第一类 m 子序列的构造

吕 虹, 段颖妮, 管必聪, 刘雨兰
(安徽工程科技学院电气工程系, 安徽芜湖 241000)

摘 要: 伪随机序列在流密码、信道编码、扩频通信等领域有着广泛的应用, m 序列是优秀的伪随机序列. 基于 m 序列, 本文首次提出通过重构 m 序列移位寄存器状态图, 构造一类称之为 m 子序列的移位寄存器状态图. 根据重构的状态图, 提出了第一类 m 子序列并予以证明. 本文推导了第一类 m 子序列移位寄存器反馈函数式, 分析了第一类 m 子序列具有良好的周期特性、游程特性、平衡特性以及较高的线性复杂度. 仿真结果表明, m 子序列自相关特性也具有很好的 $\delta(t)$ 函数特征. 利用文中给出的构造方法, 可以构造更多性能优良的 m 子序列.

关键词: m 子序列; 移位寄存器; 重构状态图; 伪随机特性; 反馈函数
中图分类号: TN919; TN431 文献标识码: A 文章编号: 0372-2112 (2007) 10-2029-04

Construction of First Class of m Subsequences

LV Hong, DUAN Ying-ni, GUAN Bi-cong, LIU Yu-lan
(*Anhui University of Technology and Science, Wuhu, Anhui* 241000, *China*)

Abstract: Pseudorandom sequence have been widly used in stream cipher, channel coding, and spread spectrum communication. m sequence is a excellent pseudorandom sequence. Based on m sequence, we first present reconstructing it's state transition diagram and gained the state transition diagram of the new sequence called m subsequence in this paper. We prove that the first class m subsequences is existent, and present first class of m subsequences feedback functions. In the end we analyze m subsequences properties and affirm that possess with ideal balanced property、run property、periodic property and good linear complexity. Statistic results show that m subsequences autocorrelation property have $\delta(t)$ function characteristic. More new m subsequence can be obtained by using this constructing method.

Key words: m subsequence; shift register; reconstructing state transition diagram; pseudorandom property; feedback function

1 引言

GF(2) 上的伪随机序列具有极为广泛的应用, 比如测量、流密码、信道编码、扩频通信等等. m 序列是 GF(2) 上最具代表性的伪随机序列, 其平衡性、游程性、相关性都很好, 具有很好的伪随机特性. 但是, m 序列的数目有限, 线性复杂度低, 在实际应用中, 往往难以满足要求. 本文基于 m 序列, 构造了一种称之为第一类 m 子序列的序列, 它的周期长度仍然为 2^n-1, 且既保留了 m 序列的优秀伪随机特性, 又具有较高的线性复杂度, 是难得的好序列.

2 m 序列

n 级移位寄存器可以产生多种 m 序列, 每一种 m 序列都对应着一个确定的线性反馈逻辑函数式, 其形式如下:

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

其中, $c_i\in GF(2)$, 称之为反馈系数, $x_i\in GF(2)$, 为各位寄存器状态.

n 级移位寄存器共有 2^n 个状态, 且最低位取 0 或 1 的状态数相等, 各为 2^{n-1} 个, 而 n 级 m 序列移位寄存器是在非零的 2^n-1 状态中循环, 且输出每个状态的最低位, 形成 m 序列. 故 m 序列中的 0 数目比 1 数目只少 1, 具有良好的平衡性.

m 序列具有良好的平衡性、游程特性[1], 它的自相关函数具有很好的 $\delta(t)$ 函数特征, 所以, m 序列伪随机性能好.

3 m 子序列

3.1 m 序列移位寄存器状态图

m 序列移位寄存器状态转换由其反馈函数确定, 形如图 1 所示. 由图 1 知, 电路状态的转换由 $s_0\rightarrow s_1\rightarrow\cdots s_j\rightarrow\cdots s_i\rightarrow\cdots s_p\rightarrow\cdots s_{2^n-2}\rightarrow s_0$, 电路完成一个大循环, 产生一个周期 m 序列.

收稿日期: 2006-05-18; 修回日期: 2007-08-06
基金项目: 安徽省自然科学基金(No. 050420203); 安徽省教育厅自然科学基金(No. KJ2004064)

3.2 m 子序列移位寄存器状态图

m 序列移位寄存器 2^n-1 个状态的转换具有移位转换特点, 若修改图 1 中若干状态的转换, 就改变了整个状态的转换, 生成的序列也就随之改变.

如何修改图 1 的状态转换, 才能形成一个新的、长度仍然为 2^n-1 的大循环? 为此先作如下定义.

电路当前状态称之为电路的现状态, 其前一状态称之为该状态的原状态, 其后一状态称之为该状态的次状态; 两个仅最低位相异余者相同的状态称之为关于低位逻辑相邻状态, 记为 S_i、S_i' ; 两个仅最高位相异余者相同的状态称之为关于高位逻辑相邻状态, 记为 S_i、' S_i. 对于图 1, 若要修改 S_i 状态的转换, 就意味着要改变其次状态. 对于移位寄存器来说, 一对低位逻辑相邻状态的次状态, 一定是一对高位逻辑相邻状态. 所以, 修改图 1 中 S_i 状态的转换, 并且能够再次形成一个长度仍然为 2^n-1 的大循环, 就应该交换状态 S_i、S_i' 的次状态.

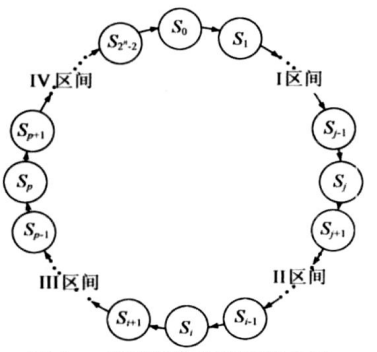

图 1 m序列移位寄存器状态图

设图 1 中 S_0、S_i 是一对低位逻辑相邻状态, 若交换次状态, 由图 1 知, S_0 到达 S_{i+1} 之后, 电路状态转换进入图 1 左边状态转换区, 如果在这个区间没有其它状态转换改变, 那么由 S_{i+1} 最终到达最后一个状态 S_{2^n-2}, 再回到 S_0, 形成了如图 2 左半部所示的状态转换图. 图 2 右半部所示的状态转换图情况相同, 显然, 整个状态图循环长度对折了, 丢失了很多有效状态, 没有形成一个长度为 2^n-1 的大循环, 不是所希望的.

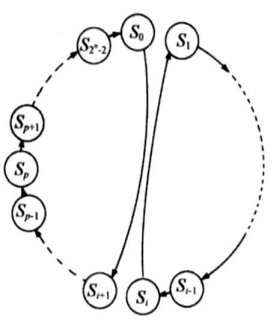

图 2 改变图 1 一对状态转换形成的状态图

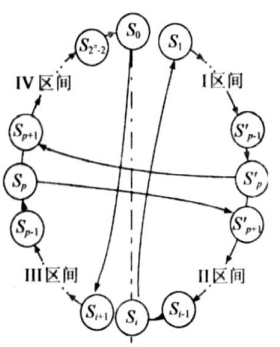

图 3 m子序列移位寄存器状态图

电路在进入状态 S_{i+1} 之后的转换过程中, 如果存在一状态, 设为 S_p, 其低位逻辑相邻状态 S_p' 又恰好落在图 1 的右半部状态转换区之间, 如图 3 所示, 那么, 交换 S_p 和 S_p' 状态的次状态, 电路将由 S_p 状态到达 S_{p+1}' 状态, 进入图 3 的右边状态转换区间转换. 当电路由 S_{p+1}' 状态转换到达 S_i 状态时, 由于 S_i 与 S_0 是两低位逻辑相邻状态, 且已交换了次状态, 所以, 由 S_i 状态将到达 S_1, 进入图 3 的Ⅰ状态转换区间. 完成Ⅰ区间的状态转换, 电路到达 S_p' 状态, 由于 S_p' 与 S_p 是两个低位逻辑相邻状态, 也已交换了次状态, 所以, 由 S_p' 状态将到达 S_{p+1}, 接着电路在Ⅳ区间转换状态, 到达 S_{2^n-2} 状态, 再回到 S_0, 最后完成了 $S_0 \rightarrow S_{i+1} \rightarrow$ Ⅲ区间 $\rightarrow S_p \rightarrow S_{p+1}' \rightarrow$ Ⅱ区间 $\rightarrow S_i \rightarrow S_1 \rightarrow$ Ⅰ区间 $\rightarrow S_p' \rightarrow S_{p+1} \rightarrow$ Ⅳ区间 $\rightarrow S_{2^n-2} \rightarrow S_0$ 一个大循环, 如图 3 所示.

3.3 第一类 m 子序列移位寄存器状态图的构造

由上述分析知, 只要交换 m 序列移位寄存器的两对特定低位逻辑相邻状态的次状态, 就能形成 m 子序列移位寄存器状态图(本文中所指移位均以右移位为例).

如何确定低位逻辑相邻的两对特定状态? 由于这两对特定状态间存在一定的约束, 所以, 先要确定第一对状态. 在 m 序列状态图中, 设 10……00 为初状态 S_0, 不妨以初状态 10……00 和其低位逻辑相邻状态 10……01 为第一对状态, 那么, 第二对状态中的两个状态就应分别处于以第一对状态的连线为轴线的 m 序列状态图两侧, 见图 3. 只有这样的两对状态, 两两交换次状态后, 对应的 m 序列状态图才能转变成 m 子序列状态图.

定理: 在所有 m 序列移位寄存器中, 低位逻辑相邻状态 0000……010、0000……011, 一定处在以第一对低位逻辑相邻状态 10……00、10……01 为轴线的 m 序列状态图的两侧. 证明如下:

1. 设 m 序列移位寄存器初态 S_0 为 10……00, 则其末状态 S_{2^n-2} 一定是 00……01, 初态 S_0 的低位逻辑相邻状态 S_i 一定是 10……01, 且称其为 S_0', 按照图 3, S_0、S_i 交换次态, 电路进入左边 III区间转换.

2. 设图 3 左边的 S_p 状态为 m 序列移位寄存器末状态 00……01 的原状态, 则其对应的 m 序列移位寄存器状态图如图 4 所示. 这样, S_p 状态一定是第二对低位逻辑相邻状态 00……010、00……011 中之一状态, 所以在图 4 左边至少存在第二对高位逻辑相邻状态 00……010、00……011 中之一. 那么, 这两个状态是否可能同时处于图 4 左边区域?

若图 4 左边区间同时存在这两个状态(S_p、S_p'), 按照上述假设, 电路首先到达的应该是 S_p' 状态, 其次态也一定在左边区间且和 S_p 次态(电路末状态) 00……01 构成高位逻辑相邻状态对(00……01、10……01), 但是, 这与 S_i 为 10……01 相矛盾, 显然图 4 左边区间不可能同时存在这两个状态, 所以图 4 左边区间只存在一个且为电路末状态 00……01 的原状态 S_p.

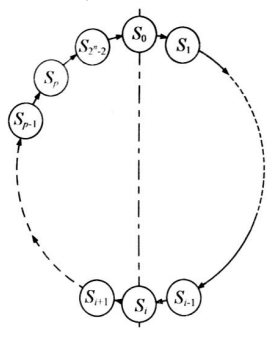

图 4　m序列状态图

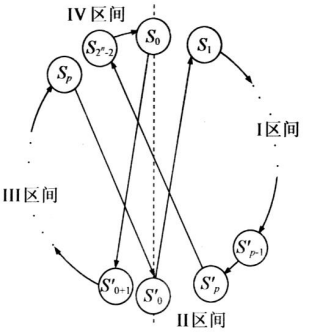

图 5　第一类 m 子序列移位寄存器状态图

3. 第二对低位相邻状态对 00 ……010、00 …… 011 中的另一状态 S'_p 不在状态图4 左边, 也不是 S_0 或 $S_i(S'_0)$, 那么, 一定存在于状态图 4 右边, 如图 5 所示. 所以, 交换 S_p、S'_p 各自的次状态, 电路由 S_p 进入状态图右边, 经过转换再到达 S_i(10 ……01) 状态, 即 S'_0 状态, 由 S_i 将转换到S_1, 电路又进入Ⅰ 区间转换, 完成Ⅰ 区间转换, 再到达 S'_p , 电路由 S'_p 进入末状态 00 ……01, 由 00 …… 01→10 ……00, 形成了一个大循环, 状态图如图 5. 由上状态图分析知: 不管是何种 m 序列移位寄存器, 只要改变这两对低位逻辑相邻状态转换规律, 交换两两次状态, 一定能形成一个长度仍然为 2^n-1 的非线性大循环, 产生m 子序列.

定义: m 序列中凡是改变这两对状态的转换而形成的长度为2^n-1 的非线性序列称为第一类 m 子序列, 其 m 序列是对应子序列的母序列.

3.4　第一类 m 子序列移位寄存器反馈函数的构成

m 序列移位寄存器反馈函数如式(1) , 若改变状态转换, 其反馈函数也随之改变. 图 1 是 m 序列移位寄存器的状态图, 若交换两对低位逻辑相邻状态对 10 …… 00、10 ……01 和 00 ……010、00 …… 011 次状态, 电路状态图如图 5 所示. 显然, 相对于 m 序列移位寄存器, 第一类 m 子序列移位寄存器的状态只在四处发生改变, 其它不变, 所以, 只需在这四点处改变 m 序列反馈函数值, 即可获得第一类 m 子序列反馈函数. 改变这四点处的反馈函数值, 就意味着在这四点处将原 m 序列反馈函数值求反, 即进行加 1(模 2) .

第一类 m 序列反馈函数仅在四点处再完成模 2 加 1, 就能形成 m 子序列, 而其它不变, 不变也就是模 2 加 0, 所以第一类 m 子序列移位寄存器反馈函数$f'(x)$由 m 序列反馈函数$f(x)$与另一函数再作一次模 2 加构成, 形如下式:

$$f'(x)=f(x)\oplus y(x) \qquad (2)$$

称$y(x)$是第一类 m 子序列个性函数, 它只在两对低位逻辑相邻状态处取值为 1, 余者为 0. 显然, 这四处的小项之和构成了 $y(x)$ 函数, 在这里:

$$\begin{aligned} y(x) &= x_{n-1}\bar{x}_{n-2}\cdots\bar{x}_1\bar{x}_0+x_{n-1}\bar{x}_{n-2}\cdots\bar{x}_1x_0+\bar{x}_{n-1}\bar{x}_{n-2}\\ &\quad \cdots x_1\bar{x}_0+\bar{x}_{n-1}\bar{x}_{n-2}\cdots x_1x_0\\ &= x_{n-1}\bar{x}_{n-2}\bar{x}_{n-3}\cdots\bar{x}_1+\bar{x}_{n-1}\bar{x}_{n-2}\bar{x}_{n-3}\cdots x_1\\ &= \bar{x}_{n-2}\bar{x}_{n-3}\cdots\bar{x}_2\bullet(x_{n-1}\oplus x_1) \end{aligned}$$

4　m 子序列性能分析

第一类 m 子序列移位寄存器是基于 m 序列移位寄存器, 且进行了一定状态重组, 其循环状态也是 2^n-1 个非零状态, 所以第一类 m 子序列 $\tilde{a}$ 的平衡性、游程性同 m 序列, 同时, 它具有非线性反馈函数, 所以, 其线性复杂度较 m 序列高.

现考查第一类 m 子序列自相关特性. 在讨论自相关函数时, 习惯上, 总是把 0、1 序列变成 1、-1 序列, 为此作变换得到的序列称为 $\tilde{b}$, 根据自相关函数的定义, 自相关函数如下:

$$c(\tau)=\frac{1}{2^n-1}\sum_{k=1}^{2^n-1}\tilde{b}_k\tilde{b}_{k+\tau},\ \tau=0,\ \cdots,\ 2^n-1$$

m 子序列 $\tilde{a}$ 是非线性序列, 不具有线性可加性. 但 m 子序列是基于线性序列, 其自相关函数虽不同于 m 序列, 但通过对 25 位以内的线性反馈移位寄存器产生的子序列进行了统计分析, 结果显示 m 子序列自相关函数收敛于其母序列自相关函数. 当 $\tau=0$ 时, $|c(\tau)|=1$, 取值最大; $\tau\neq0$ 时, $|c(\tau)|$ 迅速下降. 表 1 对文献 1 列出的 8 至 17 位的各本原多项式所确定的式(2) 进行了$|C(\tau)|$ 统计, 得到各 m 子序列的$|C(\tau)|$ 主、副峰值如表 1. 由表知, 随着 n 的增大, 这类 m 子序列的副、主峰比迅速下降, 呈现尖锐自相关特性.

当移位寄存器位数大于 15 时, 其自相关函数副峰与主峰比小于百分之一. 所以, m 子序列也具有良好的自相关特性, 是好的伪随机序列.

5　m 子序列移位寄存器可实现性分析

m 子序列移位寄存器与 m 序列移位寄存器间的差异在于 m 子序列移位寄存器反馈函数增加了个性函数 y, 对 y 函数处理如下:

$$\begin{aligned} y(x) &= \overline{\bar{x}_{n-2}\bar{x}_{n-3}\cdots\bar{x}_1\bullet(x_{n-1}\oplus x_1)}\\ &= \overline{x_{n-2}+x_{n-3}+\cdots+x_2\bullet(x_{n-1}\oplus x_1)} \end{aligned}$$

y 函数逻辑关系是两项之积, 一项为异或关系, 另一项为或非关系. 虽然或非的因子数随寄存器位数增加而增加, 但随着可编程器件的广泛应用, 或非逻辑是最易于实现的逻辑电路, 所以, 不需要增加额外器件, 只要

表 1

n 位数	8	9	10	11	12	13	14	15	16	17
$\|c(\tau)\|$ 副峰值	0.102	0.0998	0.0694	0.0523	0.0335	0.0226	0.0192	0.0125	0.0077	0.0049
$\|c(\tau)\|$ 主峰值	1	1	1	1	1	1	1	1	1	1

在可编程器件内部启用一个 y 逻辑即可实现 m 子序列移位寄存器. 其实现如图 6 所示.

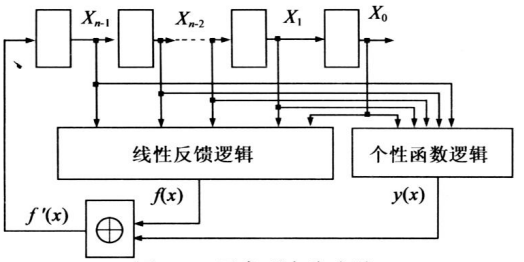

图 6 m 子序列产生电路

6 结论及几点说明

本文构造了第一类 m 子序列, 它的周期长、伪随机性能好, 是各类应用所需要的好序列. m 子序列的生成可以用移位寄存器硬件电路实现, 也可以用软件实现. 利用文中给出的构造方法, 可以得到更多性能优良的 m 子序列.

本文给出了第一类 m 子序列的反馈函数. 由于运行时间的因素, 在 PC 机上借助 VB, 我们只对 25 位以内的特定线性反馈函数 $f(x)$[1] 所对应的第一类子序列进行了验证, 且对自相关函数进行了统计分析. 在统计分析中, 我们还对部分相同位数的多个母序列对应的第一类子序列进行了统计, 结果显示, 母序列不同, 对应子序列的自相关函数值也不同, 但最终都收敛于各自的母序列.

参考文献:

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

[2] Chaoping Xing, San Ling. A class of linercodes with good arametmenters[J]. IEEE Trans Inform Theory, 2000, 46(6): 2184– 2188.

[3] Guang Gong. Cryptographic properties of the welchr gong transformation sequence generators[J]. IEEE Transactions on Information Theory, 2002, 48(11), : 2837– 2846.

[4] Nam Yutyu, Guang Gong. Crosscorrelation properties of binary sequences with ideal twor level autocorr elation[A]. Sequences and their applications—SETA 2006 4th[C]. 104– 118.

[5] J S No, H Chung, M S Yun. Binary pseudorandom Sequencesof period $2^n - 1$ with ideal autocorrelation[J]. IEEE Trans IT, 1998, 44(2): 814– 817.

[6] 胡玉濮. 一类理想自相关序列的伪随机性[J]. 电子学报, 2003, 31(2): 245– 247.
Hu Yurpu. Pseudor randomness of a class of sequences with ideal autocorrelation[J]. Acta Electronica Sinica, 2003, 31(2): 245– 247. (in Chinese)

[7] A Chang, P Gaal, S W Golomb, G Gong, T Helleseth, and P V Kumar. On a conjectured ideal autocorrelar tion sequence and a related tripleerror correct ing cyclic code[J]. IEEE Trans Inrform Theory, 2000, 46(3): 680– 687.

[8] S H Kim, J S No. New families of binary sequences with low correlation[J]. IEEE Trans Inform Theory, 2003, 49(11): 3059 – 3065.

[9] 孙林红, 叶顶锋, 吕述望, 冯登国. 高非线性布尔函数的构造[J]. 中国科学院研究生院学报, 2003, 20(4): 441– 445.
SUN Linr Hong, YE Ding Feng, LV Shur Wang, FENG Deng Guo. Construction of boolean function with high nonlinearity [J]. Journal of the Graduate School of the Chinese Academy of Sciences, 2003, 20(4): 441– 445. (in Chinese)

作者简介:

吕 虹 女, 1959 年出生于安徽怀宁, 硕士, 教授. 主要研究领域信息信号处理、电子系统设计、检测技术等. E-mail: ybl76@sohu.com

段颖尼 女, 1976 年出生于陕西西安, 硕士研究生. 主要研究领域信息信号处理、电子系统设计、SOC 等.

管必聪 1981 年出生于安徽无为, 硕士研究生, 主要研究领域数字信号处理、语音信号编解码等.

刘雨兰 女, 1977 年出生于江苏泰州, 硕士研究生, 主要研究领域为检测技术及数字信号处理、电子系统设计等.