乘积序列的相关分析

肖 鸿[1,2]，肖国镇[1]，王新梅[1]

(1. 西安电子科技大学 综合业务网理论及关键技术国家重点实验室，陕西 西安 710071；
2. 空军工程大学 电讯工程学院，陕西 西安 710077)

摘要：给出了基于任意有限多个线性移位寄存器与一个与门逻辑构成的非线性组合器而生成的非线性乘积序列的自相关函数在整个数轴上的完整表述，给出了这种序列在一个周期内的 Hamming 重量的计算公式，并且指出任意 l 个 m 序列的乘积序列的自相关函数是 $l+1$ 值函数，并且主峰值很高.

关键词：乘积序列；自相关函数；Hamming 重量

中图分类号：O211.6 **文献标识码**：A **文章编号**：1001-2400(2008)01-0076-05

On the correlation analysis of product sequences

XIAO Hong[1,2], *XIAO Guo-zhen*[1], *WANG Xin-mei*[1]

(1. State Key Lab. of Integrated Service Networks, Xidian Univ., Xi′an 710071, China; 2. The Telecommunication Engineering Inst, Air Force Engineering Univ., Xi′an 710077, China)

Abstract: This paper presents a complete representation of auto-correlation functions of product sequences generated by one nonlinear combining function which consists of a finite number of l linear feedback shift registers (LFSR's) with an AND gate logic, gives a formula for determining the Hamming weight of this product sequences in a period, and shows that the auto-correlation functions of such a kind of product sequences take $l+1$ values and that the main maximum value is high.

Key Words: product sequence; auto-correlation function; Hamming weight

在传统的单钥加密体制中，必须保证密钥流的每一位均具有良好的伪随机特性. 通常应该满足 Golomb 提出的 3 条标准[1]，其中“周期自相关函数为二值函数或接近二值函数”集中反映了序列的每一位出现的随机性. 另外，具有该标准的序列也因此而被广泛地应用于通信、雷达、光学测距等重要领域. 笔者在引出流密码系统中经常使用的由 s 个线性反馈移位寄存器(负责提供随机性较好的序列，常用的是 m 序列)和一个非线性组合器(负责提高密钥流序列的线性复杂度)所组成的非线性密钥流生成器(见图 1)之后，集中讨论了这种乘积序列的自相关函数，并且得到了一定的结果.

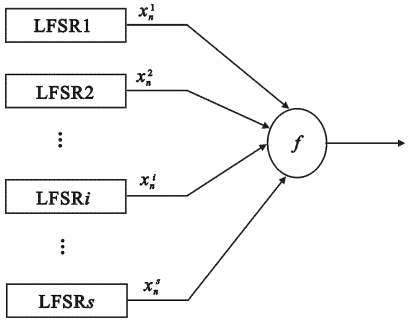

图 1 非线性组合生成器

非线性移位寄存器序列由于缺乏行之有效的数学工具，目前关于它的研究理论还很不成熟. 人们试图寻求在线性移位寄存器基础上产生的非线性前馈网络及非线性组合生成器的研究. 文[2,3]建议在线性反馈移位寄存器的基础上利用非线性“滤波”之输出作为密钥系统. Groth 提出的这种非线性生成器，是由一个以本原多项式为联接多项式的线性反馈移位寄存器并且在两级上带有非线性逻辑作为输出的网络，称这种网络为前馈网络[4]. 由于这种生成器只需一个线性移位寄存器，所以有一定的实用价值. 然而，在一般的情况下，这类密钥流生成器的分析是比较困难的，并且对二端与门前馈网络来说，其生成的非线性序列的周期并没有增大原来 m 序列的周期.

收稿日期：2007-08-08

基金项目：国家自然科学基金资助(60473028)

作者简介：肖 鸿(1967-)，男，西安电子科技大学博士研究生，E-mail：siaohong@126.com.

1　二个级数互素的 m 序列的乘积序列的相关分析

为了进一步改善上面提及的乘积序列的密码体制和构造更为复杂的二元序列,Pless,Rubin 等人提出了如图 1 所示的由两个乃至多个线性移位寄存器的输出端通过一个选定的非线性逻辑函数来产生相应的输出序列.先来分析由两个线性反馈移位寄存器(LFSR)诱导出的乘积序列,再将结果推广到有限多个 LFSR 的情形.从 Boole 函数的角度来看,任何一个 Boole 函数的运算都可归结为若干个变元的乘积以及这些乘积的模 2 和的运算,下面来研究由两个级数互素的 LFSR 诱导出的乘积序列的生成器,对于这种乘积序列已有如下结论[2,5,6].

设 LFSR1,LFSR2 分别是以 GF(2)上 r 次,s 次本原多项式 $f_r(x)$,$f_s(x)$ 为联接多项式的两个线性移位寄存器,$\gcd(r,s)=1$,并且分别假定 $\{\alpha^{2^{i-1}}\}$,$1\leqslant i\leqslant r$ 及 $\{\beta^{2^{j-1}}\}$,$1\leqslant j\leqslant s$ 为 $f_r^*(x)$,$f_s^*(x)$ 的共轭根组,$(f_r^*(x),f_s^*(x))$ 分别是 $f_r(x)$,$f_s(x)$ 的互反多项式,$\{a_n\}$,$\{b_n\}$ 分别是由 LFSR1 及 LFSR2 输出的 r 级,s 级 m 序列,$\{c_n\}=\{a_nb_n\}$ 是最后输出的乘积序列.于是

(1) $\{c_n\}$ 以 $f(x)=\prod_{i=1}^{r-1}\prod_{j=1}^{s-1}(x-\alpha^{-2^{i-1}}\beta^{-2^{j-1}})$ 为极小多项式.

(2) $\{c_n\}$ 的周期为 $(2^r-1)(2^s-1)$.

(3) $\{c_n\}$ 的复杂度为 rs.

但是,这种乘积序列在一个周期段内 0,1 出现的概率是否相等,即该序列的周期自相关函数是否为二值或接近二值函数,该序列在一个周期内的 Hamming 重量怎样求得,对于有限多个 m 序列的乘积序列的自相关函数和 Hamming 重量又是怎样.下面给出笔者针对这几个问题的解答.

定义 1　一个二元序列 Y 的 Hamming 重量定义为该序列在一个周期内 1 的个数,表示为 $W_H(Y)$.

定义 2　设二元序列 $Y=\{y_n\}(n=1,2,\cdots)$ 的周期为 T,作变换 $\eta(y_n)=(-1)^{y_n}$,$y_n=0$ 或 1,则 $\eta(0)=1$,$\eta(1)=-1$.周期序列的自相关函数定义为 $R_Y(\tau)=\sum_{n=1}^{T}\eta(y_n)\eta(y_{n+\tau})$.

按上述定义,可对 $R_Y(\tau)$ 作如下推导:

$$R_Y(\tau)=\sum_{n=1}^{T}\eta(y_n)\eta(y_{n+\tau})=\sum_{n=1}^{T}(-1)^{y_n}(-1)^{y_{n+\tau}}=\sum_{n=1}^{T}(-1)^{y_n\oplus y_{n+\tau}}=\sum_{n=1}^{T}(1-2(y_n\oplus y_{n+\tau}))=$$

$$T-2\sum_{n=1}^{T}(y_n\oplus y_{n+\tau})=T-2W_H(Y\oplus Y_\tau),\text{令}\quad Y_\tau=\{y_{n+\tau}\}\quad,\tag{1}$$

由关系式 $y_n\oplus y_{n+\tau}=y_n+y_{n+\tau}-2y_ny_{n+\tau}$ 可得

$$\sum_{n=1}^{T}(y_n\oplus y_{n+\tau})=\sum_{n=1}^{T}y_n+\sum_{n=1}^{T}y_{n+\tau}-2\sum_{n=1}^{T}y_ny_{n+\tau}\quad,$$

即

$$W_H(Y\oplus Y_\tau)=2W_H(Y)-2R_Y'(\tau)=2W_H(Y)-2W_H(YY_\tau)\quad,\tag{2}$$

式中 $R_Y'(\tau)=\sum_{n=1}^{T}y_ny_{n+\tau}$.

由周期序列的自相关函数定义得出自相关函数与 $R_Y'(\tau)$(即 Y 与 Y_τ 乘积序列的重量)之间的一个关系为

$$R_Y(\tau)=T-2W_H(Y\oplus Y_\tau)=T-4W_H(Y)+4R_Y'(\tau)\quad,$$

$$R_Y'(\tau)=W_H(Y)-(T-R_Y(\tau))/4\quad.\tag{3}$$

由上述关系式可以看出,求一个周期序列的自相关函数的值与 $R_Y'(\tau)$ 的值密切相关.因此,可以将结果应用到求乘积序列的自相关函数.

设二元 m 序列 $X=\{x_n\}$,$Y=\{y_n\}$,$C=\{c_n\}=\{x_ny_n\}$,$\{x_n\}$ 与 $\{y_n\}$ 的周期分别是 $P_1=2^{r_1}-1$,$P_2=2^{r_2}-1$,且 $(r_1,r_2)=1$.$(r_1,r_2)=1$ 当且仅当 $(P_1,P_2)=1$.由前述已知结论可得:c_n 的周期为 P_1P_2,c_n 的自相关函数 $R_C(\tau)$ 与 $R_C'(\tau)$ 有关.

$$R'_C(\tau)=\sum_{n=1}^{P_1P_2}c_nc_{n+\tau}=\sum_{n=1}^{P_1P_2}x_nx_{n+\tau}y_ny_{n+\tau}=\sum_{t=1}^{P_2}\sum_{i=0}^{P_1-1}x_{iP_2+t}x_{iP_2+t+\tau}y_{iP_2+t}y_{iP_2+t+\tau}=$$
$$\sum_{t=1}^{P_2}y_ty_{t+\tau}\sum_{i=0}^{P_1-1}x_{iP_2+t}x_{iP_2+t+\tau}=R'_Y(\tau)R'_X(\tau)\quad . \tag{4}$$

式(4)中 $x_nx_{n+\tau}y_ny_{n+\tau}$ 按下标排成的矩阵有$P_1\times P_2$ 和$P_2\times P_1$ 两种排法,且都有上述结果.

因为 $(P_1,P_2)=1$,当 i 遍历模 P_1 的完全剩余类时,iP_2+t 也遍历模 P_1 的完全剩余类. 因此 $\sum_{i=0}^{P_1-1}x_{iP_2+t}x_{iP_2+t+\tau}=\sum_{n=1}^{P_1}x_nx_{n+\tau}=R'_X(\tau)$. 同理$\sum_{i=0}^{P_2-1}y_{iP_1+t}y_{iP_1+t+\tau}=\sum_{n=1}^{P_2}y_ny_{n+\tau}=R'_Y(\tau)$.

由于 $R'_X(\tau)$ 的定义,$R'_X(\tau)=\sum_{n=1}^{P_1}x_nx_{n+\tau}$ 要求下标必须遍历 m 序列 X 的周期,因此,只有当$(P_1,P_2)=1$ 时才有结果$R'_C(\tau)=R'_X(\tau)R'_Y(\tau)$,即这个结果无法推广到两个级数不是互素的 m 序列的乘积序列中去. 这就给研究任意有限个对级数没有限制的一组 LFSR 组成的非线性生成器带来很大的困难. 因此,笔者在一开始就假定两个 m 序列的周期是互素的,对于有限多个的情况也是如此.

通过上述推导有如下定理.

定理 1 设 $X=\{x_n\}$ 与 $Y=\{y_n\}$ 分别是周期为$P_1=2^{r_1}-1$,$P_2=2^{r_2}-1$ 的 m 序列,其中$(r_1,r_2)=1$. 则 (1) 对于乘积序列 $C=\{c_n=x_ny_n\}$ 有 $R'_C(\tau)=R'_X(\tau)R'_Y(\tau)$. (2) $W_H(C)=R'_C(0)=R'_X(0)R'_Y(0)=W_H(X)W_H(Y)$.

现利用定理 1,计算乘积序列 $C=\{c_n=x_ny_n\}$ 的自相关函数 $R_C(\tau)$ 的值. 根据前面的结论,应先计算 $R'_C(\tau)$:

(1) $T=P_1P_2=(2^{r_1}-1)(2^{r_2}-1)$.

(2) $W_H(C)=W_H(X)W_H(Y)=(2^{r_1-1})(2^{r_2-1})$.

(3) $R'_C(\tau)=R'_X(\tau)R'_Y(\tau)$.

由式(3) $R'_X(\tau)=W_H(X)-\dfrac{P_1-R_X(\tau)}{4}=\begin{cases}2^{r_1-1} & ,\quad \tau\equiv 0 \bmod P_1 \quad ,\\ 2^{r_1-2} & ,\quad \tau\not\equiv 0 \bmod P_1 \quad .\end{cases}$

同理,$R'_Y(\tau)=W_H(Y)-\dfrac{P_2-R_Y(\tau)}{4}=\begin{cases}2^{r_2-1} & ,\quad \tau\equiv 0 \bmod P_2 \quad ,\\ 2^{r_2-2} & ,\quad \tau\not\equiv 0 \bmod P_2 \quad .\end{cases}$

现在来计算 $R'_C(\tau)$ 及 $R_C(\tau)$. 注意到 τ 从 1 到 P_1P_2 取值,其中存在节点$\tau\equiv 0 \bmod P_1$且$\tau\not\equiv 0 \bmod P_2$以及$\tau\not\equiv 0 \bmod P_1$且$\tau\equiv 0 \bmod P_2$,因此有

$$R'_C(\tau)=R'_X(\tau)R'_Y(\tau)=\begin{cases}2^{r_1-1}2^{r_2-1}=2^{r_1+r_2-2} & ,\quad \tau\equiv 0 \bmod P_1P_2 \quad ,\\ \left.\begin{matrix}2^{r_1-1}2^{r_2-2}\\ 2^{r_1-2}2^{r_2-1}\end{matrix}\right\}=2^{r_1+r_2-3} & ,\quad \begin{matrix}\tau\equiv 0 \bmod P_1 \text{且} \tau\not\equiv 0 \bmod P_2 \quad ,\\ \tau\not\equiv 0 \bmod P_1 \text{且} \tau\equiv 0 \bmod P_2 \quad ,\end{matrix}\\ 2^{r_1-2}2^{r_2-2}=2^{r_1+r_2-4} & ,\quad \tau\not\equiv 0 \bmod P_1 \text{且} \tau\not\equiv 0 \bmod P_2 \quad .\end{cases}$$

根据前面的结果 $R_C(\tau)=T-4W_H(C)+4R'_C(\tau)$ 可得

$$R_C(\tau)=\begin{cases}(2^{r_1}-1)(2^{r_2}-1) & ,\quad \tau\equiv 0 \bmod P_1P_2 \quad ,\\ 2^{r_1+r_2-1}-2^{r_1}-2^{r_2}+1 & ,\quad \begin{matrix}\tau\equiv 0 \bmod P_1 \text{ 且 } \tau\not\equiv 0 \bmod P_2 \quad ,\\ \tau\not\equiv 0 \bmod P_1 \text{ 且 } \tau\equiv 0 \bmod P_2 \quad ,\end{matrix}\\ 2^{r_1+r_2-2}-2^{r_1}-2^{r_2}+1 & ,\quad \tau\not\equiv 0 \bmod P_1 \text{且} \tau\not\equiv 0 \bmod P_2 \quad .\end{cases}$$

至此完全解决了前面提出的前两个问题. 下一节将这种结果推广到任意有限多个级数互素的 m 序列的乘积序列中.

2 任意有限个级数互素的 m 序列的乘积序列的相关分析

设 $X=\{x_n\}$,$Y=\{y_n\}$,$Z=\{z_n\}$ 分别是级数为 r_1,r_2,r_3,周期为 P_1,P_2,P_3 的 m 序列,且 r_1,r_2,r_3 两两

互素,即$(P_i,P_j)=1,i\neq j$. $C=c_n=x_ny_nz_n$,C 的周期为$T=P_1P_2P_3$,$R'_C(\tau)=\sum_{n=1}^{T}x_ny_nz_nx_{n+\tau}y_{n+\tau}z_{n+\tau}$. 按下述下标矩阵可将一重和变为二重和.

$n=iP_3+t$	$t=1$	$t=2$	$\cdots$	$t=P_3$
$i=0$	1	2	$\cdots$	P_3
$i=1$	P_3+1	P_3+2	$\cdots$	$2P_3$
$i=2$	$2P_3+1$	$2P_3+2$	$\cdots$	$3P_3$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
$i=P_1P_2-1$	$(P_1P_2-1)P_3+1$	$(P_1P_2-1)P_3+2$	$\cdots$	$P_1P_2P_3$

故 $R'_C(\tau)=\sum_{t=1}^{P_3}\sum_{i=0}^{P_1P_2-1}x_{iP_3+t}x_{iP_3+t+\tau}y_{iP_3+t}y_{iP_3+t+\tau}z_{iP_3+t}z_{iP_3+t+\tau}=\sum_{t=1}^{P_3}z_tz_{t+\tau}\sum_{i=0}^{P_1P_2-1}x_{iP_3+t}x_{iP_3+t+\tau}y_{iP_3+t}y_{iP_3+t+\tau}$.

因 $(P_3,P_1P_2)=1$,所以当 i 遍历模 P_1P_2 的完全剩余类时,iP_3+t 同样也遍历模 P_1P_2 的完全剩余类.

因此有 $\sum_{i=0}^{P_1P_2-1}x_{iP_3+t}x_{iP_3+t+\tau}y_{iP_3+t}y_{iP_3+t+\tau}=\sum_{n=1}^{P_1P_2}x_nx_{n+\tau}y_ny_{n+\tau}=R'_X(\tau)R'_Y(\tau)$,

故 $R'_C(\tau)=R'_X(\tau)R'_Y(\tau)R'_Z(\tau)$, $W_H(C)=W_H(X)W_H(Y)W_H(Z)$.

以上说明,可以将前面的结果用归纳法推广到任意有限个 m 序列的乘积序列中.

定理 2　设 $X_i=(x_n^{(i)})_{n=0}^{\infty}$,$i=1,2,\cdots,l$ 是周期为$P_i=2^{r_i}-1$ 的 l 个 m 序列,且假设$(P_i,P_j)=1,i\neq j$,于是对乘积序列$Y=X_1X_2\cdots X_l$ 有:(1) $R'_Y(\tau)=\prod_{i=1}^{l}R'_{X_i}(\tau)$. (2) $W_H(Y)=\prod_{i=1}^{l}W_H(X_i)=\prod_{i=1}^{l}(2^{r_i-1})$.

根据定理 2,现在来计算乘积序列 $Y=X_1\cdots X_l$ 的自相关函数.

由于 $R_Y(\tau)=T+4R'_Y(\tau)-4W_H(Y)$,其中 $T=\prod_{i=1}^{l}P_i$,$W_H(Y)=\prod_{i=1}^{l}(2^{r_i-1})$,$R'_Y(\tau)=\prod_{i=1}^{l}R'_{X_i}(\tau)$,

$$R_{X'_i}(\tau)=W_H(X_i)-\frac{P_i-R_{X_i}(\tau)}{4}=\begin{cases}2^{r_i-1}, & \tau\equiv 0 \bmod P_i,\\ 2^{r_i-2}, & \tau\not\equiv 0 \bmod P_i.\end{cases}$$

注意:

Ⅰ. 对 Y 而言,其周期为 $T=\prod_{i=1}^{l}P_i$,故对每一个 X_i 而言,其自相关函数 $R_{X_i}(\tau)$ 可在$(0,P_i)$ 而外按周期 P_i 拓展,直至 $P_1P_2\cdots P_l-1$.

Ⅱ. 在计算 $R_Y(\tau)$ 时,应注意到 τ 共有以下 $l+1$ 种情况:(1) $\tau\equiv 0 \bmod (P_1P_2\cdots P_l)$. (2) 对于某一个 j_1,$\tau\not\equiv 0 \bmod P_j$,而$\tau\equiv 0 \bmod \left(\prod_{i\neq j}P_i\right)$. (3) 对于某二个 j_1,j_2,$j_1\neq j_2$,$\tau\not\equiv 0 \bmod P_{j_1}$ 且$\tau\not\equiv 0 \bmod P_{j_2}$,而$\tau\equiv 0 \bmod \left(\prod_{i\neq j_1,j_2}P_i\right)$,$\cdots$,$(l+1)$ 对于一切的$i=1,2,\cdots,l$,$\tau\not\equiv 0 \bmod P_i$.

因此,可以得到 $R'_Y(\tau)$ 的 $l+1$ 个值.

$$R'_Y(\tau)=\prod_{i=1}^{l}R'_{X_i}(\tau)=\begin{cases}\prod_{i=1}^{l}(2^{r_i-1}), & \tau\equiv 0 \bmod P_1P_2\cdots P_l,\\ 2^{-1}\prod_{i=1}^{l}(2^{r_i-1}), & \tau\not\equiv 0 \bmod P_j \text{ 且 } \tau\equiv 0 \bmod \prod_{i\neq j}P_i,\\ 2^{-2}\prod_{i=1}^{l}(2^{r_i-1}), & \tau\not\equiv 0 \bmod P_{j_1},\tau\not\equiv 0 \bmod P_{j_2},j_1\neq j_2,\\ & \text{且 } \tau\equiv 0 \bmod \prod_{i\neq j_1,j_2}P_i,\\ \vdots & \\ 2^{-l}\prod_{i=1}^{l}(2^{r_i-1}), & \tau\not\equiv 0 \bmod P_i,\quad i=1,2,\cdots,l.\end{cases}$$

综上所述,可以得到如下定理.

定理 3 设 $X_i=(x_n^{(i)})_{n=0}^{\infty}$,$i=1,2,\cdots,l$ 是周期为 $P_i=2^{r_i}-1$ 的 l 个 m 序列,进一步假设 $(P_i,P_j)=1$,$i\neq j$,于是乘积序列 $Y=X_1X_2\cdots X_l$ 具有周期 $T=\prod_{i=1}^{l}P_i$,并且

$$(1)\ R_Y(\tau)=\begin{cases}T, & \tau\equiv 0 \bmod P_1P_2\cdots P_l,\\ T+(2^{2-1}-2^2)\prod_{i=1}^{l}(2^{r_i-1}), & \tau\not\equiv 0 \bmod P_j,\ \tau\equiv 0 \bmod \prod_{i\neq j}P_i,\\ T+(2^{2-2}-2^2)\prod_{i=1}^{l}(2^{r_i-1}), & \tau\not\equiv 0 \bmod P_{j_1},\ \tau\not\equiv 0 \bmod P_{j_2},\ j_1\neq j_2,\\ & \text{且 } \tau\equiv 0 \bmod \prod_{i\neq j_1,j_2}P_i,\\ \vdots & \\ T+(2^{2-l}-2^2)\prod_{i=1}^{l}(2^{r_i-1}), & \tau\not\equiv 0 \bmod P_i,\quad i=1,2,\cdots,l,\end{cases}$$

$$(2)\ W_H(Y)=\prod_{i=1}^{l}W_H(X_i)=\prod_{i=1}^{l}(2^{r_i-1}).$$

由上述讨论,得到的结果为:在上述假定下,任意 l 个 m 序列的乘积序列,其自相关函数永远是 $l+1$ 值函数,且其主峰值 $R_Y(0)$ 很高.

3 结束语

非线性移位寄存器序列由于它的良好特性一直受到通信、密码学、导航等领域的高度重视.笔者给出了基于任意有限多个线性移位寄存器与一个与门逻辑构成的非线性组合器生成的非线性乘积序列的自相关函数的完整表述,同时又给出了计算这种序列在一个周期内的 Hamming 重量的计算公式.笔者只给出了与门逻辑输出的乘积序列的相关特性,而对于一般的非线性组合序列,即其反馈逻辑函数还具有模 2 和的运算的反馈输出序列的相关特性值得进一步研究,文中的结果可由 GF(2)推广到 GF(q)中.

参考文献:

[1] Golomb S W, Gong G. Signal Designs with Good Correlation: for Wireless Communications, Cryptography and Radar Applications[M]. Cambridge: Cambridge University Press, 2005.

[2] Groth E J. Generation of Binary Sequences with Controllable Complexity[J]. IEEE Trans on Information Theory, 1971, 17(3): 288-296.

[3] Key E L. An Analysis of the Structure and Complexity of Nonlinear Binary Sequence Generators [J]. IEEE Trans on Inform Theory, 1976, 22(6): 732-736.

[4] Kalouptsidis N, Manolarakis M. Sequences of Linear Feedback Shift Registers with Nonlinear Feed-forward Logic [C]// Proceedings of IEEE. [s.l.]: IEEE, 1983, 16: 174-176.

[5] Ding C, Helleseth T, Martinsen H. New Families of Binary Sequences with Optimal Three-level Autocorrelation[J]. IEEE Trans on Information Theory, 2001, 47(1): 428-433.

[6] Helleseth T, Gong G. New Nonbinary Sequences with Ideal Two-level Autocorrelation[J]. IEEE Trans on Information. Theory, 2002, 48(11): 2 868-2 872.

(编辑:齐淑娟)