

文章编号:1001 – 893X(2011)05 – 0028 – 05

长周期跳频码序列性能统计检测^{*}

蔡善法,刘 刚,汤宏伟
(空军装备研究院 通信所,北京 100085)

摘 要:针对长周期跳频码序列,在周期序列性能检测分析方法基础上进行了修正,使之与实际使用情况更趋一致,并采用此方法对某实际使用的跳频码序列进行统计分析,为长周期跳频序列性能检测提供了一种新方法。
关键词:跳频通信;跳频码序列;序列周期;均匀性;相关性能;线性复杂度
中图分类号:TN914.4 **文献标识码:**A doi:10.3969/j.issn.1001 – 893x.2011.05.006

Test and Analysis Methods for Long – period FH Code Sequence

CAI Shan-fa , LIU Gang , TANG Hong-wei
(Communication Institute, Air Force Equipment Academy, Beijing 100085, China)

Abstract: Based on the test and analysis methods for periodical sequence, an improved analysis method is proposed for long – period FH(Frequency Hopping) code sequence. Some FH code sequence is analysed with this method. The experiment result shows the proposed method can work better than traditional methods in the application. It provides a new method for detection of long – period FH sequence.
Key words: FH communication; FH code sequence; sequence periods; uniformity; correlation; linear complexity

1 引 言

跳频通信作为一种抗干扰通信方式,在军事通信中的应用越来越受到重视。作为跳频通信的一个重要组成部分,跳频码序列性能的好坏将直接决定跳频通信系统的抗干扰能力。

衡量跳频码序列的性能指标主要有一维均匀性、自相关、互相关、宽间隔和线性复杂度等^[1,2],对应的实际使用性能主要有两方面:一是抗敌方破译能力,要求序列具有很长的周期、很好的随机性和非线性;二是组网能力,要求序列具有良好的相关性。对跳频码序列性能的检测通常采用以理想跳频码序列为目标的 χ^2 统计检测,只要通过 χ^2 统计检测,就可认为此项指标达到实用要求。

随着软硬件技术的飞速发展,目前实用跳频系统大都采用长周期跳频码序列,针对周期序列的性

能检测分析方法已不能准确表述长周期跳频码序列的性能。目前已有的方法是截取序列中的若干段,采用周期序列的检测方法进行统计分析,来定量分析长周期序列的性能^[3,4]。本文对已有的分析检测方法进行了修正,使之能更好地反映长周期跳频码序列的实际使用性能。

2 理论基础

2.1 一维均匀性检验(等分布检验)

对于一段长度为 L 、频隙数为 q 的跳频码序列,若要满足一维均匀性要求,即在 q 个频率点上跳频码出现的概率应相同。对实用长周期跳频码序列分布的一维均匀性检测采用以理想跳频码序列为目标的 χ^2 统计。

一维均匀性判据:设在这段长度为 L 的序列中

^{*} 收稿日期:2011 – 04 – 07;修回日期:2011 – 05 – 18
• 28 •

第 $i(i \in GF(q))$ 个频率点的出现次数为 f_i , 则:

$$\chi^2_{q-1} = \sum_{i \in GF(q)} \frac{\left(f_i - \frac{L}{q}\right)^2}{\frac{L}{q}} \quad (1)$$

当计算的 χ^2_{q-1} 值小于指定的显著性水平 (例如 5%) 下自由度为 $q-1$ 的 χ^2 理论值时, 则 f_i 以值 L/q 均匀分布的假设为真, 否则为假。

2.2 汉明相关性检验

随着跳频通信的广泛使用, 在同一战场上将会同时存在许多跳频电台, 它们之间必然会相互干扰。由于各用户 TOD 设置不同或因传输延时的差异, 在某一时刻, 可能有两个或更多电台跳变到同一频率, 造成频率重合干扰, 表征这一参数采用汉明相关。对周期序列, 汉明相关采用周期移位相关^[1]。

对长周期跳频码序列, 应采用与跳频通信系统实际使用相一致的汉明相关。考虑到目前大多跳频通信系统采用基于 TOD 的同步方式, 允许跳频同步时差为 t 秒, 跳频速率为 n 跳/秒。为了实现异步组网时网内成员在不同网间的自由进出, 则各网间时差 Δt 必须满足 $-\frac{t}{2} \leq \Delta t \leq \frac{t}{2}$ 。因此在分析序列互相关性能时, 采用修正的非周期汉明相关, 即将周期汉明相关的相关时延 τ 调整为 $-\frac{t \times n}{2} \leq \tau \leq \frac{t \times n}{2}$ 。对于长度为 L 的被测序列, 截取的陪测序列长度为 $2M+L$, 且 $M = \frac{t \times n}{2}$, 被测序列在陪测序列内滑动计算相关值。

2.3 非周期汉明异相自相关

对于同步引导用的跳频码序列, 汉明自相关性主要影响系统同步性能, 同时也影响系统的抗多径干扰能力。

(1) 非宽间隔跳频码序列

对于长度为 L (陪测序列长度 $2M+L$, $M = \frac{t \times n}{2}$)、频隙数为 q 的非宽间隔跳频码序列, 在相对时延 τ 下, 计算非周期汉明异相自相关 $H_A(X, \tau)$ 和均值 $\overline{H_A(X)}$:

$$\begin{cases} H_A(X, \tau) = \sum_{j=0}^{L-1} h[x(j), x(j+\tau)] \\ \overline{H_A(X)} = \frac{1}{2M} \left[\sum_{\tau=-M}^{-1} H_A(X, \tau) + \sum_{\tau=1}^M H_A(X, \tau) \right] \end{cases} \quad (2)$$

式中, $-M \leq \tau \leq M, \tau \neq 0$ 。

$$\begin{aligned} h[x(j), x(j+\tau)] &= \begin{cases} 0, & x(j) \neq x(j+\tau) \\ 1, & x(j) = x(j+\tau) \end{cases} \\ \chi^2_{2M-1} &= \sum_{\tau=-M}^{-1} \frac{[H_A(X, \tau) - \overline{H_A(X)}]^2}{\overline{H_A(X)}} + \sum_{\tau=1}^M \frac{[H_A(X, \tau) - \overline{H_A(X)}]^2}{\overline{H_A(X)}} \end{aligned} \quad (3)$$

若 χ^2_{2M-1} 的值小于指定显著性水平 (例如 5%) 下的自由度为 $2M-1$ 的 χ^2 理论值, 则 $H_A(X, \tau)$ 以 $\overline{H_A(X)}$ 均匀分布的假设为真, 否则为假。

(2) 宽间隔跳频码序列

对于长度为 L (陪测序列长度为 $2M+L$, $M = \frac{t \times n}{2}$)、频隙数为 q 、最小频隙间隔为 d 的宽间隔跳频码序列, 在相对时延 τ 下, 计算非周期汉明异相自相关 $H_A(X, \tau)$ 和均值 $\overline{H_A(X)}$:

$$\begin{cases} H_A(X, \tau) = \sum_{j=0}^{L-1} h[x(j), x(j+\tau)] \\ \overline{H_A(X)} = \frac{1}{2M-2} \left[\sum_{\tau=-M}^{-2} H_A(X, \tau) + \sum_{\tau=2}^M H_A(X, \tau) \right] \end{cases} \quad (4)$$

式中, $-M \leq \tau \leq M, \tau \neq 0, \tau \neq \pm 1$,

$$\begin{aligned} h[x(j), x(j+\tau)] &= \begin{cases} 0, & x(j) \neq x(j+\tau) \\ 1, & x(j) = x(j+\tau) \end{cases} \\ \chi^2_{2M-3} &= \sum_{\tau=-M}^{-2} \frac{[H_A(X, \tau) - \overline{H_A(X)}]^2}{\overline{H_A(X)}} + \sum_{\tau=2}^M \frac{[H_A(X, \tau) - \overline{H_A(X)}]^2}{\overline{H_A(X)}} \end{aligned} \quad (5)$$

若 χ^2_{2M-3} 的值小于指定显著性水平 (例如 5%) 下的自由度为 $2M-3$ 的 χ^2 理论值, 则 $H_A(X, \tau)$ 以 $\overline{H_A(X)}$ 均匀分布的假设为真, 否则为假。

2.4 非周期汉明互相关

汉明互相关性能主要影响系统的多址组网能力和抗干扰性能。

对于长度为 L (陪测序列长度为 $2M+L$, $M = \frac{t \times n}{2}$)、频隙数为 q 的非宽间隔跳频码序列, 在相对时延 τ 下, 计算非周期汉明互相关 $H_A(X, Y, \tau)$ 和均值 $\overline{H_A(X, Y)}$:

$$\begin{cases} H_A(X, Y, \tau) = \sum_{j=0}^{L-1} h[x(j), y(j+\tau)] \\ \overline{H_A(X, Y)} = \frac{1}{2M+1} \left[\sum_{\tau=-M}^M H_A(X, Y, \tau) \right] \end{cases} \quad (6)$$

式中, $-M \leq \tau \leq M$,

$$h[x(j), y(j + \tau)] = \begin{cases} 0, & x(j) \neq y(j + \tau) \\ 1, & x(j) = y(j + \tau) \end{cases} \circ$$
$$\chi^2_{2M} = \sum_{\tau=-M}^M \frac{[H_A(X, Y, \tau) - \overline{H_A(X, Y)}]^2}{\overline{H_A(X, Y)}} \quad (7)$$

若 χ^2_{2M} 的值小于指定显著性水平(例如 5%)下的自由度为 $2M$ 的 χ^2 理论值, 则 $H_A(X, Y, \tau)$ 以均值 $\overline{H_A(X, Y)}$ 均匀分布的假设为真, 否则为假。

2.5 宽间隔^[5,6]

跳频通信是一种躲避式的抗干扰技术, 电台在同一频点附近停留时间越长, 连续受干扰的概率越大, 系统突发错误增加, 通信性能恶化。因此, 在跳频码序列设计时, 应采用宽间隔设计, 避免频隙滞留。

对于频隙数为 q 的跳频码序列 X , 只要任意两个相邻跳频码 $x(j)$ 和 $x(j + 1)$ 满足:

$$d + 1 \leq |x(j) - x(j + 1)| \leq q - (d + 1)$$

则认为该序列为最小频隙间隔为 d 的狭义宽间隔序列。

2.6 线性复杂度^[7,8]

线性复杂度是序列非线性性能的测度, 是衡量序列线性预测性的一个重要指标。

当频隙数 q 为素数时, 可使用推广的 B-M 算法获得序列的线性复杂度; 而当频隙数 q 为非素数时, 其线性复杂度测试目前通常采用将其展开写成或取位写成二进制表示后, 用二进制序列 B-M 算法进行分析。

二进制序列的 B-M 算法: 长度为 L_2 的独立等概同分布的二进制随机码序列 X , 其线性复杂度的数学期望为

$$E[LC(X)] = \frac{L_2}{2} + \frac{1}{18} [4 + (L_2 \bmod 2)] - 2^{-L_2} \left(\frac{L_2}{3} + \frac{2}{9} \right) \approx \frac{L_2}{2}$$

因此, 只要跳频码序列的二进制表示的线性复杂度数学期望为 $\frac{L_2}{2}$, 则认为该序列具有较好的非线性。

3 对某实用跳频码序列统计测试分析

采用上述理论, 对某实用跳频码序列进行了统计测试, 此序列重复周期为 2^{48} , 频率集 128, 跳频速率为 1 000 hop/s。跳频码发生器在密钥参数控制下, 每输入一个 TOD, 对应输出一个跳频码。

跳频同步最大时差 $t = 30$ s, 起始 TOD 为 2004 年

5 月 12 日 11 时 11 分 50.117 秒, 测试序列长度取 20 480, 取 $M = 30\,000$, 分析 10 个密钥 ($K1, K2, \dots, K10$) 对应输出序列的性能。利用计算机仿真工具, 测试其一维均匀性、相关性能、宽间隔和线性复杂度。

3.1 一维均匀性

表 1 给出了显著值为 5% 条件下一维均匀性 χ^2 测试通过率。

表 1 一维均匀性 χ^2 测试通过率
Table 1 Pass rate of χ^2 test of one dimensional uniformity

密钥序号	通过率/%
K1	97
K2	93
K3	98
K4	93
K5	93
K6	91
K7	96
K8	96
K9	98
K10	96

从表 1 可以看出, 序列一维均匀性 χ^2 测试通过率在 95% 左右, 也就是说序列具有很好的一维均匀性。

3.2 非周期汉明异相自相关

表 2 给出了显著值为 5% 条件下非周期汉明异相自相关性能 χ^2 测试通过率。

表 2 非周期汉明自相关性能 χ^2 测试通过率
Table 2 Pass rate of χ^2 test of nonperiodic Hamming autocorrelation performance

密钥序号	通过率/%
K1	95
K2	85
K3	89
K4	85
K5	83
K6	80
K7	91
K8	92
K9	90
K10	91

从表 2 可以看出, 序列非周期汉明自相关性能不甚理想。但通常实用战术跳频通信系统基于 TOD 实现收发同步, 而不是靠检测自相关峰实现同步; 对 1 000 hop/s 的跳频通信系统, 每跳占用时间为 1 ms,

电波可传播300 km。在视距通信范围内,由序列自相关性能带来的多径干扰对系统影响甚微。

3.3 非周期汉明互相关

表 3 给出了显著值为 5% 条件下非周期汉明互相关性能 χ^2 测试通过率。

表 3 非周期汉明互相关性能 χ^2 测试通过率 Table 3 Pass rate of χ^2 test of nonperiodic Hamming cross – correlation performance									
密钥	通过率/%								
	K2	K3	K4	K5	K6	K7	K8	K9	K10
K1	92	95	94	98	96	97	99	97	96
K2		95	96	97	96	93	97	96	94
K3			94	96	95	95	95	94	98
K4				95	97	99	99	100	94
K5					94	95	96	98	97
K6						97	93	95	97
K7							95	96	96
K8								95	93
K9									98

从表 3 可以看出,序列非周期汉明互相关性能较好,可以满足实际使用中的多址异步组网应用。

3.4 宽间隔

图 1 给出了密钥 K1 控制下的一段跳频码序列相邻跳频码的间隔统计分析。

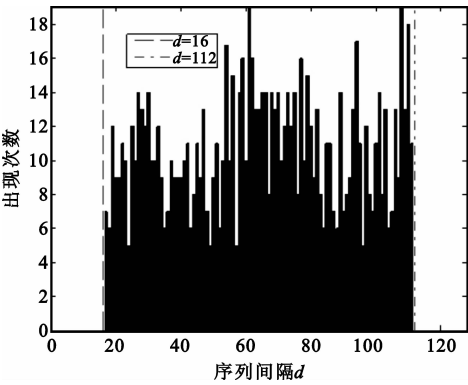


图 1 序列间隔统计图
Fig.1 Statistical chart of sequence interval

从图 1 中可以看出 $17 \leq |x(j) - x(j + 1)| \leq 111$, 相邻跳频码之间的间隔满足狭义宽间隔要求, 且最小跳频间隔为 16。

3.5 线性复杂度

图 2 和图 3 给出了密钥 K1 控制下的一段跳频码序列(测试序列长度为 500, 二进制表示序列长度为 3 500 bit)的线性复杂度曲线。

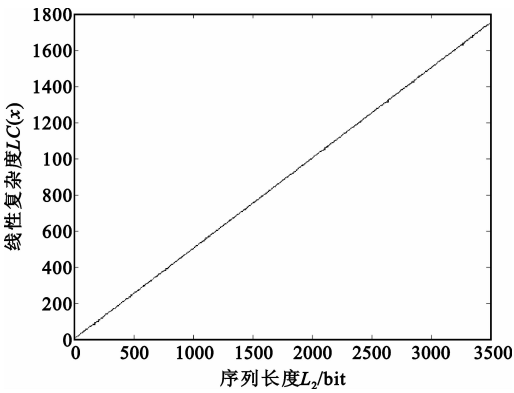


图 2 序列线性复杂度曲线图
Fig.2 The linear complexity of sequence

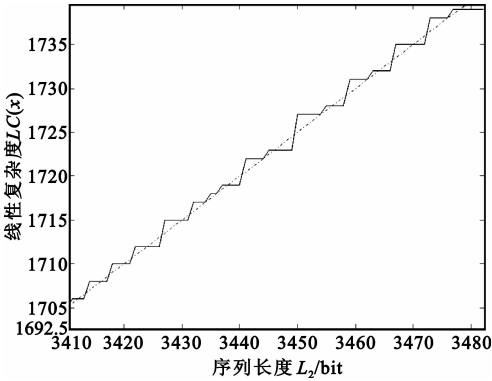


图 3 序列线性复杂度曲线局部放大图
Fig.3 Partial enlargement of Fig.2

我们用这种方法进行了大量的测试,发现结果基本上都类似于图 3 所示。可以看出,被测序列十分相似于理想伪随机码序列的复杂度曲线要求:以平均斜率 $k = \frac{1}{2}$ 增长,图像呈骑跨在 $LC(X) = \frac{L_2}{2}$ 直线的阶梯状,阶梯不太规则。

4 结束语

跳频码序列性能是影响跳频通信系统抗干扰能力的一个重要因素。目前针对周期跳频码序列的性能理论分析不适用于长周期序列,长周期序列性能检测困难。通过对周期序列性能检测方法进行修正,使其更好地反映了跳频码序列的实际使用性能,为长周期跳频序列性能检测提供了一种方法。

参考文献:

[1] 梅文华,杨义先.跳频通信地址编码理论[M].北京:国防工业出版社,1996.
MEI Wen - hua, YANG Yi - xian. The theory of frequency hopping communication address coding[M]. Beijing: National

Defense Industry Press, 1996. (in Chinese)

[2] 梅文华,王淑波,邱永红,等. 跳频通信[M]. 北京:国防工业出版社,2005.

MEI Wen-hua, WANG Shu-bo, QIU Yong-hong, et al. FH Communication[M]. Beijing: National Defense Industry Press, 2005. (in Chinese)

[3] 张申如,王庭昌. 跳频码序列的统计检测[J]. 现代军事通信, 1997, 5(3): 1-7.

ZHANG Shen-ru, WANG Ting-chang. Statistics Detection of FH Code Sequence[J]. Modern Military Communication, 1997, 5(3): 1-7. (in Chinese)

[4] 扈新林,姚富强. 跳频码序列性能检验探讨[J]. 军事通信技术, 1995(2): 14-18.

HU Xin-lin, YAO Fu-qiang. FH Code Sequence Performance Check[J]. Military Communication Technology, 1995 (2): 14-18. (in Chinese)

[5] 甘良才,吴燕翔. 基于混沌的宽间隔跳频序列[J]. 通信学报, 1999, 20(4): 72-76.

GAN Liang-cai, WU Yan-xiang. FH Sequences with Given Minimum Gap Based on Chaos[J]. Journal on Communications, 1999, 20(4): 72-76. (in Chinese)

[6] 何维苗,李剑澄,叶永涛. 一种新的实现宽间隔跳频的方法-随机平移替代法[J]. 现代军事通信, 1999, 7(4): 13-15.

HE Wei-miao, LI Jian-cheng, YE Yong-tao. A Novel Method of Generating FH Sequences with Given Minimum Gap——Method of Random Shifted Replace[J]. Modern Military Communication, 1999, 7(4): 13-15. (in Chinese)

[7] 扈新林,姚富强. 跳频码序列复杂度分析[J]. 通信学报, 1996, 17(5): 21-27.

HU Xin-lin, YAO Fu-qiang. Analysis of the FH Code Sequence Complexity[J]. Journal on Communications, 1996, 17 (5): 21-27. (in Chinese)

[8] Andrew Rukhin, Juan Soto, James N, et al. A Statistical Test Suite For Random And Pseudorandom Number Generators For Cryptographic Applications[M]. Gaithersburg, MD: National Institute of Standards and Technology, 2000.

作者简介:

蔡善法(1963—),男,山东高密人,硕士,高级工程师,主要研究方向为军事通信和扩频通信技术;

CAI Shan-fa was born in Gaomi, Shandong Province, in 1963. He is now a senior engineer with the M. S. degree. His research concerns military communication and spread spectrum communication.

刘刚(1976—),男,湖北黄梅人,博士,高级工程师,主要研究方向为无线通信和扩频通信技术;

LIU Gang was born in Huangmei, Hubei Province, in 1976. He is now a senior engineer with the Ph. D. degree. His research concerns wireless communication and spread spectrum communication.

Email: 361lxj@sina.com

汤宏伟(1976—),男,江苏溧阳人,硕士,工程师,主要研究方向为扩频通信和仿真技术。

TANG Hong-wei was born in Liyang, Jiangsu Province, in 1976. He is now an engineer with the M. S. degree. His research concerns spread spectrum communication and simulation technology.

本刊加入“万方数据-数字化期刊群” 等数据库的声明

为了适应我国信息化建设的需要,扩大作者学术交流渠道,实现科技期刊编辑、出版发行工作的电子化,推进科技信息交流的网络化进程,本刊现已加入“万方数据-数字化期刊群”、“中国学术期刊(光盘版)”、“中国期刊全文数据库”、“中国学术期刊网”、“中文科技期刊数据库”、“中国期刊网”等本刊目次页上著录的数据库,本刊录用发表的论文,将由编辑部统一纳入上述数据库,进入因特网或光盘提供信息服务。本刊所付稿酬已包含著作权使用费和刊物内容上网服务报酬,不再另付。凡有不同意见者,请事先声明,本刊将作适当处理。

《电讯技术》编辑部