文章编号:1673-9469(2015)01-0096-03 doi:10.3969/j.issn.1673-9469.2015.01.025

m子序列的特性研究

张爱雪,年夫生,韩 春
(安徽工程大学 电气工程学院 安徽省电气传动与控制重点实验室,安徽 芜湖 241000)

摘要: 针对m序列线性复杂度不高,非线性度为零等问题,采用B-M算法对构造出的第一类m子序列进行了线性复杂度的研究,得出m子序列的线性复杂度和m序列相比大的多,逼近序列长度的一半的结论。利用Walsh频谱技术分析了m子序列的非线性度,仿真和计算结果表明m子序列的非线性度与m序列相比有了很大的改善,可以广泛用于流密码、信道编码、扩频通信等领域。

关键词: m子序列;线性复杂度;B-M算法;Walsh谱;非线性度
中图分类号: TN919 **文献标识码:** A

Study on the characteristics of m Subsequence

ZHANG Ai-xue, NIAN Fu-sheng, HAN Chun
(Anhui Provincial Key Laboratory of Electric and Control, School of Electrical Engineering, Anhui Polytechnic University, Anhui Wuhu 241000, China)

Abstract: M sequence has good pseudo-random characteristics, but its linear complexity is not high and the nonlinearity is zero. So the application fields of m sequence are limited. Adopting the B-M algorithm this paper gives the studies of the linear complexity of m subsequences which are constructed. We get conclusion that the linear complexity of m sequence is bigger than m subsequences', approaching the half of the sequence's length. The nonlinearity of the m subsequence is analyzed using the Walsh spectrum technology. The simulation and the calculation results show that the nonlinearity of m subsequence has made a lot of improvement compared with the m sequence, and can be widely used in flow password, channel coding, spread spectrum communication, etc.

Key words: m subsequence; the linear complexity; B-M algorithm; Walsh spectrum; nonlinearity

基于线性移位寄存器(LFSR)构造产生的伪随机m序列是成熟的理论,m序列具有周期性、游程性、平衡性和相关性良好的伪随机性。但m序列的数目有限,线性复杂度低,非线性度为零,往往不能满足实际应用的需要。近年来,研究出更具有科学和社会价值的伪随机m序列是国内外相关领域的热点问题。本文主要讨论基于m序列构造出的第一类m子序列的线性复杂度和非线性度,从而证明第一类m子序列具有很好的线性复杂度和良好的非线性度。

1 m序列和m子序列

1.1 m序列及其特性

假设以F_2上n次多项式$f(x)=c_0+c_1x+\cdots+c_nx^n$为联接多项式的$n$级线性移位寄存器所产生的非零序列a的周期为$2^n-1$,便称序列$a$是$n$级最大周期线性移位寄存器序列,简称m序列。

m序列具有良好的平衡性、游程特性,它的自相关函数具有很好的$\delta(t)$函数特征,所以,m序列具有很好的伪随机特性。

1.2 m子序列

第一类m子序列是在m序列线性反馈函数所确定状态转移图上,修改一定的状态后继,将会在保留原状态转移图主构架基础上,形成一个新的状态转移图,这个新的状态转移图对应一个新的移位寄存器,这个新的移位寄存器所产生的序列就是m子序列,其总的状态数目也是2^{n-1}。

收稿日期:2014-09-20
基金项目:安徽工程大学国家级大学生创新创业训练计划(201210363157)
作者简介:张爱雪(1977-),女,山东郓城人,讲师,主要从事信息信号处理和嵌入式系统的研究。

m 序列移位寄存器反馈函数式如式(1),若改变状态转换,其反馈函数也随之改变。

$$f(x) = c_0x_0 \oplus c_1x_1 \oplus c_2x_2 \oplus \cdots \oplus c_{n-1}x_{n-1} \quad (1)$$

根据参考文献[1],m 序列反馈函数在四点处完成模 2 加 1 就能形成 m 子序列。所以 m 子序列的反馈函数 $f'(x)$ 的形式如下:

$$f'(x) = f(x) \oplus x_{n-1}\overline{x_{n-2}}\cdots\overline{x_1}\ \overline{x_0} \oplus x_{n-1}\overline{x_{n-2}}\cdots \overline{x_1}\ \overline{x_0} \oplus \overline{x_{n-1}}\overline{x_{n-2}}\cdots x_1x_0 \oplus \overline{x_{n-1}}\overline{x_{n-2}}\cdots x_1x_0 \quad (2)$$

m 子序列移位寄存器是基于 m 序列移位寄存器,且进行了一定的状态重组,其循环状态也是 2^{n-1} 个非零状态,所以 m 子序列的平衡性、游程特性和自相关特性都很好。

2 m 子序列的线性复杂度

线性复杂度及其稳定性的研究是评价序列不可预测性的重要指标,序列的线性复杂度不仅要足够大,而且必须有很好的稳定性。由线性复杂度的定义可知[2]:对于非线性序列,其等效线性移位寄存器的长度为该序列的线性复杂度,在已知 N 长二元序列 $a_0, a_1, a_2, \cdots, a_{N-1}$ 的情形下,求取这样一个等效线性移位寄存器的长度,采用 Berreka-mp-Messey 算法来完成。该算法的核心思想是运用数学归纳法求出一系列线性移位寄存器。

对于一个 $GF(2)$ 上的多项式:

$$f(x) = c_0 + c_1x + c_2x^2 + \cdots + c_1x^l \quad (3)$$

其中 $c_0 = 1$,但并不限定 $c_1 = 1$。我们把以 $f(x)$ 为联接多项式的 l 级线性移位寄存器简记为 $<f(x), l>$。如果递归关系:

$$a_k = c_1a_{k-1} + c_2a_{k-2} + \cdots + c_la_{k-1},$$
$$k = l, l+1, \cdots, N-1 \quad (4)$$

成立。我们就说 $<f(x), l>$ 产生二元序列 $a_0, a_1, a_2, \cdots, a_{N-1}$。B-M 算法的流程图如图 1 所示:

根据线性复杂度定义,设 $a = a_0a_1a_2\cdots a_{1-1}$ 是一 n 级 m 序列,则 n 级 m 序列线性复杂度是 n。同一周期($p = 2^n - 1$)的 m 子序列的线性复杂度较 m 序列的线性复杂度大的多,应用 B-M 算法可以计算出第一类 m 子序列的线性复杂度。对最高次数 n 取 7 ~ 10 的各 m 序列本原多项式(文献[2]中的附表三)所确定的式(1-2)的 m 子序列进行了线性复杂度的统计,部分结果如表 1 所示。

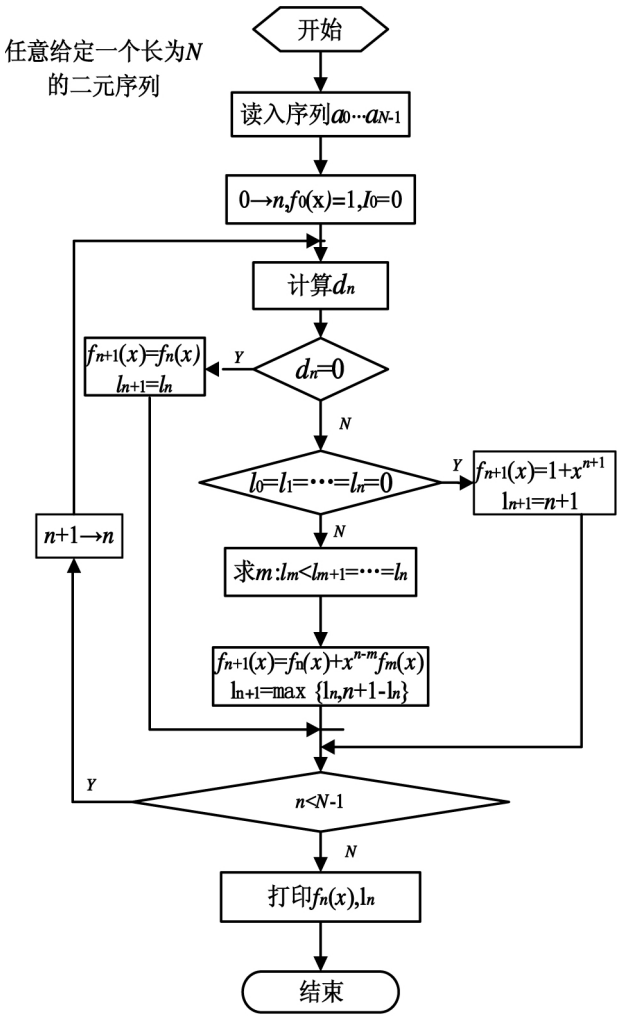

图1 B-M流程图

Fig. 1 B-M flow chart

由表 1 可知: m 子序列的线性复杂度比 m 序列的线性复杂度大的多,逼近于序列周期的一半,正好符合文献[3]中对于密钥序列的要求。

表 1 具有同一周期的 m 序列和 m 子序列线性复杂度

Tab. 1 The linear complexity of m sequence and m subsequence which have the same period length

序列 / 周期	m 序列	m 子序列 1	m 子序列 2	m 子序列 3	m 子序列 4
$2^7 - 1 = 127$	7	62	54	59	63
$2^8 - 1 = 255$	8	146	128	127	120
$2^9 - 1 = 511$	9	298	254	256	256
$2^{10} - 1 = 1\,023$	10	615	512	512	512

3 m 子序列的非线性度

为了抵抗各种攻击,流密码和分组密码算法中所用的 m 序列必须满足一些密码学准则,比如具有相关免疫性,有高的非线性度。我们知道,m 序列是由线性移位寄存器产生的,LFSR 的反馈函数是线性函数,它的非线性度为零,所以 m 序列抵抗线性攻击的能力不强。接下来我们分析 m 子序列的非线性度。

布尔函数 $f(x)$ 的 Walsh 变换,也称 Walsh 谱,是研究布尔函数非线性度的有力工具。

设 $f(x)$ 是 F_2^n 上的布尔函数,称

$$W_f(\omega) = \sum_{x\in F_2^n} (-1)^{f(x)} (-1)^{\omega\cdot x} = \sum_{x\in F_2^n} (-1)^{f(x)+\omega x} \quad (5)$$

为 $f(x)$ 在 ω 处的 Walsh 谱,其中 $\omega\cdot x$ 代表 ω 与 x 的内积,即:

$$\omega\cdot x = \omega_1 x_1 + \omega_2 x_2 + \cdots + \omega_n x_n \quad (6)$$

这里 $\omega = (\omega_1, \omega_2, \cdots \omega_n) \in F_2^n$,所有的 $W_f(\omega)$ 称为 $f(x)$ 的 Walsh 谱。

设 $f(x)$ 是 F_2^n 上的布尔函数,$f(x)$ 的非线性度 (Nonlinearity),记为 N_f,等于它与所有线性函数的汉明距离的最小值,即:

$$N_f = \min_{l\in L(n)} d(f,l) = \min_{l\in L(n)} \omega t(f+l) \quad (7)$$

布尔函数的非线性度与 Walsh 谱之间存在如下的关系:

$$N_f = 2^{n-1} - \frac{1}{2}\max_{\omega\in F_2^n} |W_f(\omega)| \quad (8)$$

因此要求出一个布尔函数的非线性度,只要求出其绝对值最大的 Walsh 谱值即可。

根据参考文献 [1] 在 m 序列状态转移图的基础上修改一定的状态后继得到 m 子序列的反馈函数 $f'(x)$,根据公式(5)和(8)可以计算出反馈函数 $f'(x)$ 产生的 m 子序列的 Walsh 谱值和非线性度的值。图 2 是 9 位的 m 序列交换不同对数的共轭状态得到的不同的 m 子序列的非线性度 N_f 的值。

m 序列是线性序列,通过计算可知任何 m 序列的非线性度都是零。m 子序列是非线性序列,m 子序列的 $|W_f(\omega)|$ 的最大值比 m 序列的要小一些,而且 m 子序列的 $W_f(\omega)$ 的非零值的个数要多一些。根据图 2 可知,相同位数的不同 m 子序列,交换序列共轭状态的对数越多,得到的 m 子序列的非线性度越大。因此 m 子序列和 m 序列相比,非线性度有了很大的提高,m 子序列用来抵抗相关攻击的能力要强的多。

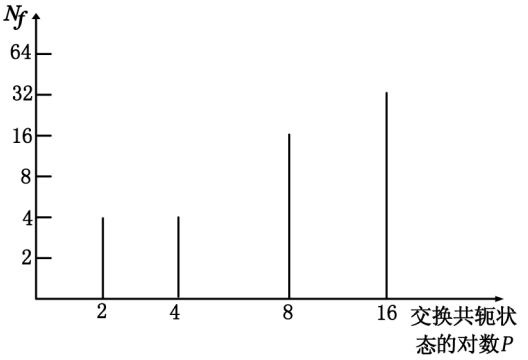

图2 交换不同共轭状态的对数得到的非线性度

Fig. 2 The nonlinearity of exchanging different conjugate states' logarithmic

4 结论

m 子序列和 m 序列一样具有周期长、游程性、平衡性和良好的相关性,研究结果表明 m 子序列的线性复杂度比 m 序列的线性复杂度大的多,其非线性度和 m 序列相比也有了很大的提高,因此 m 子序列是好序列,可以广泛用于密码序列系统中。

参考文献:

[1] 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.

[2] 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.

[3] 杨义先, 林须端. 编译密码学 [M]. 北京: 人民邮电出版社, 1992.

[4] CUANG LONG. Crypftographic properties of the welch - gong transformation sequence generators [J]. IEEE Transactions on Inforrnation Theory, 2002, 48(11): 2837 - 2846.

[5] NO J S, CHUNG H, YUN M S. Binary pseudorandom sequences of period 2n - 1 with ideal auto correlalation [J]. IEEE Trans IT, 1998, 44(2): 814 - 817.

[6] 程郁凡,洪福明. 跳频码序列复杂度与随机性分析 [J]. 电子科技大学学报,1996,25(9):351 - 357.

[7] 武传坤. 布尔函数非线性度的谱分析 [J] . 电子科学学刊,1996,18(5):487 - 494.

[8] 胡 斌,金晨辉,邵增玉. 密码学中 3 类具有特殊 Walsh 谱值布尔函数的关系 [J]. 通信学报,2010, 31(7): 104 - 109.

[9] 朱华安,谢端强. 基于 m 序列统计特性的序列密码攻击 [J] . 通信技术, 2003, 8(140):96 - 98.

(责任编辑 王利君)