改进型分段线性混沌序列用作 DS-CDMA 系统直扩码的分析

饶妮妮
(电子科技大学生命科学与技术学院,四川成都 610054)

摘 要: 本文提出用改进型分段线性混沌映射来产生 DS-CDMA 系统的直扩码;分析了这类直扩码的特性以及两种量化函数对其特性的影响;计算机仿真结果表明,在适当的初值条件下这类序列具有周期长、平衡性好、自相关函数较尖锐、互关值较小以及线性复杂度高等特性,适合用作 DS-CDMA 系统直扩码.

关键词: 改进型分段线性混沌序列; 直扩码; DS-CDMA; 量化函数
中图分类号: TN929.5 文献标识码: A 文章编号: 0372-2112 (2004) 10-1684-04

Analysis of Improved Piecewise Linear Chaotic Sequences as Spreading Codes for DS-CDMA System

RAO Ni-ni
(*Institute of Life Science and Technology, UESTC, Chengdu* 610054, *China*)

Abstract: The improved piecewise linear chaotic mapping is presented to generate the spreading codes for DS-CDMA system in this paper. The spreading properties and the effects of two quantification functions on the spreading properties are analyzed. The simulation results show that the sequences have long period, good balance, δ like autocorrelation and very small cross-correlation and great linear complexity under the condition of the proper initial values and are suitable to be used as the spreading codes for DS-CDMA.

Key words: improved piecewise linear chaotic sequence; spreading code; DS-CDMA; quantification method

1 引言

DS-CDMA 系统中的抗干扰、抗多径、抗截获、保密、多址通信、实现同步等都与所采用的直扩码的特性密切相关.纵观现有直扩码的研究知[1~3],为了满足 DS-CDMA 系统对直扩码长度的各种要求,用作直扩码的伪随机(Pseudo-Noise, PN)序列应具有较长的周期;为了有效地减小系统的载波泄漏,PN 序列应具有良好的平衡性;为了减小多径干扰和自干扰,PN 序列应具有尖锐的自相关特性;为了减小系统的多址干扰,PN 序列应具有尽可能小的互相关;为了保证系统的容量和多址通信能力,PN 序列应有足够多的序列数;为了提高系统的保密性以及抗截获能力,PN 序列应具有较高的复杂度;为便于系统的同步,PN 序列的产生应在工程上易于实现.迄今为止,已有多种混沌映射所产生的混沌序列被建议作为直扩码[4~7],例如,Logistic 映射、Tent 映射以及 Chebyshev 映射等[8].然而,它们的共同缺陷是不能控制混沌序列的统计特性.在众多的混沌系统中有一类被称为"逐段线性映射"的系统[9,10],多年的研究表明它们具有均匀的分布函数及可控的统计特性.本文提出用改进型分段线性混沌映射来产生 DS-CDMA 系统的直扩码,分析了这类直扩码的特性以及量化函数对其特性的影响,证实了改进型分段线性混沌序列用作 DS-CDMA 系统直扩码的可行性.

2 改进型分段线性混沌序列的产生

本文采用如下的分段线性离散混沌系统 F 来产生混沌序列,即

$$x_{t+1}=F(x_t)=\begin{cases}-1+2(x_t+1)/p & x_t\le -1+p\\ -1+2(x_t+1-p)/(1-p) & -1+p<x_t\le 0\\ F(-x_t) & F(-x_t)\end{cases}\quad(1)$$

其中 $p\in(0,1)$, $I=[-1,1]$, $x_t\in I$. 文献[9]已经证明,迭代系统(1)是混沌的;它的输出信号 $\{x_t\}$ 在 I 上遍历且具有均匀的不变分布函数.

为满足 DS-CDMA 系统的需要,对上述模拟信号进行量化得到 0-1 二进制序列 $\{s_n(t)\}_{t=1}^{\infty}$. 已有多种量化函数被提出,本文采用的量化函数 $T_n(\cdot)$ 定义为

$$\{s_n(t)\}_{t=1}^{\infty}=T_n(x_t)=\begin{cases}0, & \text{if } x\in\bigcup_{d=0}^{2^{n-1}-1}I_{2d}^n\\ 1, & \text{if } x\in\bigcup_{d=0}^{2^{n-1}-1}I_{2d+1}^n\end{cases}\quad(2)$$

式中:$n>0$ 为任意正整数;$I_0^n, I_1^n, \cdots, I_{2^n-1}^n$ 代表 $[-1,1]$ 的 2^n 个连续的等分区间.这种量化函数使 $\{s_n(t)\}_{t=1}^{\infty}$ 在理论上具有优良的统计特性[10].不同量化函数对混沌二进制序列的特

收稿日期: 2002-12-13; 修回日期: 2004-08-06
基金项目: 电子对抗国防科技重点实验室项目资助

性产生的影响不同.

考虑到大多数混沌序列发生器都是在有限精度下实现的, 受有限精度效应的影响, 混沌系统会产生短周期的混沌序列, 而且混沌序列的特性也将变差[9]. 周红等人提出了用扰动的方法来克服混沌系统的有限精度效应. 他们的结论是, 对一个特定的混沌系统, 其对应的扰动序列必须满足一定的周期、幅度和分布才能使该混沌系统在有限精度下的输出信号接近理论特性. 在他们的研究中, m 序列被作为扰动序列. 扰动方法的引入为混沌系统的工程实现提供了可行的途径.

本文提出采用 *KMM* 序列 $\{\omega_t\}_{t=1}^{\infty}$ 来实现对式(1)的分段线性混沌系统进行扰动, 得到改进型分段线性混沌序列发生器, 如图 1 所示. 其中, *KMM* 序列的产生方法请参见文献[11].

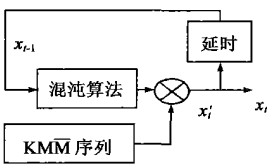

图 1　改进型分段线性混沌序列发生器框图

KMM 序列通过如下方法形成扰动向量 $p_t = (-1)^{\omega_t}\sum_{i=2}^{m} 2^{-i}\omega_{t-i+1}$, 扰动过程为 $x_t = p_t + x'_t$. 最小扰动位数定义为[9]:

$$m_m = \lfloor \log_2(k_m + 1) \rfloor \tag{3}$$

其中, k_m 为混沌系统最大斜率的绝对值, $\lfloor x \rfloor$ 符号表示取最小大于等于 x 的整数.

根据文献[11]的结论, *KMM* 序列的周期比 m 序列长得多, 序列数量也比 m 序列大得多; 二者平衡性、线性复杂度长度和互相关等特性相同; 自相关特性比 m 序列的差; 二者的分布类似. 与 m 序列扰动相比较, 采用 *KMM* 扰动能够使输出序列的周期更长, 序列数量更多.

3　直扩码特性分析

3.1　初值敏感性(序列数量)

众所周知, 混沌系统具有对初值十分敏感的特性. 换句话说, 只要初值作微小的改变, 混沌系统便输出两组完全平移相异的序列. 混沌系统的这一大优势使它能够提供数量巨大的 PN 序列, 以便满足大容量 CDMA 系统的要求, 是其他任何伪随机序列发生器均无可比拟的.

通过计算机仿真来分析改进型分段线性混沌系统的初值敏感性. 具体做法是: (1) 随机选择两组不同初值, 要求两组初值中参数 p 相同, x_0 仅相差 10^{-14}; (2) 随机选择两组不同初值, 要求两组初值中参数 x_0 相同, p 仅相差 10^{-14}, 各进行 1000 次仿真. 结果表明, 各次仿真的输出序列在平均经历约 25 次迭代后, 均得到两组完全不同的混沌序列, 说明改进型分段线性混沌系统对参数 x_0 和 p 很敏感, 而且初值和参数值相差越大, 得到不同序列所需的迭代次数越少.

由于改进型分段线性系统对初值敏感, 因此, 通过改变初值可以得到数量巨大的混沌序列, 这正是大容量 CDMA 系统所需要的直扩码特性.

3.2　周期

根据文献[9]的结论, 改进型分段线性混沌序列的周期是 *KMM* 序列周期的整数倍. 由于 *KMM* 序列的周期长度可控, 所以改进型混沌序列的周期长度也可控.

3.3　平衡性

定理 1　图 1 输出序列 x_t 经式(2)的不可逆变换后, 得到二进制序列 $\{s_n(t)\}_{t=1}^{\infty}$. 设 $\{s_n(t)\}_{t=1}^{\infty}$ 中"1"的个数为 $n_1(J) = \sum_{t=1}^{J} S_n(t)$, "0"的个数为 $n_0(J) = J - n_1(J)$, 则"0"与"1"的比 $r_{01} = \lim_{J\to\infty}\frac{n_0(J)}{n_1(J)} = 1$. 证明略.

表 1 给出了在两组不同初值和参数下, 长度分别为 J = 32、64、128、256、512 的改进型混沌序列的 r_{01} 值.

仿真实验结果表明, 平衡性与初值有关. 在不同初值下, 可能出现长序列的平衡性比短序列的平衡性差, 如表 1 中初值 1 下 J = 128 的平衡性比初值 2 下 J = 512 的好. 在大多数初值条件下, 平衡性与序列长度有关, 序列越长, 其平衡性愈好, 随着序列长度无限增长, 序列的平衡性将与理论分析结果吻合. 因此, 在实际应用中, 应该根据 DS-CDMA 系统对平衡性的要求通过改变初值优选直扩码序列.

表 1　改进型混沌序列的平衡性(初值起始值)

序列长度	32	64	128	256	512
r_{01}(初值 1)	1.05	0.99	1	1	1
r_{01}(初值 2)	1.033	1.039	1.03	1.033	1.022

初值 1: p = 0.812345612223456, x_0 = 0.6339012345646,
初值 2: p = 0.112345612223456, x_0 = 0.433901234564.

表 2　归一化自相关最大旁瓣值

序列长度	32	64	128	256	512
θ_{amax}(初值 1)	0.3	0.262	0.209	0.159	0.123
θ_{amax}(初值 2)	0.275	0.231	0.22	0.164	0.123
θ_{amax}(初值 3)	0.337	0.262	0.212	0.176	0.123

初值 1: p = 0.812345612223456, x_0 = 0.5789012345646;
初值 2: p = 0.812345612223456, x_0 = 0.2389012345646;
初值 3: p = 0.612345612345 6, x_0 = 0.3389012345646.

3.4　相关性

本文用 $\theta_a(\tau)$ 表示自相关, 用 $\theta_c(\tau)$ 表示互相关.

(1) 自相关

定理 2　图 1 输出序列 x_t 经式(2)的不可逆变换后, 得到二进制序列 $\{s_n(t)\}_{t=1}^{\infty}$. $\{s_n(t)\}_{t=1}^{\infty}$ 具有 δ-*like* 的自相关特性, 即 $\theta_a(\tau) = \delta(\tau)$. 证明略.

表 2 给出了三组不同初值和不同序列长度下自相关函数归一化最大旁瓣值的计算机仿真结果. 归一化最大旁瓣值 θ_{amax} 的大小反映了自相关函数的尖锐程度. 通常, 归一化最大旁瓣值越小, 自相关函数越尖锐, DS-CDMA 系统的多径干扰和自干扰就越小.

从表 2 中知, 在同一初值条件下, 序列越长, 归一化自相关最大旁瓣值越小, 显然有 $\lim_{J\to\infty}\theta_{amax} = 0$, 与理论分析结果相吻合. 在序列长度 J 较短(J < 512)的情况下, 归一化自相关最大旁瓣大小受初值影响较大, 即同一长度下, 不同初值的归一化自相关最大旁瓣相差较大; 但当 J 较长时(一般 J > 512), 初值对归自相关最大旁瓣值的影响减小.

(2) 互相关

定理 3[9] 图 1 输出序列 x_t 经式(2)的不可逆变换后,得到二进制序列$\{s_n(t)\}|_{t=1}^{\infty}$.$\{s_n(t)\}|_{t=1}^{\infty}$具有为零的互相关特性,即对于不同的 m 和 $n(m, n>0)$, $\theta_c(m, n, \tau)=\delta(m-n, \tau)$.

在三组不同初值和不同序列长度下改进型分段线性混沌序列归一化最大互相关函数值 θ_{cmax} 的计算机仿真结果表 3 所示.通过仿真可以发现,在同一初值条件下,序列越长,其归一化最大互相关函数值越小,当序列长度 $J\to\infty$时,必有 $\theta_{cmax}\to 0$,与理论分析一致;在不同的初值条件下,相同长度序列的归一化最大互相关函数值受初值参数变化的影响较大,例如,当 $J=512$,表 3 中初值 3 的 θ_{cmax} 最小.这些结果表明,可以通过选择初值来产生具有较理想互相关特性的改进型分段线性混沌序列.

表 3 最大互相关

序列长度	32	64	128	256	512
θ_{cmax}(初值 1)	0.343	0.290	0.220	0.185	0.139
θ_{cmax}(初值 2)	0.331	0.309	0.223	0.171	0.137
θ_{cmax}(初值 3)	0.356	0.287	0.214	0.152	0.118

初值 1: $p1=0.67543256780945$, $x_{01}=-0.6789012345646$, $p2=0.51234561223456$, $x_{02}=-0.3389012345646$;

初值 2: $p1=0.6754001256893 4$, $x_{01}=0.1789012345646$, $p2=0.80103241223456$, $x_{02}=-0.3389012345646$;

初值 3: $p1=0.33$, $x_{01}=0.7890123456461$, $p2=0.01032412234568$, $x_{02}=-0.68901234564633$.

3.5 线性复杂度

图 1 输出序列 x_t 经式(2)的不可逆变换后,得到二进制序列$\{s_n(t)\}|_{t=1}^{\infty}$.$\{s_n(t)\}|_{t=1}^{\infty}$中各比特是独立二项分布的,即概率关系

$$p(s_n(1)=b_1, s_n(2)=b_2, \cdots, s_n(t)=b_t)=0.5^t,\ t\geq 1$$

成立,从而$\{s_n(t)\}|_{t=1}^{\infty}$有下述线性复杂度 LC

$$\lim_{J\to\infty} LC(\{s_n(t)\}_{t=1}^{J})\approx J/2 \qquad (4)$$

计算机仿真计算 1000 组不同初值和各种序列长度下的线性复杂度均与理论结果很吻合.

4 量化函数对直扩码特性的影响分析

虽然实值混沌序列可以直接作为直扩码序列,但是二进制混沌序列在 DS-CDMA 系统中也大有"用武之地".目前,将实值混沌序列量化成二进制混沌序列的主要方法有:门限函数法、二进制取值法和不可逆映射法.有关研究表明,量化函数对序列的特性有较大影响[6].由于门限函数方法是一种比较粗造的量化方法,已较少采用,因此这里主要将二进制取值法和不可逆映射法用作改进型分段线性混沌序列的量化函数,用统计分析法比较二者对直扩码特性的影响.

4.1 对平衡性的影响

通过计算 1000 组不同初值和长度 J 分别为 32、64、128、256、512 的序列的 0-1 比 r_{01} 和 χ^2 通过率的平均值来检验两种量化函数对平衡性的影响.r_{01} 的大小反映了长度为 J 的序列中"0"的个数与"1"的个数相差多大,χ^2 检验通过率反映了长度为 N 的序列中"0"和"1"的分布情况.表 4 是在一组初值条件下,分别采用二进制取值法和不可逆映射法所得序列的平衡性;表 5 是另一组初值下所得的平衡性.

表 4 对平衡性的影响

序列长度	32	64	128	256	512
二进制 r_{01}	1.07	1.03	0.99	1	1
不可逆 r_{01}	1.05	0.99	1	1	1
二进制 χ^2	95%	96%	98%	96%	95%
不可逆 χ^2	95%	95%	97%	97%	99%

初值 $p=0.81234561223456$, $x_0=0.6339012345646$

表 5 对平衡性的影响

序列长度	32	64	128	256	512
二进制 r_{01}	1.06	1.03	1.01	0.99	1
不可逆 r_{01}	1.033	1.039	1.03	1.033	1.022
二进制 χ^2	98%	98%	98%	97%	98%
不可逆 χ^2	99%	98%	98%	95%	96%

初值: $p=0.11234561223456$, $x_0=0.4339012345646$

表 4 和表 5 的结果表明序列的平衡性主要受混沌系统初值和序列长度的影响较大,与采用的量化函数关系不大.

4.2 对自/互相关特性的影响

通过比较同一初值条件下由两种量化函数所得序列的自相关最大旁瓣值 θ_{amax} 或互相关值 θ_{cmax} 的大小来检验两种量化方法对序列自/互相关特性的影响.随机选取三组不同初值,表 6 和表 7 分别给出了在其中一组初值下自相关和互相关的仿真结果.

从表 6 的结果知,同一长度下二进制取值法所得自相关最大旁瓣值略小于不可逆映射法,即采用二进制取值法能获得略优于不可逆映射法的自相关特性.

与自相关特性的结论类似,同一长度下二进制取值法所得互相关最大值略小于不可逆映射法,即采用二进制取值法能获得略优于不可逆映射法的互相关特性.

表 6 对自相关特性的影响

序列长度	32	64	128	256	512
二进制 θ_{amax}	0.287	0.256	0.218	0.153	0.127
不可逆 θ_{amax}	0.3	0.262	0.231	0.161	0.129

初值 $p=0.81234561223456$, $x_0=0.6339012345646$

表 7 对互相关的影响

序列长度	32	64	128	256	512
二进制 θ_{cmax}	0.256	0.231	0.190	0.150	0.114
不可逆 θ_{cmax}	0.356	0.287	0.214	0.152	0.118

初值 $p1=0.33$, $x_{01}=0.7890456745646 1$, $p2=0.01032412234568$, $x_{02}=-0.68901234564633$

4.3 对线性复杂度的影响

大量统计实验表明,任意初值条件下不可逆映射法与二进制取值法所得线性复杂度曲线相同,所以两种量化函数对序列线性复杂度的影响相同.

综上所述,不可逆映射法的算法较复杂,硬件实现的复杂度较大,而二进制取值法十分易于硬件实现,数字混沌序列发生器电路本身就是直接对二进制数进行处理,因此,二进制取值法是一种比不可逆映射法更适合应用于改进型分段线性混

沌系统的量化函数.

5 结论

采用 *KMW* 序列对分段线性混沌系统实施扰动得到改进型分段线性混沌序列. 这类序列能够克服因有限精度效应引起的短周期行为, 在适当的初值条件下具有周期长、平衡性好、自相关函数较尖锐、互相关较小以及线性复杂度理想等直扩码特性. 量化函数对这类序列的平衡性几乎无影响; 由二进制取值法映射所得序列的自相关和互相关特性略优于不可逆映射法; 两种量化函数对序列的线性复杂度影响相同. 然而, 不可逆映射法的算法较复杂, 硬件实现复杂度较大. 由于数字混沌序列发生器电路本身就是直接对二进制数进行处理, 所以二进制取值法十分易于硬件实现. 二进制取值法是一种比不可逆映射法更适合应用于改进型分段线性混沌系统的量化函数. 改进型分段线性混沌序列是一类有潜力的、适合用作 DS-CDMA 系统直扩码的 PN 序列.

参考文献:

[1] M B Pursley, H F A Roefs. Numerical evaluation of correlation parameters for optimal phases of binary shift-register sequences[J]. IEEE Trans on COM, 1979, 27(10): 1597- 1604.

[2] R A Scholtz, L R Welch. GMW sequences[J]. IEEE Trans On IT, 1984, 30(3): 548- 553.

[3] Xu Duan Lin, Kyung Hi Chang. Optimal PN sequence design for quarrsisynchronous CDMA communication systems[J]. IEEE Trans on COM, 1997, 45(2): 221- 226.

[4] D Sandoval-Morantes, D Munoz-Rodriguez. Chaotic sequences for multiple access[J]. Electronics Letters, 1998, 34(3): 235- 237.

[5] Tohur Kohda, Akio Tsuneda. Pseudonoise sequences by chaotic nonlinear maps and their correlation properties[A]. IEICE Trans Commun[C]. 1993, E97~ B(8): 855- 862.

[6] Gianluca Mazzini, Gianluca Setti, Riccardo Rovatti. Chaotic complex spreading sequences for asynchronous DS-CDMA[J]. IEEE Trans On-CAS, 1997, 44(10): 937- 947.

[7] Ghobad Heidari-Bateni, Clare D McGillem. A chaotic direct-sequence-spread-spectrum communication system[J]. IEEE Trans on COM., 1994, 42(2/3/4): 1524- 1527.

[8] 胡健栋, 郑朝辉, 龙必起, 李兴明. 码分多址与个人通信[M]. 北京: 人民邮电出版社, 1996: 90- 155.

[9] 周红等. 有限精度混沌系统的 m 序列扰动实现[J]. 电子学报. 1997, 25(7): 95- 97.

[10] 桑涛, 王汝笠. 一类新型混沌反馈序列的理论设计[J]. 电子学报, 1999, 27(7): 47- 50.

[11] 饶妮妮, 龚耀寰. KMW 序列伪随机特性分析[J]. 电子科技大学学报, 1994, 23(4): 363- 369.

作者简介:

饶妮妮　女, 1963 年生于四川宜宾, 籍贯重庆, 教授、博士生导师, 1997 年 9 月至 1998 年 9 月和 2003 年 11 月至 2004 年 2 月在英国作学术访问, 在国内外核心刊物、国际国内学术会议上发表涉及生物信息学、生物医学工程、移动通信和教学研究的论文 30 多篇, 现在的研究兴趣包括: 移动通信、信号/图像处理、生物医学信息学.

(上接第 1689 页)

参考文献:

[1] A Shamir. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612- 613.

[2] H.-Y. Lin, Ham L. A generalized secret sharing scheme with cheater detection[A]. Advances in Cryptology-ASIACRYPT' 91 Proceedings[C], Berlin: Springer-Verlag, 1993. 149- 158.

[3] M Carpentieri. A perfect threshold secret sharing scheme to identify cheaters[J]. Designs, Codes and Cryptography, 1995, 5(3): 183- 197.

[4] J Rifa-Coma. How to avoid the cheaters succeeding in the key sharing scheme[J]. Designs, Codes and cryptography, 1993, 3(3): 221- 228.

[5] C Padró, G Sáez. Detection of cheaters in vector space secret sharing schemes[J]. Designs, Codes and Cryptography, 1999, 16(1): 75- 85.

[6] 张建中, 肖国镇. 可防止欺诈的秘密共享方案. 通信学报, 2000, 21(5): 81- 83.

[7] E F Brickell, D R Stinson. The detection of cheaters in threshold scheme[A]. Advances in Cryptology-CRYPTO' 88[C], Berlin: Springer-Verlag, 1988. 564- 577.

[8] L Ham, H Lin. An l-span generalized secret sharing scheme[A]. Advances in Cryptology-CRYPTO' 92[C]. Berlin: Springer-Verlag, 1992. 558- 565.

[9] L Ham. Efficient sharing (Broadcasting) of multiple secrets, IEE Proc.-Comput. Digit. Tech. 1995, 142(3): 237- 240.

[10] L Chen, D Gollmann, C J Mitchell, P Wild. Secret sharing with reusable polynomials[A]. The Second Australasian Conference on Information Security and Privacy-ACISP' 97[C]. Berlin: Springer-Verlag, 1997. 183- 192.

[11] GENNARO R., JARECKI S., KRAWCZYK H. et al. Robust and efficient sharing of RSA functions[A]. Advanced in Cryptology-- CRYPTO' 96 Proceedings[C]. Berlin: Springer Verlag, 1996. 157- 172.