一类混沌跳频序列的性能分析

米 良
(西南电子电信技术研究所 成都 610041)

摘 要: 对一类基于混沌映射，由混沌轨道多值量化和比特抽取相结合产生的跳频序列进行了性能分析。理论分析和统计性能实验表明，该方法构造的跳频序列是贝努利随机序列，其汉明相关函数服从泊松分布。在相同的条件下(频率数目和序列长度相同)，其均匀分布性、汉明相关值和线性复杂度与其它方法产生的混沌跳频序列相当，然而其所需的迭代次数却大大减少，从而能够产生更多的跳频序列，非常适合在跳频多址通信中应用。

关键词: 跳频序列，混沌映射，汉明相关函数，线性复杂度

中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2005)11-1741-04

The Performance Analysis of Chaotic Frequency-Hopping Sequences

Mi Liang
(*Southwest Electronic & Telecommunication Technology Institute, Chengdu* 610041, *China*)

Abstract The performance analysis of chaotic Frequency-Hopping (FH) sequences, which are generated by quantization function and reshaping operation based on chaotic map, is presented in this paper. Theory analysis and performance experimental at results show that this sequence is Bernoulli sequence and its Hamming correlation is shown to be Poisson distributed. It is comparable to other FH sequences on the properties of uniform distribution, Hamming correlation and linear complexity when they have the same number of frequency slots and the same period, but much less requirements of iterative operation. It can be concluded that more FH sequences can be generated by this method and they are suitable for FH code-division multiple-access systems.

Key words Frequency-hopping sequences, Chaotic map, Hamming correlation function, Linear complexity

1 引言

目前混沌通信的研究热点有两个：一个是保密通信[1,2]，另一个是扩频通信[3－12]。混沌扩频通信的研究已取得一些进展，特别是混沌跳频序列[5－12]的研究，引起了人们的广泛关注。

针对混沌跳频通信中跳频序列的产生这一关键问题，文献[7]提出了对 Logistic 映射的轨道点进行多值量化产生 q 元跳频序列的方法，产生的混沌跳频序列具有良好的性能，但其不足之处是在某些时延下存在较大的汉明相关值。为此，文献[8]给出了一种减小其汉明相关值的新方法，构造出的跳频序列为贝努利随机序列，其汉明相关服从泊松分布，但其迭代次数较前一种方法增加了 $(\log_2 q-1)$ 倍。文献[12]对此提出了一种将混沌轨道多值量化与比特抽取相结合产生混沌跳频序列的新方法，可以在保持与文献[8]中序列性能基本不变的条件下，使其所需的迭代次数大大减少，但文献[12]只是对该方法作了计算机模拟，没有进行理论分析。本文在文献[12]的基础上，给出了该方法的理论分析，证明其构造的跳频序列是贝努利随机序列，并对该跳频序列的均匀分布性、汉明相关值和线性复杂度作了性能比较。

2 混沌跳频序列的产生

Logistic映射[7]的满映射由下式给出:

$$x_{n+1}=f(x_n)=1-2x_n^2,\ x_n\in[-1,1] \tag{1}$$

它的轨道点概率密度为

$$\rho(x)=\begin{cases}\dfrac{1}{\pi\sqrt{1-x^2}}, & x\in(-1,1)\\ 0, & \text{其它}\end{cases} \tag{2}$$

只要选取不同的初始值，经过迭代就可以得到完全不同的混沌序列，因此序列数量可以说是无穷的。

由文献[7]可知，要产生频率数目为 q 的跳频序列 $X=\{X_0,X_1,\cdots,X_{N-1}\}$，其中，$N$ 是任意的序列长度，X_n 在整数集合 $\{0,1,2,\cdots,q-1\}$ 中取值，分别代表频率 $\{f_1,f_2,\cdots,f_q\}$，可将区间 $[-1,1]$ 划分为 q 个相邻的连续子区间，使得 x_n 点落入各个子区间的概率相等。令划分点依次为

2004-06-16 收到, 2004-11-02 改回

$d_0, d_1, d_2, \cdots, d_q$，其中 $d_0 = -1$，$d_q = 1$，

易知划分点为

$$d_k = -\cos(k\pi / q), \quad k = 0,1,2,\cdots,q \tag{3}$$

文献[7]中跳频序列的生成规则为：$X_n = Q(x_n)$，其中量化函数 $Q(x)$ 定义为：如果 $d_k \le x < d_{k+1}$，则 $Q(x) = k$。

文献[8]指出这种方法产生的序列的汉明相关值较大，为此采用每隔 $\log_2 q$ 次迭代产生新的频率，即 $\{X_n = Q(x_{\delta n})\}$。当 $\delta = \log_2 q$ 时，$\{X_n\}$ 为贝努利随机序列。

文献[12]提出将混沌轨道多值量化与比特抽取相结合产生混沌跳频序列的新方法，即若要产生 N 个 q 元混沌跳频序列，首先利用 Logistic 映射迭代 N 次，产生 N 个实数值序列元素 x_n，然后进行多值量化编码，方法与文献[7]完全相同。x_n 的量化值用二进制可表示为

$$X_n = Q(x_n) = b_1(x_n)b_2(x_n)\cdots b_{\log_2 q}(x_n), \quad b_i(x_n) \in \{0,1\} \tag{4}$$

这样就可得到一个 $N \times \log_2 q$ 的矩阵

$$\begin{bmatrix} b_1(x_0) & b_2(x_0) & \cdots & b_{\log_2 q}(x_0) \\ b_1(x_1) & b_2(x_1) & \cdots & b_{\log_2 q}(x_1) \\ \vdots & \vdots & \ddots & \vdots \\ b_1(x_{N-1}) & b_2(x_{N-1}) & \cdots & b_{\log_2 q}(x_{N-1}) \end{bmatrix} \tag{5}$$

然后，对该矩阵按照列的顺序依次截取 $\log_2 q$ 个二元符号为一组，取完所有矩阵元素，即可得到 N 个 q 元混沌跳频序列 $\{F_n\}$，不妨记这种变换为 $F_n = H[X_n]$。显然，这种方法产生周期为 N、频隙数目为 q 的跳频序列，所需进行的迭代总次数为 N，而采用文献[8]的方法则至少需要进行 $N\log_2 q$ 次迭代，这样迭代总次数就减少了 $(\log_2 q - 1)$ 倍。这不仅意味着运算量的减少，而且也表明其产生的可用跳频序列数目大大增加了。

该方法可以推广应用到任何一维混沌映射

$$x_{n+1} = f(x_n) \tag{6}$$

其中 $x_n \in I, n = 0,1,2,\cdots$，$f: I \to I$ 是一个非线性映射，I 是实数域 R 中的一个闭区间。将区间 I 划分为 q 个相邻的连续子区间，使得 x_n 点落入各个子区间的概率相等，根据这些区间对 x_n 进行量化 $X_n = Q(x_n)$，并变换得到 $F_n = H[X_n]$。下面证明这种方法产生的序列是独立、均匀分布的序列，即是贝努利随机序列。

定理 设 $\{x_n\}$ 是一维混沌映射序列，$\{F_n = H[Q(x_n)]\}$ 是 q 元跳频序列，则 $\{F_n\}$ 是贝努利随机序列。

证明 由分布密度可知，量化序列 $\{Q(x_n)\}$ 在 $\{0,1,2,\cdots,q-1\}$ 上均匀分布，则其各个比特位“0”和“1”的分布也是均匀的，因此由这些比特位构成的序列 F_n 在 $\{0,1,2,\cdots,q-1\}$ 上均匀分布。将量化比特位按列抽取 $\log_2 q$ 个，就打破了量化序列 $\{Q(x_n)\}$ 原有的相关性(参见文献[8]中的图 1(a))，得到类似文献[8] 中图 1(b)的状态转移图，即 F_n 等概率地跳往 $0,1,2,\cdots,q-1$，因此其一步转移概率矩阵 P 的每项都是 $1/q$。注意到 n 步转移概率矩阵 $P^n = P$，利用 $\{F_n\}$ 的 Markov 性质，对 $k = 2,\cdots,N$ 有

$$\begin{aligned} &P(F_{i_k} = j_k, F_{i_{k-1}} = j_{k-1}, \cdots, F_{i_1} = j_1) \\ &= P(F_{i_k} = j_k \mid F_{i_{k-1}} = j_{k-1}) \cdots P(F_{i_2} = j_2 \mid F_{i_1} = j_1) P(F_{i_1} = j_1) \\ &= 1/q^k \\ &= P(F_{i_k} = j_k) P(F_{i_{k-1}} = j_{k-1}) \cdots P(F_{i_1} = j_1) \end{aligned} \tag{7}$$

式中 $0 \le i_1 < \cdots < i_k \le N-1$。因此 $F_n, n = 0,1,\cdots,N-1$ 是统计独立的，故 $\{F_n\}$ 是贝努利序列。 证毕

由上述定理可知，要设计得到 q 元扩频序列，对于某些测度熵不等于 $\log_2 q$ 的混沌映射，可以不进行每隔 $\log_2 q$ 次的迭代，只要按上述方法进行比特抽取，仍然可以得到贝努利随机序列。下面就以 Logistic 映射为例，进行性能分析。

3 性能分析

3.1 均匀分布特性

理想跳频码应具有良好的均匀分布特性，即各频点在一个码周期中出现的次数应相同。对均匀性的检测采用统计中的 χ^2 检测方法，设跳频序列长度为 N，若 q 个频率点中的第 i 个频率出现的次数为 N_i，则

$$\chi^2_{q-1} = \sum_{i=1}^{q} \frac{(N_i - N/q)^2}{N/q} \tag{8}$$

当实际序列的 χ^2_{q-1} 小于指定的显著性水平(例如 5%)下的 χ^2_{q-1} 值时，则认为该序列满足均匀分布。对序列长度 $N = 1024$，频率点 $q = 64$，任取产生的 100 个跳频序列进行检测，其检测结果如图 1 所示。长度为 1024 的 64 元跳频序列在显著性水平为 5%下的 χ^2_{q-1} 值为 82.5。采用本文方法产生的 100 个检测跳频序列中，有 4 个超过 82.5，通过率为 96%，平均的 χ^2_{q-1} 为 61.55；采用文献[8]的方法产生的 100 个检测跳频序列中，有 3 个超过 82.5，通过率为 97%，平均的 χ^2_{q-1} 为 61.99。重复 10 次试验，采用两种方法得到的平均通过率都为 95.7%。因此，本文的方法和文献[8]的方法所产生的混沌跳频序列的均匀分布性几乎完全一致，且都满足均匀分布。

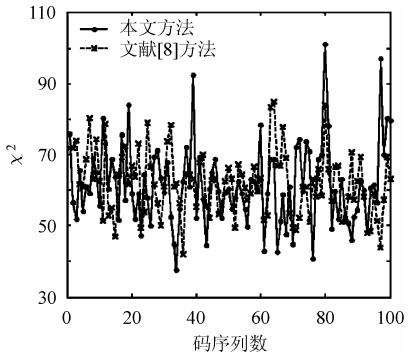

图 1 混沌跳频序列的 χ^2_{q-1} 检测

3.2　汉明相关函数

通常用周期汉明相关函数来衡量跳频序列的性能，其定义为[7]

$$H_{XY}(\tau)=\sum_{i=0}^{N-1}h(X_i,Y_{i+\tau}),\qquad 0\le\tau\le N-1 \tag{9}$$

这里，X，Y 是两个跳频序列，$(i+\tau)$ 模 N 取值且

$$h(x,y)=\begin{cases}0, & x\ne y\\ 1, & x=y\end{cases} \tag{10}$$

显然，由于本文生成的跳频序列是贝努利序列，并且由混沌的初始敏感依赖性可知，两个混沌跳频序列的汉明相关函数服从二项分布，且在 N 和 q 很大时服从参数为 N/q 的泊松分布[7]。因此，混沌跳频序列的平均汉明自相关旁瓣和互相关分别为

$$<H_{XX}>=\frac{1}{N-1}\sum_{\tau=1}^{N-1}H_{XX}(\tau)\approx N/q \tag{11}$$

$$<H_{XY}>=\frac{1}{N}\sum_{\tau=0}^{N-1}H_{XY}(\tau)=N/q \tag{12}$$

定义两个参数 $H_{XX}=\max\limits_{1\le\tau<N}\{H_{XX}(\tau)\}/N$，$H_{XY}=\max\limits_{0\le\tau<N}\{H_{XY}(\tau)\}/N$ 来分别衡量汉明自相关最大旁瓣和汉明互相关的最大值。由文献[10]可知，这两个参数的理论值都可近似为 $\left(1+\sqrt{2q\ln(N)/N}\right)\Big/q$。

数值实验中，频率点 q 分别为 64 和 128，在不同的周期长度 N 下，每个周期长度任意取 50 个序列，产生方式与前面相同，计算它们的汉明自相关最大旁瓣和汉明互相关最大值的均值以及理论值，结果如图 2 所示。由图 2 可知，本文提出的方法与文献[8]中的方法产生的混沌跳频序列相比较，其汉明自相关最大旁瓣稍差于文献[8]的方法，但其汉明互相关最大值则优于文献[8]的方法。

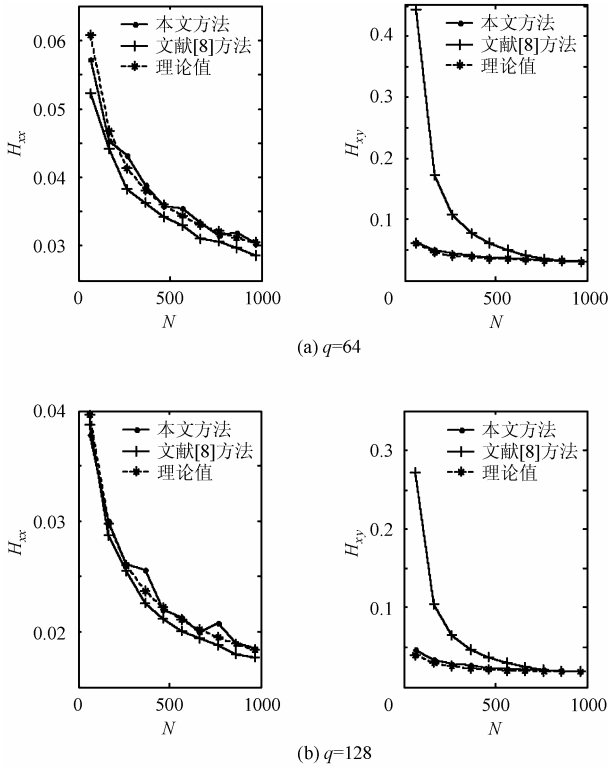

图 2　混沌跳频序列的汉明相关

根据文献[7]对混沌跳频序列的汉明相关分布的分析，混沌跳频序列的汉明互相关、汉明自相关旁瓣应服从均值为 N/q 的高斯分布。下面检测跳频序列的汉明相关分布，取序列的长度 N 为 32768，频率点 q 为 32，检测的汉明自相关旁瓣、汉明互相关分布如图 3 所示，可以看出该方法和文献[8]产生的跳频序列的汉明相关分布都与理论一致。

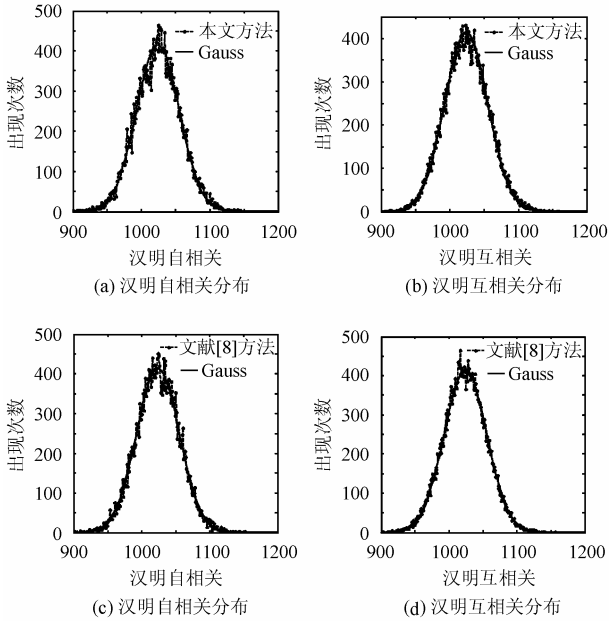

图 3　混沌跳频序列的汉明相关分布

3.3 线性复杂度

线性复杂度定义为能产生该序列的最短线性移位寄存器的阶数，在抗干扰应用中有特别重要的意义。混沌扩频序列本质上是随机二进制序列，因此它的线性复杂度的均值等于序列长度的一半，方差约为 86/81[13]，具有较理想的线性复杂度特性，这是混沌扩频序列优于传统扩频序列的一个重要体现。

跳频序列的线性复杂度测试是先将其用二进制表示，然后再对该二进制序列进行测试。数值实验中，频率点 q 分别为 64 和 128，在不同的周期长度 N 下，根据Berlekamp-Massey算法[13]得到的这些序列的线性复杂度如表 1 所示。由表 1 可知，本文方法和文献[8]方法产生的跳频序列的线性复杂度都约等于序列长度的一半，具有较理想的线性复杂度特性。

表 1 混沌跳频序列的线性复杂度

	N=200	N=400	N=600	N=800	N=1000
q=64，文献[8]方法	100	200	301	400	500
q=64，本文方法	100	200	300	402	500
q=128，文献[8]方法	100	200	300	401	498
q=128，本文方法	99	198	300	402	498

4 结束语

本文基于文献[12]，对一类混沌跳频序列的性能进行了分析。该类混沌跳频序列是先对混沌映射的轨道点进行多值量化，然后利用比特抽取产生的。理论分析和统计性能实验表明，该方法构造的跳频序列是贝努利随机序列，其汉明相关函数服从泊松分布。在相同的条件下(频率数目 q 和序列长度 N 相同)，其均匀分布性、汉明相关值和线性复杂度都与其它方法产生的混沌跳频序列相当。对于某些测度熵不等于 $\log_2 q$ 的混沌映射，可以不进行每隔 $\log_2 q$ 次的迭代，只要按上述方法进行比特抽取，仍然可以得到贝努利随机序列。这样，其所需的迭代次数较文献[8]中的方法减少了 $(\log_2 q-1)$ 倍，这不仅减少了计算量，而且大大增加了混沌跳频序列的可用数目，因此非常适合在跳频多址通信中应用。

参 考 文 献

[1] Abarbanel H D I, Linsay P S. Secure communications and unstable periodic orbits of strange attractors. *IEEE Trans. on Circuits and Syst.*, 1993, CAS-I-40(10): 643 – 645.

[2] Frey D R. Chaotic digital encoding: An approach to secure communication. *IEEE Trans. on Circuits and Syst.*, 1993, CAS-I-40(10): 660 – 666.

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

[4] Mazzini G, Setti G, Rovatti R. Chaotic complex spreading sequences for asynchronous DS-CDMA-Part I: System modeling and results. *IEEE Trans. on Circuits and Syst.*, 1997, CAS-I-44(10): 937 – 947.

[5] Ling Cong, Sun Songgeng. Chaotic frequency hopping sequences. *IEEE T ans. on Commun.*, 1998, 46(11): 1433 – 1437.

[6] 李文化, 王智顺, 何振亚. 用于跳频多址通信的混沌跳频码. 通信学报, 1996, 17(6): 17 – 21.

[7] 凌聪, 孙松庚. Logistic 映射跳频序列. 电子学报，1997, 25(10): 79 – 81.

[8] 凌聪, 孙松庚. 用于跳频码分多址通信的混沌跳频序列. 电子学报，1999, 27(1): 67 – 69.

[9] 甘良才, 易丹. 基于 Baker 变换的混沌跳频序列. 电波科学学报，2000, 15(3): 371 – 375.

[10] 骆文，甘良才. 一种组合映射产生混沌跳频序列的方法. 电波科学学报，2001, 16(3): 375 – 378.

[11] 陈勇, 凌聪. 混沌跳频序列发生器的 FPGA 实现. 电子学报，2001, 29(7): 868 – 872.

[12] 米良, 朱中梁. 一种基于 Logistic 映射的混沌跳频序列. 电波科学学报，2004, 19(3): 333 – 337.

[13] 杨义先, 林须端. 编码密码学. 北京:人民邮电出版社, 1992, 第十五章、第十六章.

米 良： 男，1970 年生，博士，研究方向为抗干扰通信技术、混沌理论及其应用等.