文章编号:1673-9469(2015)02-0090-04 doi:10.3969/j.issn.1673-9469.2015.02.022

由m序列构造的同级类m序列及性能研究

方俊初[1],张爱雪[1],吕 虹[2]
(1.安徽工程大学 电气工程学院,安徽 芜湖 2410002;2.安徽建筑大学 电子与信息学院,安徽 合肥 230022)

摘要:根据实践中用状态剪接法获得的一种级数有限的类m序列,用数学手段证明级数为任意数时这种类m序列仍然存在,方法是将m序列移位寄存器的状态和有效反馈位都按奇数位和偶数位分开,分别研究它们对反馈值的影响,从理论上证明了级数为任意整数时,相关的共轭状态都符合类m序列的形成条件。经过分析和测试表明,该类m序列具有良好的伪随机特性。

关键词:m序列;状态剪接;类m序列;奇偶位分类;伪随机性
中图分类号:TN914 **文献标识码**:A

A Kind of Allied m-sequence Obtained by m-sequence And its Performance

FANG Jun-chu[1], ZHANG Ai-xue[1], LV Hong[2]
(1. School of Electrical Engineering, Anhui Polytechnic University, Wuhu 241000 China;
2. School of Electronic and Information Engineering, Anhui Jianzhu University, Hefei 230022, China)

Abstract: In reality, a kind of allied m-sequence with finite series can be obtained by the way of state splicing. On the basis of this, we can prove the existence of this allied m-sequence when the series are any numbers by the way of mathematics: That is to separate the state of m-sequence shift register and the effective feedback bits based on the odd and even numbers, and study their influence on feedbacks respectively. On the basis of theory, we can get a finding that when series are any numbers, relative conjugate states have the condition to form an allied m-sequence. By analysis and tests, allied m-sequence, we get has a perfect pseudo random character.

Key words: m-sequence; rebuilding states; allied m-sequence; odd-even taxis; pseudo random character

m序列用途广泛,子序列是由m序列衍生出的一种序列[1-3]。子序列很多[4-5],对这部分子序列研究的难点在于当级数变化时,交换同样的共轭状态对的后继状态,还能否得到子序列。目前只能根据共轭状态对的特点用不同方法予以证明,文献[3]中指出符合条件的一对共轭状态并用直观的方法予以证明,文献[6]中用"模3取余法"证明了一些符合条件的共轭状态对。本文研究的是实践中发现的另一对符合条件的共轭状态对,根据其状态的构成特点,将移位寄存器的状态和反馈按奇数位和偶数位分开,分别研究它们对反馈值的影响,并选取级数不同的几个子序列,对它们的伪随机特性进行了研究,为它们的应用奠定了基础。

1 一种类m序列(子序列)的实现

经观察,在n变化的过程中,状态1010…101,其共轭状态与0101…010,及其共轭状态在状态图上始终处于交错状态,也就是满足生成子序列的条件,下面从理论上予以证明。

1.1 m序列移位寄存器抽头位置的表示方法

生成m序列的线性移位寄存器如图1所示(下面简称m序列移位寄存器),它是由n位移位

收稿日期:2014-11-10
基金项目:国家自然科学基金项目(61071001,61372094)
作者简介:方俊初(1974-),男,安徽六安人,硕士,研究领域为数字信号处理、电子技术等。

表 1 级数 $n=5$、6 时的反馈位置

Tab. 1 Feedback for stage $n=5$ and $n=6$ register

级数 n	序列长度	抽头位置
5	31	[2,5] [3,5] [1,2,3,5] [1,2,4,5] [1,3,4,5] [1,2,4,5]
6	63	[1,6] [5,6] [1,2,5,6] [1,3,5,6] [2,3,5,6] [1,4,5,6]

寄存器、若干个模 2 加法器组成的线性反馈网络及时钟发生电路构成。模 2 加法器的输入通过系数与移位寄存器的各位状态相联,$c_i=1$ 表示此线接通,该位状态参与反馈运算;$c_i=0$ 则表示该位断开,不参与反馈运算[1]。常将形成 m 序列时参与反馈的抽头位置用一个集合表示 ,如表 1 所示。

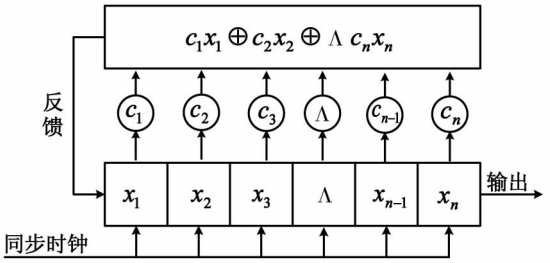

图1 右移型线性移位寄存器的构成

Fig. 1 The structure of right shift register

表中[2,5]即表示对应的本原多项式为 $f(x)=1+x^2+x^5$,也就是图 1 中 $c_2=c_5=1$,$c_1=c_3=c_4=0$。为下面描述方便,将每一个这样的集合统称为 X。

引理 1:m 序列移位寄存器的抽头个数一定为偶数。

根据 m 序列的特点可以用反证法来证明这个结论,若反馈抽头个数为奇数,则当移位寄存器进入全“1”状态即“111……11”时,其反馈信号必然为“1”,其下一个状态仍然是“111……11”,进入死循环,不能产生 m 序列。因而 m 序列移位寄存器的抽头个数一定为偶数,不可能是奇数。

1.2 状态转换过程的证明

定理 1:状态 1010…101,其共轭状态与 0101…010,及其共轭状态在“圈”内必然呈交错状态,具体地说是,级数 n 为奇数时,一对共轭状态 1010…101、1010…100 和另一对共轭状态 0101…010、0101…011 必然成交叉状态;级数 n 为偶数时一对共轭状态 1010…10、1010…11 和另一对共轭状态 0101…01、0101…00 必然形成交叉状态,要证明上面的结论,需要从下面四个方面证明状态的转换过程:

(1)在 $n=2k+1(k=1、2……)$ 的情况下,若 X 中有奇数个奇数位,则必然有这样状态转换过程:1010…100→0101…010→1010…101……

证明:在 $n=2k+1(k=1、2……)$ 的情况下,若 X 中有奇数个奇数,根据引理 1,其中必然有奇数(也可能为零)个偶数。也就是反馈线是由奇数个奇数位和奇数(也可能为零)个偶数位组成的。状态“1010…100”最高位是奇数位且为“0”其余皆为“1”,最高位是必然参与反馈的,则剩下的偶数个奇数位全为“1”,“模 2 加”后结果为“0”,因为偶位全为“0”,不管有几位参与反馈,结果都是“0”,总之,状态“1010…100”对应的反馈是“0”,从而进入下一个状态“0101…010”,此时奇数位皆为“0”,偶数位皆为“1”,其中奇数个偶数位参与反馈得反馈值为“1”,移位寄存器进入下一状态“1010…101”。

(2)在 $n=2k+1(k=1、2……)$ 的情况下,若 X 中有偶数个奇数位,则必然有这样的状态转换过程:0101…011→1010…101→0101…010……

证明:在 $n=2k+1(k=1、2……)$ 的情况下,若 X 中有偶数个奇数位,则必然有偶数个偶数位,状态“0101…011”的偶数位皆为“1”,参与反馈的偶数个偶数位“模 2 加”后结果为“0”,奇数位中最高位“1”必然参与反馈而其它奇数位全为“0”,即可得状态“0101…011”对应的反馈值为“1”,进入下一状态“1010…101”,此时偶数位全为“0”,“模 2 加”后结果为“0”,奇数位全为“1”,其中的偶数个参与反馈(必然包括最高位),决定了反馈值为“0”,进入下状态“0101…010”。

(3)在 $n=2k(k=1、2……)$ 的情况下,若 X 中有奇数个偶数位,则必然有这样状态转换过程:1010…11→0101…01→1010…10……

证明:在 $n=2k(k=1、2……)$ 的情况下,若 X 中有奇数个偶数位,也必然有奇数(也可能为零)个奇数位。状态“1010…11”中奇数位全为“1”,即奇数位的反馈值为“1”,偶数位中只最高位是“1”,其他均为“0”,注意到最高位必然参与反馈,因而偶数位的反馈值也为“1”,这样,状态“1010…11”对应的反馈值就是“0”,移位寄存器进入下一状态“0101…01”,这时的奇数位全为“0”,偶数位全为“1”,其中奇数个偶数位参与反馈决定了反馈

值为“1”,移位寄存器进入下状态“1010…10”。

(4)在 $n=2k(k=1、2\cdots\cdots)$ 的情况下,若 X 中有偶数个偶数位,则必然有这样状态转换过程:0101…00→1010…10→0101…01……

证明:在 $n=2k(k=1、2\cdots\cdots)$ 的情况下,若 X 中有偶数个偶数位,也必然有偶数(也可能为零)个奇数位。状态“0101…00”中奇数位全为“0”,即奇数位的反馈值为“0”,偶数位中除最高位外全为“1”,最高位必然参与反馈,这样偶数个偶数位形成的反馈值为“1”,因而状态“0101…00”所对应的反馈就是“1”,移位寄存器进入下一状态“1010…10”,此时,偶数位全为“0”,即偶数个偶数位形成的反馈分量是“0”,而奇数位全为“1”,其中的偶数个奇数位参与反馈,形成的反馈分量是“0”,因而状态“1010…10”对应的反馈值是“0”,进入下一状态“0101…01”。

1.3 反馈函数的提取及生成的非线性序列

这类子序列的优点是级数不同时,其反馈函数有统一的实现方法。

实现子序列,就要改变原有 m 序列移位寄存器的反馈函数,方法是在原有 $f(x)$ 基础上附加一个函数 $g(x)$,形成新的反馈函数 $f'(x)$,形式如下

$$f'(x)=f(x)\oplus g(x) \tag{1}$$

其中 $g(x)$ 只有在指定的共轭状态时取值“1”,否则为“0”,从而改变了 $f(x)$ 在此状态处对应的反馈值,也就改变了状态转移顺序。

例如,阶数 $n=6$ 时,取原本多项式 $1+x+x^6$,即反馈函数是 $f(x)=x_1\oplus x_6$,得到的 m 序列为:

000001111110101011001101110110100100111000101111001010001100001 (2)

子序列的反馈函数是 $f'(x)=f(x)\oplus x_1\bar{x}_2x_3\bar{x}_4x_5\oplus\bar{x}_1x_2\bar{x}_3x_4\bar{x}_5$,得到的新的序列(子序列)为:

000001111110101100110111011010010011100010111100101010001100001 (3)

2 子序列与原序列的特性比较

2.1 周期性及结构特点

子序列是在 m 序列移位寄存器的基础上,只改变某些状态的转换顺序,没有增加和减少原有状态,所以子序列和原 m 序列具有相同的码元结构。例如上述序列原序列(2)和子序列(3),具有相同的周期 63 ,其中“1”的个数都为 32,“0”的个数都为 31。

2.2 游程特性

将序列(2)和序列(3)按游程分段,结果如下:

00000 111111 0 1 0 1 0 11 00 11 0 111 0 11 0 1 00 1 00 111 000 1 0 1111 00 1 0 1 000 11 0000 1 00000 111111 0 1 0 11 00 11 0 111 0 11 0 1 00 1 00 111 000 1 0 1111 00 1 0 1 0 1 000 11 0000 1

它们的游程分布情况见表 2 。

从表中可见,子序列和原序列具有相同的游程结构,即 n 阶 m 序列一个周期中共有游程 2^{n-1} 个,其中长度为 1 的游程占 $\frac{1}{2}$,长度为 2 的占 $\frac{1}{4}$,长度为 3 的占 $\frac{1}{8}$……,长度为 n 及 $n-1$ 的游程特殊,都只有一个[7-8]。

2.3 自相关特性

对于一周期为 p 的二元序列,其自相关特性定义为:

$$C_a(t)=\sum_{k=0}^{p-1}\eta(a_k)\eta(a_{k+t})/p \tag{4}$$

其中 $\eta(^*)$ 表示映射

$$\begin{cases}\eta(0)=1\\ \eta(1)=-1\end{cases} \tag{5}$$

Matlab 环境下,对 m 序列和其子序列的自相关特性进行测试。

表 2 游程分布情况统计

Tab. 2 Statistic for the run length

游程长度		1	2	3	4	5	6
序列(2)	个数	16	8	4	2	1	1
	分布	8 个“0” 8 个“1”	4 个“00” 4 个“11”	2 个“000” 2 个“111”	1 个“0000” 1 个“1111”	1 个“00000”	1 个“111111”
序列(3)	个数	16	8	4	2	1	1
	分布	8 个“0” 8 个“1”	4 个“00” 4 个“11”	2 个“000” 2 个“111”	1 个“0000” 1 个“1111”	1 个“00000”	1 个“111111”

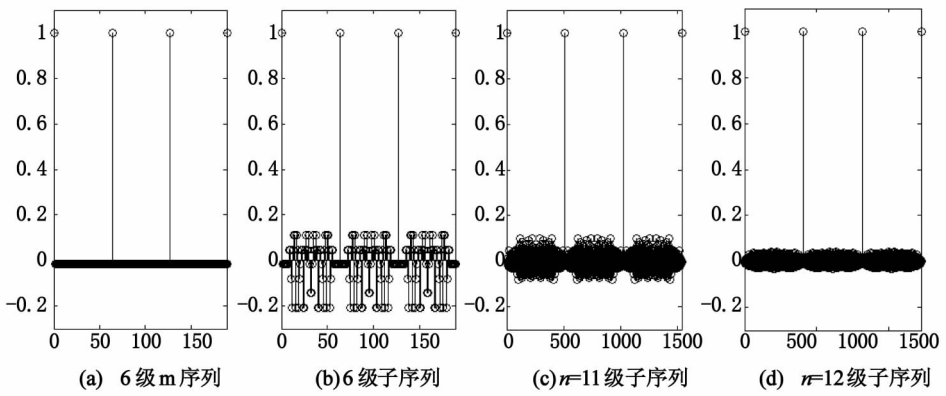

图2 m序列和子序列自相关特性对比

Fig. 2 Autocorrelation comparison for m sequence and its sub-sequence

由图 2 可见,(1)m 序列是线性序列,其自相关特性具有典型的二值特性。子序列是非线性序列,其自相关特性不同于 m 序列,呈现多值特性;(2)子序列也具有非常尖锐的自相关特性,图中可见其主峰值为 1,副峰值随阶数 n 增大而明显减小;(3)进一步实验表明,当级数增大一定程度时,子序列的自相关特性十分接近于 m 序列的自相关特性[9]。

3 总结

基于本文给出的这一共轭状态对一定能获得相应的子序列,特性测试表明,这一类子序列是良好的伪随机序列。不足之处在于对子序列的自相关特性尚不能给出准确的数学表达式,只能通过测试的方法得出其趋势。

参考文献:

[1]肖国镇,梁传甲,王育民. 伪随机序列及其应用[M]. 北京:国防工业出版社,1985.

[2]尹晓琪. 伪随机序列及其在通信加密中的应用[J]. 现代电子技术, 2005(19):42 - 44.

[3]吕 虹,段颖妮,管必聪,等. 第一类 m 子序列的构造[J]. 电子学报,2007,35(10):2029 - 2032.

[4]方俊初,吕 虹,张爱雪. 产生 m 子序列的一种实用算法[J]. 河北工程大学学报:自然科学版,2012,29(4):79 - 83.

[5]方俊初,吕 虹. 由 m 序列生成非线性序列的 C 语言实现[J]. 河南科技大学学报:自然科学版,2013,34(6):47 - 50.

[6]吕 虹,张爱雪,方俊初,等. 基于母函数的非线性反馈函数及其子序列研究[J]. 电子学报,2012,40(10):2128 - 2132.

[7]GAO ZHIHAN,FU FANGWEI. The minimal polynomial of a sequence obtained from the componentwise linear transformation of a linear recurring sequence[J]. Theoretical Computer Science,2010(411):3883 - 3893.

[8] LVHONG. Design and Implementation of A Maximal Length Nonlinear Pseudorandom Sequence [C]//Proceedings of the 2009 International Conference on Computer and Commun - ications Security. 2009:64 - 67.

[9]GUANG GONG. Cryptographic properties of the welch - gong trans - formation sequence generators[J]. IEEE Transactionson Information Theory, 2002, 48(11):2837 - 2846.

(责任编辑　王利君)