

## 伪随机序列和阵列的分层高速生成<sup>1</sup>

施文洪 陈进光

(福州大学无线电工程系 福州 350002)

**摘 要** 本文提出了一种新型的高速生成伪随机序列和伪随机阵列的分层结构。该结构的原理是基于一种新的概念——多次插排, 它是一般的序列插排(采样)的推广。该结构的核心是一个低速的线性反馈移位寄存器和一些分层排列的高速时分多路器。这种新的结构比作者以前提出的各种生成结构的生成速度都要高得多。

**关键词** 伪随机序列, 伪随机阵列, 高速生成, 序列插排

**中图分类号** TN911

### 1 引 言

由于技术上的原因, 我们希望能够高速生成伪随机序列 (PRS) 和伪随机阵列 (PRA)。众所周知, 由一线性反馈移位寄存器 (LFSR) 可以很容易地生成 PRS。但是在某些应用中, 我们需要非常高速地生成 PRS, 要求的生成速度超出了 LFSR 所能达到的范围。为此, Surböck 和 Weinrichter<sup>[1]</sup> 提出了一种结构, 可以高于 LFSR 移位脉冲的速度生成 PRS。这种方案的主要思想是由一些短的基序列的插排来形成原序列。这种结构包含一个低速 LFSR 和一个高速时分多路器 (TDM)。将上述思想推广到序列的非完全采样 (improper decimation) 这样一个一般概念, 就得到了非完全采样情形下, 采样序列间的相位关系<sup>[2]</sup>。将此结果应用于 PRA, 就得到了 PRA 中列与列之间的相位关系, 并由此得到一种简单结构, 可按行生成 PRA<sup>[2]</sup>。

本文中, 首先将序列采样的概念推广到多次插排 (Multidecimation) 概念, 并且发现, 伪随机序列经过非完全采样, 得到的采样序列, 往往还可以再进行若干次非完全采样, 即多次采样, 多次采样的结果, 总可以获得一个无法继续分解的基序列。将上述过程颠倒过来, 由最后获得的基序列分层多次插排, 即可恢复原序列。由此结论, 我们首次提出了一种分层结构 (Hierarchical Structure), 可以非常高的速度生成 PRS。这个结构也适于生成一般的 LFSR 序列。其次, 由于 PRA 的每一列均为一 PRS, 且移位等价<sup>[2]</sup>, 于是将这种分层结构用于文献 [2] 中生成 PRA 的结构, 又得到了一种崭新的高速生成 PRA 的分层结构。这种分层结构比作者以前提出的各种生成结构<sup>[2,3]</sup> 的生成速度都要高得多。

<sup>1</sup> 1994-07-29 收到, 1995-05-12 定稿  
福建省科委基金资助项目

## 2 生成 PRS 的分层结构

令  $h(x) = \sum_{i=1}^m h_i X^i$  为一个  $m$  阶二进制不可约多项式。记

$$\mathbf{a} = a_0, a_1, \dots, a_{n-1}, \dots \quad (1)$$

是周期为  $n = 2^m - 1$ ，对应于  $h(x)$  的非零二进制序列。 $\mathbf{a}$  的  $D$  变换可表示为

$$F(D) = 1/\tilde{h}(D), \quad (2)$$

其中  $\tilde{h}(D)$  是  $h(D)$  的互反多项式。

下面，设  $n$  非素，于是  $n$  可分解为一串素数

$$n = \prod_{i=1}^k q_i, \quad k \geq 2, \quad (3)$$

其中  $q_i (i = 1, \dots, k)$  均为素数。不失一般性，设

$$q_1 \geq q_2 \geq \dots \geq q_k, \quad (4)$$

令

$$G_j = \prod_{i=1}^j q_i, \quad j = 1, \dots, k, \quad (5)$$

则显然

$$n = G_k. \quad (6)$$

考虑  $\mathbf{a}$  的均匀采样

$$\mathbf{a}[q, t] = a_t, a_{t+q}, a_{t+2q}, \dots \quad (7)$$

众所周知， $\mathbf{a}[q, n]$  具有如下性质：

**性质** 设  $\mathbf{a}[q, t]$  非零，则  $\mathbf{a}[q, t]$  的周期为  $n' = n/(q, n)$ ，且由多项式  $A_q(x)$  生成。其中  $A_q(x)$  为  $\alpha^q$  的最小多项式，而  $\alpha$  为  $h(x)$  的一个根。

(1) 设  $q = q_1$ ，且  $0 \leq t \leq q_1 - 1$ ，则  $\mathbf{a}[q_1, t]$  的周期为  $n_1 = n/q_1$  且相应的  $D$  变换可写为

$$F_t^{q_1}(D) = P_t^{q_1}(D)/A_{q_1}(D). \quad (8)$$

此时，若在  $\mathbf{a}[q_1, t]$  的每个元素之间加上  $(q_1 - 1)$  个零，我们可得到一个新的扩展序列，对应的  $D$  变换为

$$F_t^{q_1}(D^{q_1}) = P_t^{q_1}(D^{q_1})/A_{q_1}(D^{q_1}), \quad t = 0, \dots, q_1 - 1, \quad (9)$$

其周期为  $q_1 \cdot n_1 = n$ 。将  $F_t^{q_1}(D^{q_1})$  向右循环移  $t$  位, 可得到  $q_1$  个移位的扩展序列

$$D^t \cdot F_t^{q_1}(D^{q_1}), \quad t = 0, \dots, q_1 - 1.$$

将这些移位后的扩展序列相加, 即可恢复原序列  $a$ , 于是有

$$F(D) = 1/\tilde{h}(D) = \sum_{t=0}^{q_1-1} D^t \cdot F_t^{q_1}(D^{q_1}). \quad (10)$$

将 (9) 式代入 (10) 式, 并注意到  $q_1 = G_1$ , 可得

$$\begin{aligned} 1/\tilde{h}(D) &= [1/A_{q_1}(D^{q_1})] \cdot \sum_{t=0}^{q_1-1} D^t \cdot P_t^{q_1}(D^{q_1}) \\ &= [1/A_{G_1}(D^{G_1})] \cdot \sum_{t=0}^{q_1-1} D^t \cdot P_t^{q_1}(D^{G_1}). \end{aligned} \quad (11)$$

(2) 同理, 我们可对  $a[q, t]$  再进行间隔为  $q_2$  的非完全采样。将采样后所得序列进行类似的扩展 (在每个元素之间插入  $(q_2 - 1)$  个零) 和循环移位后再相加, 也可恢复原序列  $a[q, t]$ 。因而, 我们有

$$1/A_{G_1}(D) = [1/B_{q_2}(D^{q_2})] \cdot \sum_{j=0}^{q_2-1} D^j \cdot P_j^{q_2}(D^{q_2}), \quad (12)$$

其中  $B_{q_2}(D)$  为  $\beta^{q_2}$  的最小多项式, 而  $\beta$  为  $A_{G_1}(D)$  的一个根。容易证明,  $\beta^{q_2}$  和  $\alpha^{G_2} = (\alpha^{q_1})^{q_2}$  有相同的最小多项式, 即

$$B_{q_2}(D) = A_{G_2}(D). \quad (13)$$

将 (13) 式代入 (12) 式, 并将  $D$  换成  $D^{G_1}$ , 可得

$$\begin{aligned} 1/A_{G_1}(D^{G_1}) &= 1/A_{G_2}(D^{G_1 \cdot q_2}) \cdot \sum_{j=0}^{q_2-1} D^{jG_1} \cdot P_j^{q_2}(D^{G_1 \cdot q_2}) \\ &= 1/A_{G_2}(D^{G_2}) \cdot \sum_{j=0}^{q_2-1} D^{jG_1} \cdot P_j^{q_2}(D^{G_2}). \end{aligned} \quad (14)$$

将 (14) 式代入 (11) 式, 可得

$$F(D) = [1/A_{G_2}(D^{G_2})] \cdot \sum_{j=0}^{q_2-1} D^{jG_1} \cdot P_j^{q_2}(D^{G_2}) \cdot \sum_{t=0}^{q_1-1} D^t \cdot P_t^{q_1}(D^{G_1}). \quad (15)$$

(3) 重复上述过程, 最后可得如下结果:

$$F(D) = [1/A_{G_{k-1}}(D^{G_{k-1}})] \cdot \prod_{j=1}^{k-1} \sum_{t=0}^{q_j-1} D^{t \cdot G_{j-1}} \cdot P_t^{q_j}(D^{G_j}), \quad (16)$$

式中  $G_0 \triangleq 1$ ,

$$1/A_{G_j}(D) = [1/A_{G_{j+1}}(D^{q_{j+1}})] \cdot \sum_{t=0}^{q_{j+1}-1} D^t \cdot P_t^{q_{j+1}}(D^{q_{j+1}}),$$

$$j = 1, 2, \dots, k-2. \quad (17)$$

由上述过程可知, 一个 LFSR 序列, 总可经过多次采样, 而得到一个基序列, 基序列对应的生成多项式为  $A_{G_{k-1}}(D)$ 。反过来, 这个基序列按一定规律 ((17) 式) 分层多次插排即可恢复原序列。

由此结论, 我们设计出了一种全新的分层结构, 可以非常高的速度生成 LFSR 序列。这种结构的核心是一个对应于  $A_{G_{k-1}}(D)$  较低速的 LFSR 和一些分层排列的高速 TDM。而 LFSR 和 TDMs 之间的连接网络则由  $P_t^{q_j}(D)$  决定。特别地, 若  $h(x)$  为一本元多项式, 则  $\alpha$  为一  $m$  序列, 自然该结构也适于高速生成  $m$  序列。为了仔细地描述这种高速生成 LFSR 序列或  $m$  序列的分层结构, 特举如下具体例子。

**例** 给定  $h(x) = x^8 + x^6 + x^5 + x^4 + 1$ , 此时  $h(x)$  为一本元多项式, 对应序列为一周期为  $n = 2^8 - 1 = 255$  的  $m$  序列。将  $n$  进行素因子分解

$$n = 255 = 17 \times 5 \times 3$$

与 (3) 和 (4) 式比较, 我们有

$$q_1 = 17, \quad q_2 = 5, \quad q_3 = 3, \quad k = 3.$$

容易证明,  $\alpha^{G_1}$  和  $\alpha^{G_2}$  的最小多项式分别为

$$A_{G_1}(D) = D^4 + D + 1, \quad (18)$$

$$A_{G_2}(D) = D^2 + D + 1. \quad (19)$$

现在由 (11) 式, 有

$$\begin{aligned} \sum_{t=0}^{16} D^t \cdot P_t^{17}(D^{17}) &= A_{17}(D^{17}) / \bar{h}(D) \\ &= D^{60} + D^{56} + D^{55} + D^{54} + D^{50} + D^{47} + D^{45} + D^{44} + D^{43} + D^{36} \\ &\quad + D^{35} + D^{32} + D^{29} + D^{26} + D^{25} + D^{23} + D^{22} + D^{21} + D^{18} + D^{12} \\ &\quad + D^{10} + D^9 + D^8 + D^7 + D^3 + D^2 + 1 \\ &= 1 + (x + x^2)D + (1 + x^2)D^2 + (1 + x^3)D^3 + (x + x^3)D^4 + (x + x^3)D^5 \\ &\quad + x \cdot D^6 + D^7 + (1 + x)D^8 + (1 + x + x^2 + x^3)D^9 + (1 + x^2)D^{10} \\ &\quad + x^2 \cdot D^{11} + (1 + x)D^{12} + x^2 \cdot D^{13} + x \cdot D^{15} + x^2 \cdot D^{16}, \end{aligned} \quad (20)$$

式中  $x \triangleq D^{17}$ 。比较 (20) 式两边  $D^i (i = 0, \dots, 16)$  的系数, 即可得到所有  $P_i^{17}(x), (i = 0, \dots, 16)$ 。进一步, 在 (17) 式中, 取  $j = k - 2 = 1$ , 注意  $q_2 = 5$ , 并将 (18) 和 (19) 式代入, 有

$$\begin{aligned} \sum_{i=0}^4 D^i \cdot P_i^5(D^5) &= A_{G_2}(D^5)/A_{G_1}(D) \\ &= D^6 + D^3 + D^2 + D + 1 \\ &= 1 + (1 + y)D + D^2 + D^3, \end{aligned} \quad (21)$$

式中  $y \triangleq D^5$ , 比较上式两边  $D^i$  的系数, 即可确定每一  $P_i^5(y), (i = 0, \dots, 4)$ 。

现在, 由  $A_{G_2}(D)$  可确定核心 LFSR 的结构; 而  $P_i^5(y), (i = 0, \dots, 4)$  和  $P_i^{17}(x), (i = 0, \dots, 16)$  则分别决定第一层 (内层) 和第二层 (外层) 的连接网络结构; 再加上适当的时分多路器, 即可综合出所要的生成结构, 如图 1 和图 2 所示。

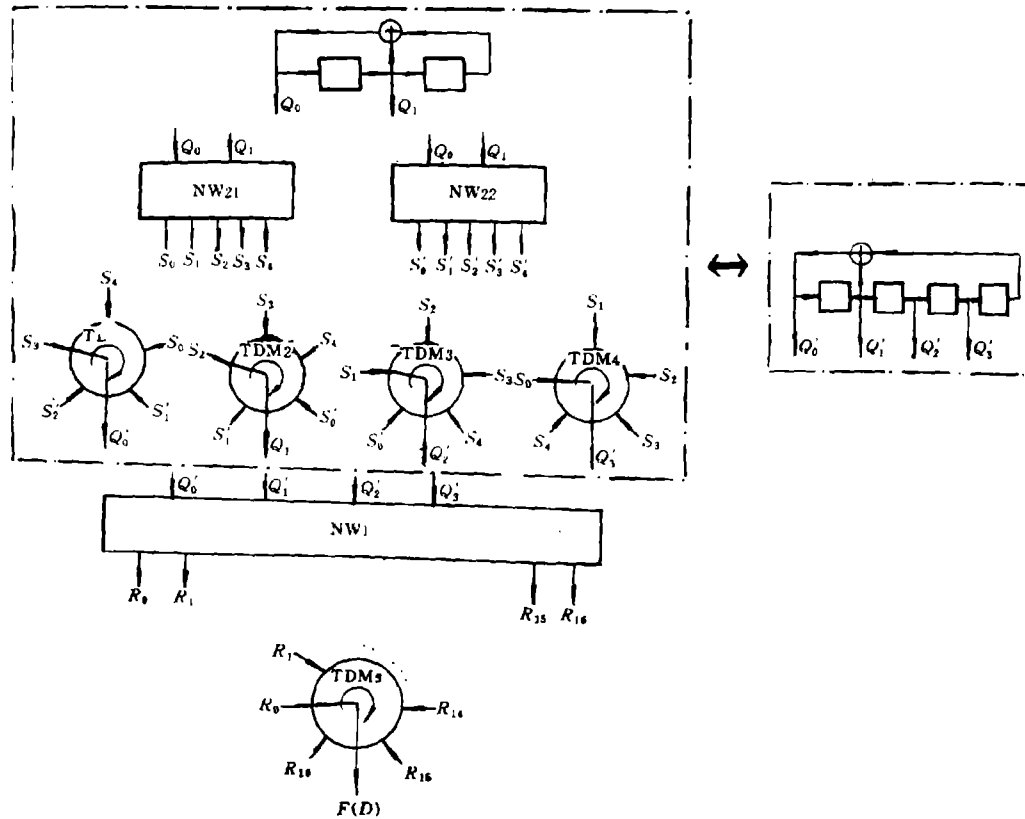


图 1 高速生成为 255 的 PRS 的分层结构

由于篇幅所限, 连接网络的具体确定过程从略。图中时分多路器 TDM1, ..., TDM4 的旋转速度是结构中 LFSR 移位脉冲速度的 5 倍, 而 TDM5 则为其 85 倍。因而, 在 LFSR 的工作速度为  $R$  时, 这个结构的工作速度为  $85R$ 。

对这个实例, 生成长为  $n = 255$  的  $m$  序列, 仅 3 个 CP 脉冲即可, 按常规方法, 则需 255 个 CP 脉冲。

这种分层结构还可应用于 PRA 的高速生成。

### 3 生成 PRA 的分层结构

在文献 [2] 中, 作者利用 PRA 列与列间的相位关系, 提出了一种结构, 可按行生成  $n_1 \times n_2$  ( $n_1 = 2^{k_1} - 1$ ) 的 PRA。这个结构的核心是一个  $k_1$  级的 LFSR。由于 LFSR 的  $k_1$  个寄存器的输出均为具有相同生成多项式、周期为  $n_1 = 2^{k_1} - 1$  的  $m$  序列, 区别仅在于相位有所不同, 因而这  $k_1$  个输出端均可由上节提出的高速分层结构来代替。将这两种结构综合起来, 并考虑到  $k_1$  个输出端的相位差, 我们就得到了一种崭新的高速生成 PRA 的分层结构。

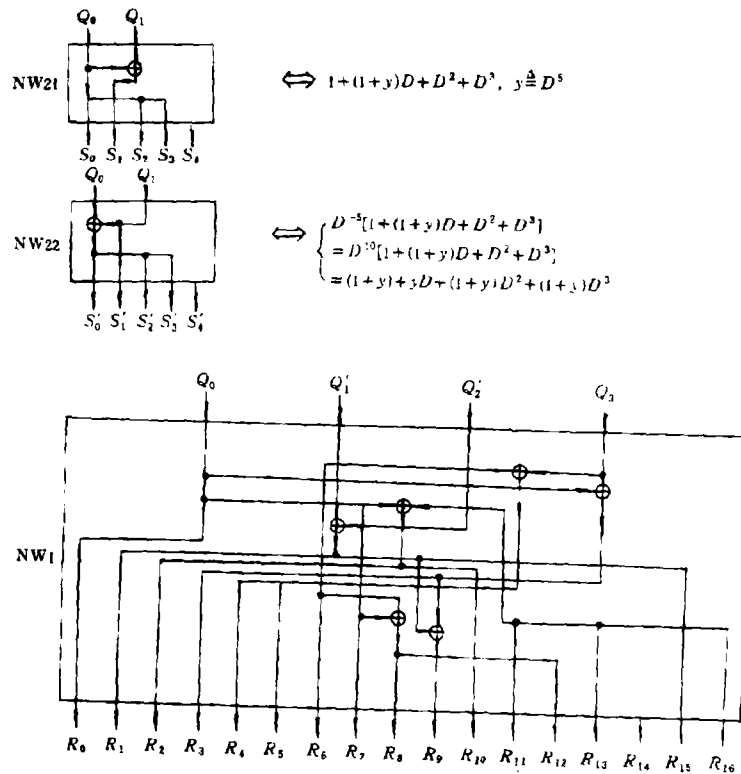


图 2 图 1 中网络 NW21, NW22 和 NW1 的细节

按此方法, 我们具体综合出了一个尺寸为  $255 \times 257$  ( $255 = 2^{k_1} - 1 = 2^8 - 1$ ) 的 PRA 的高速分层生成结构, 如图 3 所示。该结构由一个 2 级的低速 LFSR、12 个高速 TDMs 以及分层排列的一些连接网络组成。其中 TDM1, ..., TDM4 的旋转速度为该结构中 LFSR 移位脉冲速度的 5 倍, 而 TDM5, ..., TDM12 的旋转速度则为 LFSR 速度的 85 倍。连

接网络 NW1 由文献 [2] 中的 (45) 式确定, 而网络 NW21, NW22, NW31 和 NW32 则由 (16) 和 (17) 式确定。这些连接网络的细节及其具体确定过程, 限于篇幅已略去。

这个实例, 生成尺寸为  $255 \times 257$  的 PRA, 仅 3 个 CP 脉冲即可。用其它方案<sup>[2,3]</sup>, 生成同样尺寸的 PRA 则需 255 或 257 个 CP 脉冲。相比较, 分层结构的优越性不言而喻。

#### 4 结 论

本文研究了 PRS 和 PRA 的高速生成。将序列采样的概念推广到多次采样概念, 得到了 LFSR 序列的分层表达式。将 LFSR 序列的分层分解 (采样) 过程颠倒过来, 综合出了一种高速生成 LFSR 序列的新型分层结构。这种结构可直接应用于 PRS 的高速生成。接着, 将此结构应用于 PRA 的每一列, 并考虑相位差, 又获得了一种高速生成 PRA 的新型结构。这种新的结构比作者以前提出的各种生成结构的生成速度都要高得多。在具体实现这些分层结构时, 各高速时分多路器的同步和延时等问题, 将另文阐述。

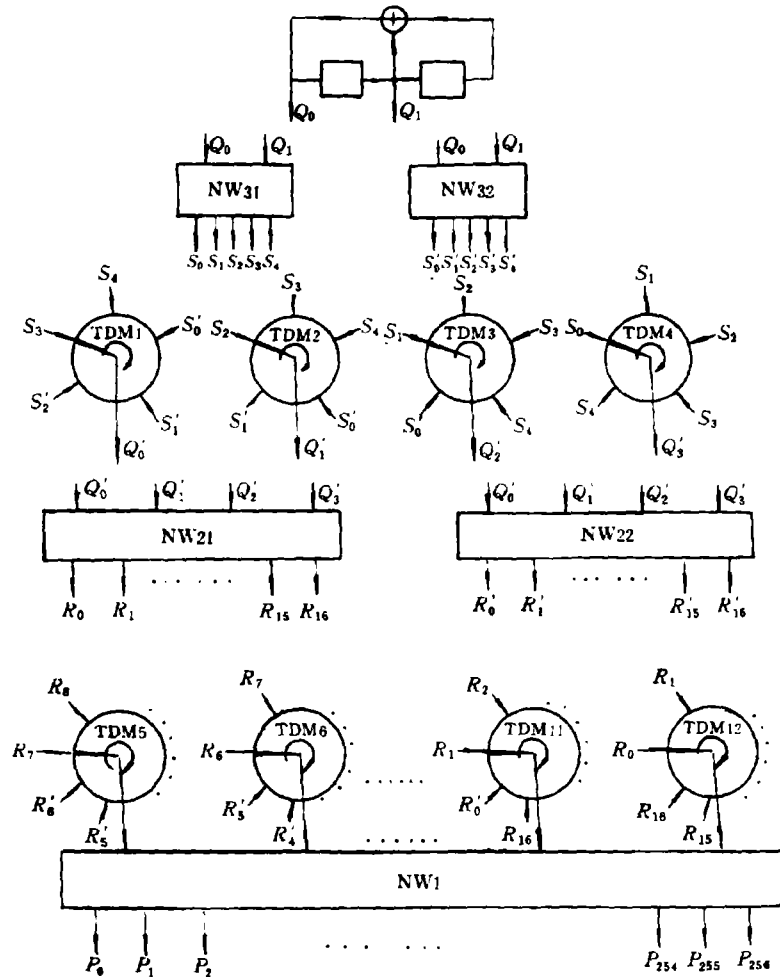


图 3 高速生成  $255 \times 257$  的 PRA 的分层结构

## 参 考 文 献

- [1] Surböck F, Weinrichter H. IEEE Trans. on IT, 1978, IT-24(2): 386-389.
- [2] 施文洪, 陈进光. 通信学报, 1989, 10(4): 82-85.
- [3] Shi Wenhong, Chen Jinguang. Recurrences of pseudorandom array and its implementation. Proc. ICCT'87, Nanjing: 1987, 698-701.

HIGH SPEED HIERARCHICAL STRUCTURES FOR GENERATING  
PSEUDO-RANDOM SEQUENCES AND ARRAYS

Shi Wenhong     Chen Jinguang

*(Department of Radio Engineering, Fuzhou University, Fuzhou 350002)*

**Abstract** This paper proposes new hierarchical structures for generating pseudo-random sequences and arrays. The principle of the structures is based on a new concept—multi-interleaving, the generalization of normal sequence decimation(sampling). The kernel of the structure is a lower speed linear feedback shift register together with several high speed time-division multiplexers arranged hierarchically. These new structures have much higher speed compared with that of other schemes proposed before.

**Key words** Pseudo-random sequences, Pseudo-random arrays, High-speed generation, Sequences decimation

施文洪: 男, 1962 年生, 副教授, 硕士, 中国电子学会高级会员, 现从事通信理论、信号处理和移动通信的教学和研究工作。

陈进光: 男, 1932 年生, 教授, IEEE 高级会员, 现从事通信和电子系统的教学和研究工作。