基于母函数的非线性反馈函数及其子序列研究

吕 虹[1],张爱雪[2],方俊初[2],解建侠[1],李炳荣[2],戚 鹏[1]
(1.安徽建筑工业学院电子与信息学院,安徽合肥 230022;2.安徽工程大学电气工程学院,安徽芜湖 241000)

摘 要: 针对非线性最大长度移位寄存器反馈函数难以构造问题,本文提出了一种基于母函数构造非线性最大长度移位寄存器反馈函数方法.首先,我们阐述了母函数模 3 分类法,证明了各类母函数新的特征状态集,提取了母函数的特征式;其次,根据特征式对母函数的筛分特性合成了非线性 m 子序列移位寄存器反馈函数;最后,分析了该移位寄存器生成的伪随机序列,对其自相关值和线性复杂度进行了大量搜索.结果一致表明该序列不仅具有良好的周期特性、平衡特性、游程特性,还具有尖锐的自相关特性和理想的线性复杂度.

关键词: 非线性; 反馈函数; 合成; 筛分; 模 3; 特征式; 伪随机序列
中图分类号: TN801 **文献标识码:** A **文章编号:** 0372-2112 (2012) 10-2127-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.10.038

Study of the Non-Linear Feedback Functions and a Class Subsequence Based on the Root-Functions

LV Hong[1], ZHANG Ai-xue[2], FANG Jun-chu[2], XIE Jian-xia[1], LI Bing-rong[2], QI Peng[1]
(1. *Department of Electronic and Information Engineering, Anhui Institute of Architecture and Industry, Hefei, Anhui* 230022, *China*;
2. *Department of Electrical Engineering, Anhui polytechnic University, Wuhu, Anhui* 241000, *China*)

Abstract: To solve the problem of constructing feedback functions of non-linear maximal length shift registers (NMLSR), the method to construct the feedback functions for NMLSR was proposed based on root function. First of all, we expatiated the classification method of the root functions modulo 3, proveded the characteristic state sets of the root functions and extracted the eigenfunctions of the root functions. Secondly, we synthesized the feedback function for the nonlinear m subsequence shift register according to the filter of the eigenfunctions on the root functions. Finally, we conducted a great number of calculations and analyses for new type sequences generated from the nonlinear m subsequence shift registers. The results show unanimously that the nonlinear m subsequences dose not only possess better period property, balance property and run-path property, but also the sharp autocorrelation property and the ideal linear complexity.

Key words: nonlinear; feedback function; synthesize; filter; modulo 3; eigenfunction; pseudo-random sequence

1 引言

伪随机序列在信息安全、通信、雷达、测试、导航等许多重要领域具有广泛应用,是信息产业不可或缺的信息资源.伪随机序列性能的优劣直接影响序列密码的安全强度和通信系统的传输性能.基于移位寄存器生成伪随机序列是序列构造中一个重要分支,其不少重要序列在相关领域得到应用[1~3],对推动信息安全积极防御、通信系统高速、安全、宽频带发展起到了积极作用.

2 问题提出

m 序列是线性反馈移位寄存器(LFSR)生成的最重要伪随机序列,它的周期特性、平衡特性、游程特性、自相关特性都很好.但是,它的序列数目有限,难以满足通信系统需要的海量地址码;它的线性复杂度低,在信息加密中难以抵抗敌方的攻击.在实际应用中,为了获得周期长、复杂度高的伪随机序列,往往需要将若干个多级反馈移位寄存器产生的 m 序列进行平移、截短、求模 2 加等运算.这种生成方法改善了序列的某些特性[4~6],但同时也丢失了一些特性.本文基于 m 序列移位寄存器反馈函数,研究并证明了一类新序列,它的周期长度、平衡特性、游程特性、自相关特性都能与 m 序列相媲美,同时还具有 m 序列所不及的线性复杂度,其数目与 m 序列相同[7].

收稿日期:2011-10-13;修回日期:2012-06-16
基金项目:国家自然科学基金(No.61071001)

3 基于母函数的特征状态集

3.1 母函数和子序列

n 级移位寄存器,可以产生多种 m 序列[8],每一种 m 序列都对应着一个确定的线性反馈函数,其形式如下:

$$f_m(x) = c_{n-1}x_{n-1} \oplus c_{n-2}x_{n-2} \cdots c_0 x_0 \quad (1)$$

其中,$\oplus$ 模 2 加;

$c_i \in GF(2)$,反馈系数,$c_0 = 1$,最低位反馈系数;

$x_i \in GF(2)$,移位寄存器第 i 位状态,$i = 0、1 \cdots n-1$.

本文基于 m 序列移位寄存器反馈函数构造新的反馈函数,故把 m 序列移位寄存器反馈函数称为母函数,移位寄存器简称为移存器.

m 序列移存器状态转换规律由其反馈函数 $f_m(x)$ 确定,设其状态为 $s_i(i = 0、1 \cdots 2^n - 2)$,则其状态转换依次由 $s_0 \rightarrow s_1 \rightarrow \cdots \rightarrow s_j \cdots \rightarrow s_{2^n-2} \rightarrow s_0$,电路完成一个大循环,如图 1 虚线所示,同时移位输出一个周期 m 序列.如果借助一函数 $y(x)$,对 m 序列反馈函数 $f_m(x)$——即母函数进行处理,改变 m 序列移存器状态转换,形成一个状态转换如图 1 实线所示,其循环长度仍然为 $2^n - 1$ 的、新的非线性移存器反馈函数,则新移存器输出的就是基于母函数的 m 子序列,对应移存器就称为 m 子序列移存器[7].为便于讨论,本文所指移存器均为右移型,图 2 是线性右移移存器.

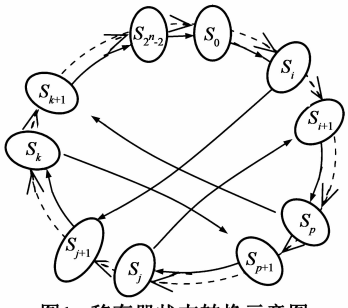

图1 移存器状态转换示意图

3.2 特征状态对

m 子序列移存器反馈函数是采用函数 $y(x)$ 对母函数 $f_m(x)$ 处理得到的.处理过程是对母函数 $f_m(x)$ 值的保留和改变过程.保留就是在特定状态下维持母函数值不变,移存器状态转换也不变;改变就是在特定状态下改变母函数值,移存器状态转换也改变.在二值逻辑中,改变就是求反.若要在状态转换中实现改变,就得在对应处对母函数值求反[7].根据移存器状态转换特点,只要对 m 序列移存器状态转换大循环中位置相互交错且仅低位互补的 $2i(i > 0)$ 对状态所对应的反馈函数值求反[5],即可得到一个新的状态转换大循环.图 1 中,实线给出的大循环是一例 m 子序列移存器状态转换大循环,图中状态$(s_i、s_j)$、$(s_p、s_k)$就是这样两对状态.称 m 序列移存器状态转换大循环中位置相互交错且仅低位互补的 $2i(i > 0)$ 对状态为母函数的特征状态,形成新的转换大循环所需要的特征状态对构成了母函数的一个特征状态集.

3.3 基于母函数的特征状态集

对于 n 级 m 序列移存器,反馈函数 $f_m(x)$ 由式(1)表达.由式(1)知,反馈函数值由具有非零系数的各项 $x_i(0 \leqslant i < n)$ 确定,故采用具有非零系数的各项 x_i 构成反馈函数数组 X,且 $f_m(x)$ 与 X 数组一一对应.为了揭示反馈函数 $f_m(x)$ 值与移存器各位状态取值之间关系,采用模 3 取余分类法对移存器各位状态 x_i 进行分类变换.模 3 取余分类法如下:n 级移存器各位为 $x_i(0 \leqslant i < n)$,用 n 减去 x_i 下标 i,即:$n - i$,其差值模 3 取余,可以得到余数 1、2、0,余数为 1 的 x_i 都称为位 1,同理有位 2、位 0.这样,对于图 2 移存器,其各位从左到右循环记为位 1、位 2、位 0.对 X 数组中元素 x_i,也采用模 3 取余进行分类,其结果使 X 数组中元素也都归为位 1、位 2、位 0 三类.

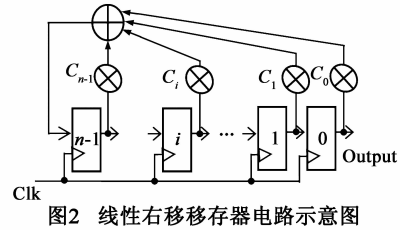

图2 线性右移移存器电路示意图

对于 n 级 m 序列移存器,反馈函数 $f_m(x)$ 均由偶数项组成,故 X 数组中对应有偶数个元素.根据数论可知,X 数组中偶数个元素的组成只可能是以下四种情况之一:位 1、位 2、位 0 元素都有偶数个;位 1 元素有偶数个,位 2、位 0 元素各有奇数个;位 2 元素有偶数个,位 1、位 0 元素各有奇数个;位 0 元素有偶数个,位 1、位 2 元素各有奇数个.

n 级 m 序列移存器,其位数 n 可以分为:$n = 3k$、$n = 3k + 1$ 和 $n = 3k + 2(k = 0,1,2 \cdots)$.根据 m 序列移存器位数 n 和 X 数组中位 1、位 2、位 0 元素数目的不同,有如下定理.

定理 对于 n 级 m 序列移存器,当位数 $n = 3k(k = 1,2 \cdots)$ 时,若 X 数组中位 1、位 2、位 0 元素都有偶数个,则低位互补状态对(001…000、001…001)和(100…100、100…101)在状态转换大循环中位置相互交错,构成母函数 $f_m(x)$ 的一个特征状态集{(001…000、001…001)、(100…100、100…101)};若 X 数组中位 1 元素有偶数个,位 2、位 0 元素各有奇数个,则低位互补状态对(010…010、010…011)和(001…000、001…001)在状态转

换大循环中位置相互交错,构成母函数 $f_m(x)$的一个特征状态集{(010…010、010…011)、(001…000、001…001)};若 X 数组中位 2 元素有偶数个,位 1、位 0 元素各有奇数个,则低位互补状态对(100…101、100…100)和(010…010、010…011)在状态转换大循环中位置相互交错,构成母函数 $f_m(x)$的一个特征状态集{(100…100、100…101)、(010…010、010…011)};X 数组中位 0 元素有偶数个,位 1、位 2 元素各有奇数个情况不可能出现.

当 $n=3k+1(k=1,2\cdots)$时,若 X 数组中位 1、位 2、位 0 元素都有偶数个,则低位互补状态对(001…0011、001…0010)和(100…1001、100…1000)构成母函数 $f_m(x)$的一个特征状态集;若 X 数组中位 1 元素有偶数个,位 2、位 0 元素各有奇数个,则低位互补状态对(010…0101、010…0100)和(001…0010、001…0011)构成母函数 $f_m(x)$的一个特征状态集;若 X 数组中位 2 元素有偶数个,位 1、位 0 元素各有奇数个,则低位互补状态对(100…1000、100…1001)和(010…0100、010…0101)构成母函数 $f_m(x)$的一个特征状态集;X 数组中位 0 元素有偶数个,位 1、位 2 元素各有奇数个情况不可能出现.

当 $n=3k+2(k=1,2\cdots)$ 时,若 X 数组中位 1、位 2、位 0 元素都有偶数个,则低位互补状态对(001…00100、001…00101)和(100…10010、100…10011)构成母函数 $f_m(x)$的一个特征状态集;若 X 数组中位 1 元素有偶数个,位 2、位 0 元素各有奇数个,则低位互补状态对(010…01000、010…01001)和(001…00100、001…00101)构成母函数 $f_m(x)$的一个特征状态集;若 X 数组中位 2 元素有偶数个,位 1、位 0 元素各有奇数个,则低位互补状态对(100…10010、100…10011)和(010…01000、010…01001)构成母函数 $f_m(x)$的一个特征状态集;X 数组中位 0 元素有偶数个,位 1、位 2 元素各有奇数个情况不可能出现.

证明:对于 n 级 m 序列移存器,当位数 $n=3k(k=1,2\cdots)$时:

(以下证明中,双引号"1"、"0"表示函数值;单引号'1'、'0'表示移存器位状态;不带引号的 0、1 组合表示移存器状态)

1. 若 X 数组中位 1、位 2、位 0 元素都有偶数个,根据(1)式可知,母函数 $f_m(x)$值由移存器偶数个位 1、偶数个位 2、偶数个位 0 状态确定,n 级 m 序列移存器由状态 001…001000 完成如下转换:

001…001000→100…100→010…010→
001…001→… (2)

在式(2)转换中,第一个状态 001…001000 的位 1、位 2 状态都为'0',只有位 0 状态有'1',而在所有的位 0 中,最后一个位 0 状态是'0',余者都是'1'.由式(1)知,母函数 $f_m(x)$一定包含移存器最低位,所以构成母函数 $f_m(x)$的各位中,仅有奇数个位 0 状态是'1',其它都是'0'.根据式(1),奇数个'1'模 2 加,使母函数 $f_m(x)$在 001…001000 状态时取值为"1",这个"1"将反馈给移存器,作为移存器下一个状态的最高位.所以,移存器由状态 001…001000 反馈、移位转换到状态 100…100100.

对于 100…100 状态,由于它的位 2、位 0 均为'0',仅位 1 都是'1'.构成母函数 $f_m(x)$的偶数个位 1、偶数个位 2 和偶数个位 0 中,只有偶数个位 1 状态是'1',其它都是'0'.根据(1)式,偶数个'1'使母函数 $f_m(x)$在 100…100 状态时值为"0",这个"0"将反馈给移存器,作为下一个状态的最高位.所以,移存器由状态 100…100 反馈、移位又转换到状态 010…010.

状态 010…010 的位 1、位 0 都是'0',位 2 均为'1',构成母函数 $f_m(x)$的偶数个位 1、偶数个位 2 和偶数个位 0 中,只有偶数个位 2 状态是'1'.根据式(1),偶数个'1'使反馈函数 $f_m(x)$在 010…010 状态时值为"0",这个"0"将反馈给移存器,作为下一个状态的最高位.所以,移存器由状态 010…010 又转换到状态 001…001.上述分析如式(2)转换,式(2)中第二个状态 100…100 的低位互补状态 100…101,没有出现在式(2)转换链中,那么一定处在由 001…000 到 001…001 转换链以外,故低位互补状态对 100…100、100…101 与 001…000、001…001 在 m 序列移存器状态转换大循环中位置一定相互交错,构成该类母函数 $f_m(x)$的一个特征状态集{(001…000、001…001)、(100…100、100…101)}.

2. 若 X 数组中位 1 元素有偶数个,位 2、位 0 元素各有奇数个,根据式(1)可知,母函数 $f_m(x)$的值由偶数个位 1、奇数个位 2、奇数个位 0 状态确定.按照上述分析方法,同样可以得到 m 序列移存器由状态 010…010011 完成如下转换:

010…010011→001…001→100…100→
010…010→… (3)

故低位互补状态对 001…000、001…001 与 010…010、010…011 在 m 序列移存器状态转换大循环中位置一定相互交错,构成该类母函数 $f_m(x)$的一个特征状态集{(010…010、010…011)、(001…000、001…001)}.

3. 若 X 数组中位 2 元素有偶数个,位 1、0 元素有奇数个,根据式(1)可知,母函数 $f_m(x)$的值由偶数个位 2、奇数个位 1、奇数个位 0 状态确定.同理,m 序列移存器状态有如下转换:

100…101→010…010→001…001→
100…100→… (4)

故状态对 100…100、100…101 与 010…010、010…011 在

m序列移存器状态转换大循环中位置一定相互交错,构成该母函数 $f_m(x)$ 的一个特征状态集{(100…100、100…101)、(010…010、010…011)}.

4)若 X 数组中位 0 元素有偶数个,位 1、位 2 元素均有奇数个,由式(1)可知,母函数 $f_m(x)$ 的值由偶数个位 0、奇数个位 1、奇数个位 2 状态确定,则 m 序列移存器状态有如下转换:

$$011\cdots011\rightarrow101\cdots101\rightarrow110\cdots110\rightarrow011\cdots011 \quad (5)$$

在式(5)转换中,第一个状态 011…011 的位 2、位 0 都为'1',位 1 都为'0',构成母函数 $f_m(x)$ 的奇数个位 2、偶数个位 0,使母函数各项中共有奇数个'1'.根据式(1),奇数个'1'使母函数 $f_m(x)$ 值为"1".这样,移存器由状态 011…011 移位转换到 101…101;状态 101…101 的位 1、位 0 都是'1',位 2 都是'0',构成母函数 $f_m(x)$ 的偶数个位0'1'和奇数个位1'1',同样使母函数 $f_m(x)$ 值为"1",所以移存器又移位转换到状态 110…110;状态 110…110 的位 1、位 2 都是'1',位 0 都是'0',构成母函数 $f_m(x)$ 的奇数个位 1'1'与奇数个位 2'1'使反馈函数 $f_m(x)$ 值为"0".所以,移存器由状态 110…110 转换到 011…011,如式(5)所示.由式(5)知,状态 011…011 经过三次转换又回到 011…011,形成了一个死循环,显然,这与 m 序列移存器状态转换相矛盾,故假设错误,这种情况不存在.

$n=3k(k=1,2\cdots)$情况证毕.

以上证明了移存器位数 $n=3k(k=1,2\cdots)$时情况,对于 $n=3k+1$、$3k+2(k=1,2\cdots)$情况证明类同,此处略.

根据以上分析知,不管移存器位数 n 是多少,m 序列移存器反馈函数数组 X 只有三种,所以母函数 $f_m(x)$ 也对应分为三类.由于其中采用了模 3 取余算法,故称这种分类为模 3 分类法.对于模 3 分类中每一类母函数都对应有各自的特征状态集.由以上证明知,001 和 100 型状态对构成第一类母函数的一个特征状态集;010 和 001 型状态对构成第二类母函数的一个特征状态集;100 和 010 型状态对构成第三类母函数的一个特征状态集.

4 非线性反馈函数

4.1 特征式提取

由 3.2 节分析知,移存器处于非特征状态时,函数 $y(x)$ 使 m 子序列移存器保持 m 序列移存器状态转换不变,m 子序列反馈函数值等于母函数值;移存器处于特征状态时,函数 $y(x)$ 改变 m 序列移存器状态转换,形成 m 子序列移存器状态转换,m 子序列反馈函数值等于母函数值的反.所以,函数 $y(x)$ 是反映特征状态集中所有特征状态的函数,当移存器处于特征状态时,$y(x)$ 值取"1",否则取值为"0".根据逻辑代数理论,$y(x)$ 是特征状态集中所有状态小项之和式,有:

$$y(x)=m_i+m_j+\cdots=\sum m_k \quad (6)$$

这里,称 $y(x)$ 为母函数的特征函数式,简称特征式.

4.2 非线性反馈函数的合成

对于移存器,每一个状态的后继状态都只有两种可能,是一对仅高位逻辑互补的状态[7].对于每一个状态来说,改变转换,就意味着移存器放弃现有后继状态,而取另一个状态为后继.3.2 节已分析,仅在特征状态处改变移存器状态转换,就能使 m 序列移存器转化为 m 子序列移存器.这种改变的实现,仅在特征状态处对母函数求反,其它状态处保留母函值不变.由式(6)知,$y(x)$ 仅在特征状态时值取"1",利用这个"1"对母函数 $f_m(x)$ 求反,滤出反函数,使 m 子序列移存器仅在特征状态处改变原转换,形成新的大循环.$y(x)$ 在其它状态时取值为"0",利用这个"0",保留母函数值,使 m 子序列移存器在非特征状态处保持原转换.综合以上分析,得到 m 子序列移存器反馈函数 $f_m'(x)$ 关于 $f_m(x)$、$y(x)$ 的合成式如下[9]:

$$f_m'(x)=f_m(x)\oplus y(x) \quad (7)$$

对于式(7):

$y(x)=0$ 时,$f_m'(x)=f_m(x)\oplus0=f_m(x)$

$y(x)=1$ 时,$f_m'(x)=f_m(x)\oplus1=\overline{f_m(x)}$

这里,$y(x)=0$ 时,$y(x)$ 式将 $f_m(x)$ 滤出,子序列反馈函数保留母函数值;$y(x)=1$ 时,$y(x)$ 式将 $\overline{f_m(x)}$ 滤出,子序列反馈函数值是母函数的反.可见,$y(x)$ 式对 $f_m(x)$ 函数的处理实现了筛分作用,$y(x)$ 又可称为 $f_m(x)$ 的筛分函数.

5 子序列特性分析

5.1 伪随机基本特性

由于 m 子序列仍然由循环长度为 2^n-1 的移存器产生,所以其周期特性、游程特性、平衡特性与 m 序列完全相同,具有良好伪随机特性.

5.2 自相关特性

设 $a_k(k=0\cdots2n-2)$ 是 m 子序列,经过 $b_k=1-2a_k$ 变换为 1、-1 的 b_k 序列,定义其归一化自相关函数为[8]:

$$R_b(\tau)=\frac{1}{2^n-1}\sum_{k=0}^{2^n-2}b_kb_{k+\tau},\quad \tau=0\cdots2^n-2 \quad (8)$$

m 序列是线性序列,具有理想的二值自相关特性.m 子序列是非线性序列,不具有线性可加性,其自相关函数虽不同于 m 序列,但通过对 20 位以内大量 m 序列、m 子序列一个周期内自相关值的计算,结果一致显

示 m 子序列自相关特性收敛于 m 序列自相关特性,且有:

$$\begin{cases}\tau=0, R_b(\tau)=1\\ \tau\neq 0, R_b(\tau)\to 0, n\to\infty\end{cases}$$

表 1 列出部分 m 子序列自相关副、主峰比值,图 3 是表 1 中 9、10、11 级 m 子序列自相关特性图.表 1、图 3 显示,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.所以,m 子序列也具有良好的自相关特性.

5.3 线性复杂度

m 子序列是非线性序列,较 m 序列线性复杂度得到改善.我们采用 b-m 算法在 VC 上对 15 位以内大量子序列线性复杂度进行了计算[10~12],结果表明,子序列线性复杂度虽然随母函数不同有所波动,但子序列线性复杂度较母序列都有很大改善,表 1 给出了部分相应计算结果.由表 1 知,m 子序列线性复杂度不仅较 m 序列有很大改善,且都趋于 m 序列长度的二分之一左右,是比较理想的.

表 1　m 序列和 m 子序列自相关特性和线性复杂度

移位寄存器位数 n	5	6	7	8	9	10	11	12	13	14	15
m 序列反馈函数	$x_3\oplus x_0$	$x_5\oplus x_0$	$x_6\oplus x_0$	$x_6\oplus x_5\oplus x_4\oplus x_0$	$x_8\oplus x_5\oplus x_1\oplus x_0$	$x_7\oplus x_0$	$x_9\oplus x_0$	$x_8\oplus x_2\oplus x_1\oplus x_0$	$x_{12}\oplus x_2\oplus x_1\oplus x_0$	$x_{13}\oplus x_2\oplus x_1\oplus x_0$	$x_{11}\oplus x_0$
m 子序列自相关副、主峰比	0.29	0.27	0.134	0.121	0.119	0.073	0.016	0.042	0.027	0.020	0.014
m 序列复杂度	5	6	7	8	9	10	11	12	13	14	15
m 子序列复杂度	16	42	83	112	293	615	1588	2420	3758	7348	17718

6 结论

本文提出了一种非线性最大长度移存器反馈函数构造方法,构造了一类非线性反馈函数,利用该反馈函数生成的伪随机序列,其周期特性、游程特性、平衡特性、自相关特性都能与 m 序列相媲美,同时还具有 m 序列所不及的线性复杂度.该类序列可用于密码、通信、测量等领域.

参考文献

[1] Mansouri Shohreh Sharif, Dubrova Elena. An improved hardware implementation of the grain stream cipher[A]. Proceedings of the 13th Euromicro Conference on Digital System Design: Architectures, Methods and Tools[C]. 2010. 433 – 440.

[2] Lan Jingjing, Goh Wang Ling, Kong Zhi Hui, Yeo Kiat Seng. A random number generator for low power cryptographic application[A]. Proceedings of the 2010 International SoC Design Conference[C]. 2010. 328 – 331.

[3] Lvhong, et al. Design and Implementation of A Maximal Length Nonlinear Pseudorandom Sequence[A]. Proceedings of the 2009 International Conference on Computer and Communications Security[C]. 2009, 12, 64 – 67.

[4] Kang Minsu. FPGA implementation of Gaussian-distributed pseudo-random number generator[A]. Proceeding of the 6th International Conference on Digital Content, Multimedia Technology and Its Applications[C]. 2010. 11 – 13.

[5] Poorghanad Alireza, Sadr Ali, Kashanipour Alireza. Generating high quality pseudo random number using evolutionary methods[A]. Proceedings of the 2008 International Conference on Computational Intelligence and Security[C]. 2008. 331 – 335.

[6] Chang Shih Yu, Wu Hsiao-Chun, Pang Ai-Chun. Theoretical exploration of pattern attributes for maximum-length shift-register sequences[A]. Proceedings of the 2009 ACM International Wireless Communications and Mobile Computing Conference[C]. 2009. 1116 – 1120.

[7] 吕虹,段颖妮,管必聪.一种非线性最大长度伪随机序列发生器的设计[J].电子器件,2008,31(3):898 – 900.

[8] 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. 124 – 145.

[9] 常祖领,柯品惠,温巧燕.高非线性度多输出布尔函数的构造[J].电子学报,2008,36 (1):141 – 145.
CHANG Zu-ling, KE Pin-hui, et al. Constructions of multi-output boolean functions with high nonlinearity[J]. Acta Electronica Sinica, 2008, 36(1): 141 – 145. (in Chinese)

[10] 刁哲军,陈嘉兴,刘志华.一种具有大线性复杂度伪随机序列的构造[J].电子学报,2008,36(10):1961 – 1965.
DIAO Zhe-jun, CHEN Jia-xing, LIU Zhi-hua. A new design

for pseudorandom sequences with large linear span[J]. Acta Electronica Sinica, 2008, 36(10): 1961 – 1965. (in Chinese)
[11] Chang, P Gaal, S W Golomb, G Gong, T Helleseth, P V Kumar. On a conjectured ideal autocorrelation sequence and a related triple error correcting cyclic code[J]. IEEE Trans Inform Theory, 2000, 46(2): 680 – 687.
[12] Marchi A, Liverani A, Del Giudice A. Polynomial pseudo-random number generator via cyclic phase [J]. Mathematics and Computers in Simulation, 2009, 79(11): 3328 – 3338.

作者简介

吕 虹 女,1959 年 10 月出生于,安徽怀宁人,硕士,教授,研究方向信号处理,检测技术、EDA 技术等.
E-mail: lvhong176@163.com

张爱雪 女,1977 年出生于山东郓城,安徽工程大学电气工程学院讲师,主要研究方向为信息信号处理、嵌入式系统等.

方俊初 男,1974 年 4 月出生,安徽六安人,硕士,讲师,研究领域涉及信号处理,电子技术,电子系统设计、检测技术等.