,E_q\}$ 是混沌动力学系统 (M,μ,f) 的生成分割，ω 是分割 E 下的符号序列，则 ω 为 q 元 Bernoulli 序列的充分必要条件是 f 的测度熵 $h(f)=\log q$。

证明　由于允许序列集在移位映射下保持不变：$\sigma(\Sigma_E)=\Sigma_E$，从信息论的角度来看，$\Sigma_E$ 是一平稳遍历离散信源。信息论中已经证明，具有 q 个符号的离散信源的熵为 $\log q$ 的充分必要条件是 $\omega\in\Sigma_E$ 是一串独立、均匀分布的随机变量组成的序列，即 ω 为 Bernoulli 序列。又因 E 是生成分割，信源 Σ_E 的熵就是 f 的测度熵 $h(f)$。故定理获证。

因此，q 元扩频序列的构造归结为寻找一个测度熵为 $\log q$ 的混沌映射和它的生成分割。测度熵在混沌动力学中已有丰富的研究成果，它与 Lyapunov 指数、信息维之间的关系使得它理论上很容易计算，而实验上也已有从时间序列中计算测度熵的算法，因此定理为混沌扩频序列的设计提供了一个简洁实用的准则。

例 1　Logistic 映射 $x_{n+1}=1-2x_n^2$ 的生成分割是以 $x=0$ 为分界点的二进制分割，符号序列 $S=\{s_0,s_1,s_2,\cdots\}$ 由下式产生

$$s_n=\begin{cases}0, & x_n<0;\\ 1, & x_n>0.\end{cases} \tag{8}$$

因为 Logistic 映射的测度熵为 1，故它产生随机的二进制序列。

例 2 以 $-\cos(j\pi/q),(j=0,1,\cdots q)$ 为端点将 q 阶 Chebyshev 映射 [2] 的值域 $[-1,1]$ 划分为 q 个子区间，这是一个生成分割，按这些区间产生 q 元序列。因为 q 阶 Chebyshev 的 Lyapunov 指数是 $\log q$，故产生的序列是 q 元 Bernoulli 序列。

文献 [5,6] 分别利用 Logistic 映射和 4 阶 Chebyshev 映射构造了二相序列和四相序列，文献 [8] 利用 q 阶 Chebyshev 映射构造了频隙数目为 q 的跳频序列。从这些例子可看出，本文基于符号动力学的构造统一了前人的工作。由于测度熵是同构变换和拓扑共轭变换下的不变量 [9]，通过同构变换或拓扑共轭变换我们可得到许多有用的映射，例如，文献 [12] 通过 Tent 映射 (测度熵为 1) 的拓扑共轭变换，得到了一批测度熵为 1 的单峰映射，它们都可以用来产生二相序列。

3 相关特性和多址性能

将符号序列转换为扩频序列，就得到了随机扩频序列，也可以周期 N 截短获得周期序列 (N 应当足够大使得遍历性起作用)。我们将不同的初始值 $x_{0j}(j=1,2,\cdots,J)$ 分配给各个用户，以获得数量足够多的一族码序列。根据混沌对初始条件的极端敏感依赖性，我们可以合理地假设不同的初值产生的非移位等价的序列是统计独立的。

由于我们构造的混沌二相扩频序列是独立、同分布的随机序列，所以该序列族有理想的线性复杂度约 $N/2$；平衡特性服从均值为 0、方差为 N 的高斯分布，不平衡范围在 $4\sqrt{N}$ 量级；奇偶相关服从均值为 0、方差为 N 的高斯分布，最大奇、偶相关的数量级是 $4\sqrt{N}$，距 Sidelnikov 次最优界 $2\sqrt{N}$ 相差不多；奇、偶相关均方值是 N，多址容量与传统序列相当。因此混沌扩频序列是一类次最优序列。文献 [5] 给出了详细的推导和实验结果，这里不再重复。总之，理论分析和计算机模拟都表明，混沌扩频序列具有与传统序列相近的相关特性和多址性能 [5-8]。表 1 是二进制混沌扩频序列与现有扩频序列的比较。

表 1 二进制混沌扩频序列与其它扩频序列的比较

序列	周期 N	序列集大小	最大偶相关	最大奇相关	线性复杂度	不平衡范围
Gold	2^r-1 $r=2s+1$	2^r+1	$2^{(r+1)/2}+1$		$2r$	$[1,2^{(r+1)/2}+1]$
Gold	2^r-1 $r=2s+1$	2^r+1	$2^{(r+2)/2}+1$		$2r$	$[1,2^{(r+2)/2}+1]$
Kasami 小集	2^r-1 $r=2s$	$2^{r/2}$	$2^{r/2}+1$		$3r/2$	$[1,2^{r/2}+1]$
Kasami 大集	2^r-1 $r=2s$	$2^{r/2}(2^r+1)$	$2^{(r+2)/2}+1$		$5r/2$	$[1,2^{(r+2)/2}+1]$
Bent	2^r-1 $r=4s$	$2^{r/2}$	$2^{r/2}+1$		$\begin{bmatrix} r/2 \\ r/4 \end{bmatrix}\cdot 2^{r/4}$	1
No	2^r-1 $r=2s$	$2^{r/2}$	$2^{r/2}+1$		$\geq r\cdot 2^{r/2-2}$	$[1,2^{r+2}+1]$
混沌	较大的数	很大	$\sim 4\sqrt{N}$	$\sim 4\sqrt{N}$	$N/2$	$[0,\sim 4\sqrt{N}]$

4 结 论

本文提出了混沌扩频序列的构造方法，我们利用符号动力学，把符号序列转换为扩频序列，给出了获得 Bernoulli 序列的测度熵判据。通过该方法我们能利用混沌系统产生一族相互独立的 Bernoulli 序列作为扩频序列。测度熵与 Lyapunov 指数、分形维数的关系使得我们能方便地寻找这样的混沌系统。本文构造的混沌扩频码序列具有与传统序列相近的相关特

性和多址性能。当然，实际应用中有限精度混沌系统产生的符号序列不可能是真正随机的。然而实验结果表明，它们的性质与随机序列非常接近。

参 考 文 献

[1] Heidari-Bateni G, McGillem C D. A chaotic direct-sequence spread-spectrum communication system. IEEE Trans. on Commun., 1994, COM-42(2/3/4): 1524–1527.

[2] Kohda T, Tsuneda A. Pseudonoise sequences by chaotic nonlinear maps and their correlation properties. IEICE Trans. Commun., 1993, E76-B(8): 855–862.

[3] Kohda T, Tsuneda A. Explicit evaluations of correlation function of Chebyshev binary and bit sequences based on Perron-Frobenius operator. IEICE Trans. Fundamentals, 1994, E77-A(11): 1794–1880.

[4] 王亥，胡健栋. Logistic-Map 混沌扩频序列. 电子学报，1997, 21(1): 19-23.

[5] 凌聪，孙松庚. Logistic 映射扩频序列的相关分布. 电子学报，已录用.

[6] 凌聪，孙松庚. 四相混沌扩频序列. 通信学报，已录用.

[7] 凌聪，孙松庚. 混沌扩频序列产生器. 电子科学学刊，已录用.

[8] 凌聪，孙松庚. 用于码分多址通信的混沌跳频序列. 电子学报，已录用.

[9] Simon M K, Omura J K, Scholtz R A, Levitt B K. Spread Spectrum Communications. Rockville, MD: Computer Science Press, Volume I, 1985, Chap. 5

[10] E. Ott. Chaos in Dynamical Systems. Cambridge: Cambridge University Press, 1993.

[11] Alekseev V M, Yakobson M V. Symbolic dynamics and hyperbolic dynamic systems. Phys. Rep., 1981, 75(5): 287–325.

[12] Grossmann S, Thome S. Invariant distributions and stationary correlation functions of one-dimensional discrete process. Z. Naturfosch, 1977, 32a: 1353–1363.

A CRITERION FOR DESIGNING CHAOTIC SPREADING CODE SEQUENCES

Ling Cong　　Sun Songgeng

(*Institute of Communications Engineering, Nanjing* 210016)

Abstract　A criterion for designing chaotic spreading sequences based on symbolic dynamics is proposed. A family of mutually independent Bernoulli sequences can be generated by this approach. A condition for the metric entropy to obtain q-ary Bernoulli sequences is proved.

Key words　Chaos, Metric entropy, Spreading sequence

凌　聪：　男，1974 年生，硕士生，研究方向为混沌在通信中的应用和调制检测理论.

孙松庚：　男，1946 年生，教授，主要从事混沌、小波和神经网络在通信中的应用研究.