文章编号:1004-9037(2014)03-0439-06

一种求解延迟型 m 序列线性组合的新算法

陈德宏 刘 梅

(安徽工业大学电气信息学院,马鞍山,243002)

摘要:首先讨论了求解延迟型 m 序列的线性组合关系的代数算法,通过对主 m 序列状态与延迟 m 序列之间线性关系的分析,提出用二元域线性方程组求解延迟 m 序列线性组合关系的新算法,并将其运用到 N-CDMA 移动通信系统用户掩码的分配设计中。该方法解决了大延迟长 m 序列的线性组合的求解难题,工程计算量大幅度简化。

关键词:延迟 m 序列;线性组合;掩码

中图分类号:TN961 **文献标志码**:A

New Algorithm of Multiplex Problem for Delayed m-Sequence

Chen Dehong, *Liu Mei*

(Institute of Electrical and Information Engineering, Anhui University of Technology, Ma′anshan, 243002, China)

Abstract: An algebra algorithm is discussed for solving the linear combination characteristic of delayed m-sequence. Based on the analysis of linear relationship between the status of the central m-sequence and the delayed sequence, a new algorithm, solving the multiplex problem of delayed m-sequence, is proposed by utilizing linear equations over binary finite field. The algorithm is also applied to the design of the mask of the N-CDMA mobile communication system. The algorithm provides a convenient way to solve the multiplex problem of long m-sequence in engineering calculation.

Key words: delayed m-sequence; linear combination; mask code

引 言

伪随机信号在 CDMA 通信、遥控、遥测、信息加密和卫星导航系统有着广泛的应用。m 序列作为最大长度线性反馈移位寄存器序列,是一类重要的也是目前研究最多的伪随机序列。在伪随机信号应用处理的过程中,经常需要产生相对时延不同的主 m 序列的平移等价序列,若采用原始方法(如设立一系列延时门),则由于器件组成庞大,求解过程繁琐而耗时长,这在延迟型长 m 序列实际研究中就显得很不现实。

设 A_0 是二元域 $GF(2)$上的 m 序列,用 A_i 表示序列 A_0 左移 i 位得到的新序列,序列 A_i 与 A_0 具有相同的特征多项式,即 A_i 与 A_0 具有相同的递归关系。若用集合 $G(f)$表示所有适合特征多项式 $f(x)$的序列的全体,则集合 $G(f)$中非零元素 A_i 都是 m 序列,它们具有以下性质

$$\begin{aligned} &\text{若} && A_i \in G(f), A_j \in G(f) \\ &\text{且} && i \neq j \pmod{L} \\ &\text{则} && A_i \oplus A_j = A_k, A_k \in G(f) \end{aligned} \tag{1}$$

这个性质称为 m 序列的移位相加特性,也称为自闭特性。由于 m 序列发生器各级移位寄存器的输出只是相移不同的平移等价 m 序列,通过 m 序列移位相加特性,可知延迟 m 序列可以由 m 序列发生器的各移位寄存器输出序列经模 2 和运算获得,即 m 序列的线性组合特性[1]。

m 序列线性组合特性为获得延迟 m 序列提供了便利,在长 m 序列的设计中具有经济灵活的实用价值。对于一个特定的延迟 k 位 m 序列是由 n 级移存器的哪几级输出序列模 2 和得到的问题,在理论上一直没有一个确定性的普遍公式,文献[2-4]利用有限域的代数法将延迟 k 位 m 序列分解为几个低延迟的 m 序列模 2 和,之后再进行多次迭

收稿日期:2012-01-11;修订日期:2013-06-09

代,直至分解为几个 n 级以内延迟 m 序列的线性模 2 和。

本文首先分析了 m 序列线性组合关系的代数迭代求解算法,针对该算法在解决多抽头大延迟长 m 序列时,迭代过程冗长繁杂、工程上难以实现等问题,利用主 m 序列状态与延迟 m 序列在二元域上存在的线性关系,提出了用求解二元域线性方程组获得延迟 m 序列线性组合关系的方法,工程计算量得到大幅简化,并将其成功运用到 N-CDMA 移动通信系统用户掩码的分配设计中,同时通过对特定 2^{41} 位的大延迟长码掩码的求解,定量分析了采用传统代数迭代法的计算复杂度。

1 m 序列线性组合关系求解的代数算法

有限域上多项式是研究伪随机序列的重要数学工具。代数算法就是由二元域 m 序列特征多项式 $f(x)$ 和延迟算子多项式 x^k,利用在二元域上定义的多项式的模 2 运算法则求解 m 序列线性组合关系[5]。

m 序列 A_0 可以写成如下形式:$A_0=\{a_0 \quad a_1 \quad a_2 \quad \cdots \quad a_{L-1}\cdots\}$,其周期 $L=2^n-1$,特征多项式为

$$f(x)=\sum_{i=0}^{n}c_i x^i,\text{其中 } c_0=c_n=1 \tag{2}$$

由于集合 $G(f)$ 表示所有适合特征多项式 $f(x)$ 的延迟序列全体,将 $G(f)$ 用两两不同的元素表示出来,有

$$G(f)=\{\theta \quad A_0 \quad A_1 \quad A_2 \quad \cdots \quad A_{L-1}\} \tag{3}$$

集合 $G(f)$ 可看作一个含有 $L+1$ 个元素的有限域,其中 $\theta=\{0 \quad 0 \quad 0 \quad \cdots \quad 0\}$ 是满足特征多项式 $f(x)$ 零序列。$G(f)$ 中的非零元素组成周期 L 的循环群,非零元素就是所求的延迟 m 序列,任一个非零元素 A_k 均可表示成一本原元 α 的幂。

令 $\alpha^0=A_0=1,\alpha=A_1$,则 $G(f)=\{\theta \quad 1 \quad \alpha \quad \alpha^2 \quad \cdots \quad \alpha^{L-1}\}$。本原元 α 是 m 序列特征多项式 $f(x)$ 的根,即 $f(\alpha)=0$。由于定义 A_k 为延迟的左移 m 序列,故 α 应该是 $f(x)$ 的互反序列多项式 $\tilde{f}(x)$ 的根

$$\begin{aligned}\tilde{f}(x)&=x^n\cdot f(x^{-1})\\ \tilde{f}(\alpha)&=\alpha^n\cdot f(\alpha^{-1})=0\end{aligned} \tag{4}$$

由于式(2)中 $f(x)$ 可以写成

$$f(x)=1+\sum_{i=1}^{n-1}C_i x^i+x^n \tag{5}$$

故 $f(x)$ 的互反多项式 $\tilde{f}(x)$ 为

$$\tilde{f}(x)=x^n\cdot f(x^{-1})=1+\sum_{i=1}^{n-1}C_{n-i}x^i+x^n$$

由 $\tilde{f}(\alpha)=0$ 得

$$\alpha^n=1+\sum_{i=1}^{n-1}C_{n-i}\alpha^i \tag{6}$$

由于在二元域 GF(2) 上,多项式具有性质

$$[f(x)]^{2^t}=f(x^{2^t}) \quad t=0,1,2,3,\cdots \tag{7}$$

可得

$$(\alpha^n)^{2^t}=1+\sum_{i=1}^{n-1}C_{n-i}\alpha^{i\cdot 2^t} \tag{8}$$

这里 $2^t\leqslant k/n$,t 在运算中选其满足条件的最大值。

令 $2^t=p$,式(8)可以表示为

$$(\alpha^n)^p=1+\sum_{i=1}^{n-1}C_{n-i}\alpha^{ip}$$

两边同乘以 α^{k-np} 得

$$\alpha^k=\alpha^{k-np}+\sum_{i=1}^{n-1}C_{n-i}\alpha^{k-np+ip}$$

再令 $k=np+r$,得

$$\alpha^k=\alpha^r+\sum_{i=1}^{n-1}C_{n-i}\alpha^{r+ip} \tag{9}$$

式(9)表明,α^k 可以分解为 n 个幂次低于 k 的 α 幂的线性组合。为了将 α^k 最终分解为 $1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$ 的线性组合,将式(9)中 α^r 以及满足 C_{n-i} 的 α^{r+ip} 继续按相同方法迭代分解为较低幂形式,同时将 α 的幂次相同的项相互抵消掉,直至将 α 的各次幂分解为低于幂次 n 为止。下面用代数算法举例。

例 1 已知特征多项式为 $f(x)=1+x^4+x^5+x^6+x^8$ 的 8 级 m 序列,求与移存器输出延迟 60 比特的移位序列的组合内容。

解:由 $f(x)=x^8+x^4+x^3+x^2+1$

得 $\alpha^8=\alpha^4+\alpha^3+\alpha^2+1$

由式(9)分解式为 $\alpha^k=\alpha^r+\alpha^{r+4p}+\alpha^{r+3p}+\alpha^{r+2p}$

现在求解 α^{60}

因为 $60=2^2\times 8+28$ $r=28,p=2^2=4$

所以 $\alpha^{60}=\alpha^{28}+\alpha^{44}+\alpha^{40}+\alpha^{36}$

因为 $28=2^1\times 8+12$ $44=2^2\times 8+12$

$40=2^2\times 8+8$ $36=2^2\times 8+4$

所以 $\alpha^{60}=\alpha^{28}+\alpha^{44}+\alpha^{40}+\alpha^{36}=(\alpha^{12}+\alpha^{20}+\alpha^{18}+\alpha^{16})+(\alpha^{12}+\alpha^{28}+\alpha^{24}+\alpha^{20})+(\alpha^8+\alpha^{24}+\alpha^{20}+\alpha^{16})+(\alpha^4+\alpha^{20}+\alpha^{16}+\alpha^{12})=\alpha^4+\alpha^8+\alpha^{12}+\alpha^{16}+\alpha^{18}+\alpha^{28}=$

$(8=2^0\times 8+02,\quad 28=2^1\times 8+12)$

$\alpha^4+(1+\alpha^4+\alpha^3+\alpha^2)+\alpha^{12}+\alpha^{16}+\alpha^{18}+(\alpha^{12}+\alpha^{20}+\alpha^{18}+$

$$\alpha^{16})=\alpha^2+\alpha^3+\alpha^{20}+1=$$
$$(20=2^1\times 8+4)$$
$$\alpha^2+\alpha^3+(\alpha^4+\alpha^{12}+\alpha^{10}+\alpha^8)+$$
$$1=\alpha^2+\alpha^3+\alpha^4+\alpha^8+(\alpha^4+\alpha^8+$$
$$\alpha^7+\alpha^6)+(\alpha^2+\alpha^6+\alpha^5+\alpha^4)+1=$$
$$1+\alpha^3+\alpha^4+\alpha^5+\alpha^7$$

分解结果表明，要得到相对于主 m 序列延迟 60 比特的延迟 m 序列，由第 1,3,4,5,8 级移存器输出序列进行模 2 和。

上述给出了求解延迟 m 序列线性组合关系的代数分解法，分析其算法的复杂度，可以发现：

(1)随着级数 n 的增加，对于大延迟 k 的分解复杂度急剧增加。

(2)若特征多项式的项数为 s，对于 α^k，分解为 α 的各次幂的数目会有 $s-1$ 项，当 s 较大时，随分解幂次的降低，分解的项数将不断增加。

(3)若特征多项式存在低幂次项，α^k 分解后的最高幂次衰减速度较慢，迭代分解复杂度也大大增加。

文献[6]用两两结合运算对代数分解法进行了改进，简化了计算，但没有从根本上降低在大级数多项数特征多项式条件下的分解复杂度。文献[7]把延迟 m 序列的线性组合问题映射成互反序列产生器状态，由推导互反序列产生器的状态递推式，来进行 m 序列组合分析的递推算法，但是任一延迟的 m 序列的线性组合需要由前一位递推得来，对于长 m 序列来说运算量依然庞大，工程上难以实现。

2　延迟 m 序列线性组合特性的分析

图 1 为一个 n 级 m 序列线性反馈移存器及其线性组合产生延迟 m 序列的原理图。m 序列产生器 n 位状态和掩码 $d_1\ d_2\ d_3\cdots d_n$ 相与运算，当 $d_i=1(i=1,2,3,\cdots,n)$ 时，对应的第 i 级移存器的抽头接入模 2 加法器；当 $d_i=0$ 时则不接入，延迟 m 序列即为所有 $d_i=1$ 的移存器输出 m 序列线性组合的全体。

设 $A_0=\{a_0\quad a_1\quad a_2\quad\cdots\quad a_{L-1}\quad\cdots\}$ 是 n 级简单式移位寄存器(Simple shift register generator, SSRG)结构输出的主 m 序列，移存器的初始状态为 $S_0=\{a_0\quad a_1\quad a_2\quad\cdots\quad a_{n-2}\quad a_{n-1}\}$，每来一个时钟脉冲，移存器的状态顺次由 S_0 变为 S_1，$S_2,S_3,\cdots,S_{L-1},\cdots$。因此 m 序列也可以用状态序列 $S=\{S_0\quad S_1\quad S_2\quad\cdots\quad S_{L-1}\quad\cdots\}$ 表示。其中，

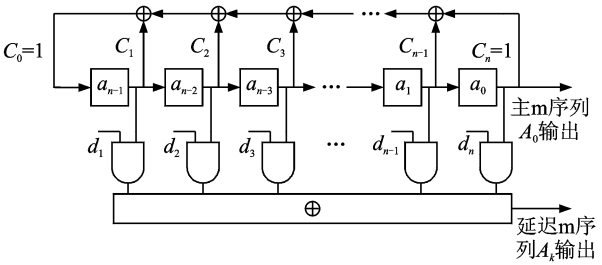

图 1　线性组合特性产生延迟 m 序列原理图

Fig. 1　Schematic diagram of producing delayed m-sequence

S_i 是由序列 A_0 中的连续 n 个元素构成，即 $S_i=\{a_i\quad a_{i+1}\quad a_{i+2}\quad\cdots\quad a_{i+n-2}\quad a_{i+n-1}\}$，由于 $L=2^n-1$ 为 m 序列周期，故 $S_L=S_0$。

序列 A_0 中任意 n 个连续的状态 $S_i,S_{i+1},S_{i+2},\cdots,S_{i+n-2},S_{i+n-1}(i\geqslant 0)$ 在 GF(2)上线性无关[8]，而 n 个元素的组合总数为 $C_n^1+C_n^2+C_n^3+\cdots+C_n^{n-1}+C_n^n=2^n-1$，可得 m 序列线性组合理论：$n$ 级 m 序列的 2^n-1 个平移等价序列即为 n 个相邻平移序列线性组合的全体。

由图 1 可知，第 i 时刻，主 m 序列状态向量 $\boldsymbol{S}_i$ 与掩码向量$[d_n\quad d_{n-1}\quad\cdots\quad d_2\quad d_1]$相与后，再模 2 加得到延迟 k 位 m 序列第 i 时刻的码元 a_{k+i}。即

$$a_{k+i}=a_i d_n\oplus a_{i+1}d_{n-1}\oplus a_{i+2}d_{n-2}\oplus\cdots\oplus a_{i+n-1}d_1 \tag{10}$$

式(10)可表示成

$$a_{k+i}=\boldsymbol{S}_i\cdot[d_n\quad d_{n-1}\quad d_{n-2}\quad\cdots\quad d_1]^{\mathrm{T}}=$$
$$[a_i\quad a_{i+1}\quad a_{i+2}\quad\cdots\quad a_{i+n-1}]\cdot\begin{bmatrix}d_n\\d_{n-1}\\d_{n-2}\\\vdots\\d_1\end{bmatrix} \tag{11}$$

根据式(11)，只要已知 n 个线性无关的主 m 序列状态向量及 n 个对应的延迟 k 位 m 序列输出码元，即可通过解线性方程组，求得线性组合关系的 n 维掩码向量。

为了方便获取方程组参数，令 $i=0$，即可从主 m 序列前 $2n$ 个码元获得连续的 n 个线性无关的 m 序列状态向量 $\boldsymbol{S}_0,\boldsymbol{S}_1,\boldsymbol{S}_2,\cdots,\boldsymbol{S}_{n-2},\boldsymbol{S}_{n-1}$，这 n 个状态向量所对应的 n 个延迟 k 位 m 序列码元 a_k，$a_{k+1},a_{k+2},\cdots,a_{k+n-2},a_{k+n-1}$ 即为主 m 序列第 k 时刻开始的 n 个输出码元。由式(11)及上述参数列出 n 元方程组

$$
\begin{aligned}
a_k &= a_0 d_n \oplus a_1 d_{n-1} \oplus \cdots \oplus a_{n-2} d_2 \oplus a_{n-1} d_1 \\
a_{k+1} &= a_1 d_n \oplus a_2 d_{n-1} \oplus \cdots \oplus a_{n-1} d_2 \oplus a_n d_1 \\
a_{k+2} &= a_2 d_n \oplus a_3 d_{n-1} \oplus \cdots \oplus a_n d_2 \oplus a_{n+1} d_1 \\
&\vdots \\
a_{k+n-2} &= a_{n-2} d_n \oplus a_{n-1} d_{n-1} \oplus \cdots \oplus a_{2n-4} d_2 \oplus \\
&\quad a_{2n-3} d_1 \\
a_{k+n-1} &= a_{n-1} d_n \oplus a_n d_{n-1} \oplus \cdots \oplus a_{2n-3} d_2 \oplus \\
&\quad a_{2n-2} d_1
\end{aligned} \tag{12}
$$

式(12)中的这种线性关系对应写成矩阵形式

$$
\begin{bmatrix}
a_0 & a_1 & a_2 & \cdots & a_{n-2} & a_{n-1} \\
a_1 & a_2 & a_3 & \cdots & a_{n-1} & a_n \\
a_2 & a_3 & a_4 & \cdots & a_n & a_{n+1} \\
\vdots & \vdots & \vdots & & \vdots & \ddots \\
a_{n-2} & a_{n-1} & a_n & \cdots & a_{2n-4} & a_{2n-3} \\
a_{n-1} & a_n & a_{n+1} & \cdots & a_{2n-3} & a_{2n-2}
\end{bmatrix}
\begin{bmatrix} d_n \\ d_{n-1} \\ d_{n-2} \\ \vdots \\ d_2 \\ d_1 \end{bmatrix} =
\begin{bmatrix} a_k \\ a_{k+1} \\ a_{k+2} \\ \vdots \\ a_{k+n-2} \\ a_{k+n-1} \end{bmatrix} \tag{13}
$$

利用矩阵的初等变换求解形如 $\boldsymbol{AX}=\boldsymbol{b}$ 形式的式(13)中线性方程组。若 $\boldsymbol{A}$ 可逆，方程组 $\boldsymbol{AX}=\boldsymbol{b}$ 的增广矩阵($\boldsymbol{A}$,$\boldsymbol{b}$)经初等行变换可以化为($\boldsymbol{E}$,$\boldsymbol{A}^{-1}\boldsymbol{b}$)，其中 $\boldsymbol{E}$ 为单位阵，$\boldsymbol{A}^{-1}\boldsymbol{b}$ 就是方程组的解，即求得的掩码向量。由于在二元域中，线性方程组进行的是模 2 运算，故矩阵亦采用模 2 运算进行矩阵初等行变换。

例 2 特征多项式为 $f(x)=1+x^4+x^5+x^6+x^8$ 的 8 级移存器的输出的主 m 序列为

1 0 0 0 0 1 0 1 1 1 1 0 0 0 1 1 0 1 0 0 0 0 0 0 0 1 0 0 0 1 1 1 0 0 0 1 0 0 1 0 1 1 1 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 1 1 0 1 1 1 0 0 1 0 0 0 0 0 1 0 1 0 1 1 0 1 1 0 1 0 1 1 0 0 1 0 1 1 0 0 0 0 1 1 1 1 1 0 1…

求与移存器输出延迟 60 Byte 的移位序列的组合内容。

从起始码元下划线取 15 个码元得到主 m 序列连续的 8 个状态，第 2 划线起始位为相对于主 m 序列延迟 60 Byte 的 m 序列的起始位置，灰色下划线处为主 m 序列连续 8 个状态对应产生的延迟 60～67 Byte 的 8 位码元且(a_{60} a_{61} a_{62} a_{63} a_{64} a_{65} a_{66} a_{67})=10111001。

根据式(12)，列出该 m 序列状态与延迟码元的线性组合关系方程，将其排成增广矩阵的形式后进行二元域的初等行变换，用模 2 运算进行矩阵单位化

$$
\begin{bmatrix}
a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & \cdots & a_{60} \\
a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & \cdots & a_{61} \\
a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 & \cdots & a_{62} \\
a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 & a_{10} & \cdots & a_{63} \\
a_4 & a_5 & a_6 & a_7 & a_8 & a_9 & a_{10} & a_{11} & \cdots & a_{64} \\
a_5 & a_6 & a_7 & a_8 & a_9 & a_{10} & a_{11} & a_{12} & \cdots & a_{65} \\
a_6 & a_7 & a_8 & a_9 & a_{10} & a_{11} & a_{12} & a_{13} & \cdots & a_{66} \\
a_7 & a_8 & a_9 & a_{10} & a_{11} & a_{12} & a_{13} & a_{14} & \cdots & a_{67}
\end{bmatrix} =
$$

$$
\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & \cdots & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & \cdots & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & \cdots & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & \cdots & 1 \\
0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & \cdots & 1 \\
1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & \cdots & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & \cdots & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & \cdots & 1
\end{bmatrix} =
$$

$$
\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & \cdots & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \cdots & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \cdots & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \cdots & 1
\end{bmatrix}
$$

经过增广矩阵的初等行变换，求得掩码向量[d_8 d_7 d_6 d_5 d_4 d_3 d_2 d_1]=[10011101]

对于 8 级 m 序列，延迟 60 位的 m 序列是由 m 序列产生器第 1,3,4,5,8 级移存器的输出序列线性组合得来，即设置掩码(d_1 d_2 d_3 d_4 d_5 d_6 d_7 d_8)=(10111001)。

3 N-CDMA 通信系统用户掩码的分配设计

基于 IS-95 标准的 N-CDMA 通信系统是 2G 时代的典型代表。N-CDMA 系统中的 PN 长码是由 42 位的掩码和 1 个 42 级线性反馈移位寄存器(Linear feedback shift register, LFSR)产生器生成。

N-CDMA 系统给每个用户分配不同的私人 42 位掩码，这个 42 级长码产生器是通过掩码确定各级移存器输出 m 序列的线性组合方式，不同的掩码值能使 m 序列产生不同相位的长码，不同的

用户使用不同相位的 PN 长码来标记各自的信道，这些长码在前向业务信道中起到数据扰乱加密的作用。在反向业务信道中，长码起到直接扩频多址的作用，PN 长码的相位随机分配且不会重复，从而区分不同的移动台和用户[9]。长码序列的特征多项式如下

$$f(x)=x^{42}+x^{41}+x^{40}+x^{39}+x^{37}+x^{36}+x^{35}+x^{32}+x^{26}+x^{25}+x^{24}+x^{23}+x^{21}+x^{20}+x^{17}+x^{16}+x^{15}+x^{11}+x^{9}+x^{7}+1 \quad (14)$$

由于该长码序列既可以由基于式(14)中特征多项式、SSRG 架构的 LFSR 产生，也可以由基于该式的互反多项式利用模块式移位寄存发生器(Multi-return shift register generator, MSRG)架构的 LFSR 产生[10]。图 2 给出了 N-CDMA 中利用 MSRG 架构的长码产生器生成不同相位长码的结构图。

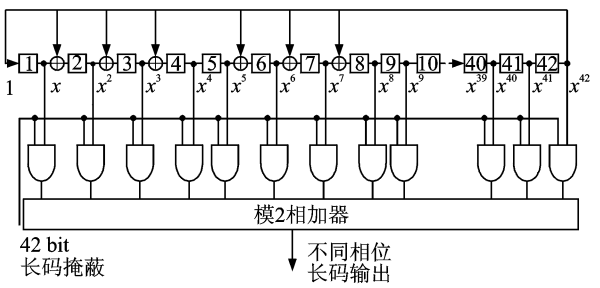

图 2　不同相位偏置的长码 MSRG 实现

Fig. 2　Long code achieved through MSRG

通常陆地移动通信环境的多径延迟小于 20 μs，为了实现多径分离，防止本地区用户的长码之间出现太大的相关值，针对速率为 1.228 8 Mcps 的长码扩频序列，不同用户长码相位间应该满足一定的相位差，即相位差码元数应大于 1.228 8 Mcps×20 μs 码片，故在工程应用上只对长码相位差满足条件的掩码进行随机分配，这样得到的私人掩码既满足多径分离对扩频地址码低相关性的要求，也能满足随机保密的要求。因此，用户掩码的分配设计需要由给定相位偏置的长码求解延迟 m 序列的线性组合关系即计算用户掩码。

下面以求解延迟半个周期(2^{41}位)长码的用户掩码为例，定量分析代数分解法的计算复杂度。由式(14)和式(9)，可得到延迟 2^{41} 位的代数分解式

$$\alpha^{2^{41}}=\alpha^{r+35p}+\alpha^{r+33p}+\alpha^{r+31p}+\alpha^{r+27p}+\alpha^{r+26p}+\alpha^{r+25p}+\alpha^{r+22p}+\alpha^{r+21p}+\alpha^{r+19p}+\alpha^{r+18p}+\alpha^{r+17p}+\alpha^{r+16p}+\alpha^{r+10p}+\alpha^{r+7p}+\alpha^{r+6p}+\alpha^{r+5p}+\alpha^{r+3p}+\alpha^{r+2p}+\alpha^{r+p}+\alpha^{r}$$

式中：$r=755\ 914\ 244\ 096$，$p=2^{35}$。

显然式(15)中分解后的这 20 项的幂均大于级数 42，需要继续按相同方法迭代多次，直至将 α 的各幂次分解为低于 42 为止。以分解后最高幂次项为例，共需要迭代分解 205 次，由于每一项的分解都会产生 20 项低次幂，理论上用迭代分解法求解延迟 2^{41} 位长码的用户掩码共需迭代 20^{205} 次，见表 1。虽然在运算中通过抵消掉部分同次幂项，实际迭代次数会小于理论值，但分解的运算量仍然相当庞大，工程上处理起来相当复杂。

表 1　代数法求解延迟 2^{41} 位长码掩码的复杂度分析

Table 1　Complexity of Algebra algorithm

最高幂迭代次数	最高幂次 $k=r+35p$	r	p	分解后总项数
1	2^{41}	755 914 244 096	2^{35}	20
2	755 914 244 096+35×2^{35}	515 396 075 520	2^{35}	20^2
3	515 396 075 520+35×2^{35}	274 877 906 944	2^{35}	20^3
⋮	⋮	⋮	⋮	⋮
204	16+35×2^0=51	9	2^0	20^{204}
205	9+35×2^0=44	2	2^0	20^{205}

若采用线性方程组求解延迟 2^{41} 位长码的用户掩码，则不受 m 序列产生器抽头数目以及延迟位数的影响，可以方便地解决延迟 m 序列线性组合的问题。首先选取任意 42 比特作为移存器初始状态，利用式(14)产生长码序列，有

111111111111111111111111111111111111111111
000000011001110101001100101010000011101010
110101101001000011101001110111001111000101…
111010110110010110011001110110110111010
000 第 2 划线起始位为相位延迟 2^{41} 位的长码位置，之间的码元在求解过程中没有运用，故省略。根据式(13)，取前 83 码元构成的连续 42 个移存器状态和这 42 个状态对应产生的延迟长码(灰色划线部分比特)列出 42×43 的增广矩阵，编写程序对该矩阵进行二元域初等化变换得到单位阵，最后一列即为产生延迟 2^{41} 位的长码掩 00111111101011111111100110011001110111100。

4　结束语

本文将矩阵初等化求解二元域线性方程组的方法应用于求解延迟 m 序列的线性组合关系，该方法相对于代数法运算复杂度大为简化，尤其对工程上难以求解的大延迟长 m 序列的线性组合关系

而言,是一种行之有效的解决方法。

参考文献:

[1] Abhijit M. On the properties of pseudo noise sequences with a simple proposal of randomness test [J]. International Journal of Electrical and Computer Engineering, 2008,3(3):676-681.

[2] Zeng Fanxin, Ge Lijia. An algorithm for cycle and add property of m-sequence[C]//The 2003 IEEE Information Theory Workshop (ITW2003). Paris, France: IEEE, 2003:119-112.

[3] Kai P Y. A simple method for the determination of feedback shift register connections for delayed maximal-length sequences [J]. Proceedings of IEEE, 1980,68(4):537-538.

[4] Miller A J, Brown A W, Mars P. A simple technique for the determination of delayed maximal length linear binary sequences[J]. IEEE Trans Computers, 1977,268(8):808-811.

[5] 张惠民.二元 m 序列自闭规律的确定及应用[J].北京邮电大学学报,1980,2:107-115.
Zhang Huimin. The closure law of binary m-sequence and its application[J]. Journal of Beijing University of Posts and Telecommunications, 1980,2:107-115.

[6] 周大华.延迟型 m 序列产生的几种方法[J].电子学报,1982,2:94-96.
Zhou Dahua. Several methods for the generation of delayed m-sequence[J]. Chinese Journal of Electronics, 1982,2:94-96.

[7] 周井泉.延迟 m 序列线性组合的递推算法[J].南京邮电学院学报,1996,16(3):95-97.
Zhou Jingquan. A recurring algorithm of multiplex problem for delayed m-sequence[J]. Journal of Nanjing Institute of Posts and Telecommunications, 1996,16(3):95-97.

[8] 万哲先.代数与编码[M].3 版.北京:高等教育出版社,2008:260-273.
Wan Zhexian. Algebra and coding[M]. Third Edition. Beijing: Higher Education Press, 2008: 260-273.

[9] TIA/EIA-95-B. Mobile station-base station compatibility standard for dual-mode spread spectrum systems[M]. Washington, America: ANSI Publication Version, 1998.

[10] Kim S C, Lee B G. Parallel scrambling techniques for multibit-interleaved multiplexing environments [C]//Proc ICC′93. Geneva: [s. n.], 1993: 1526-1530.

作者简介:陈德宏(1965-),男,副教授,研究方向:通信系统总体设计、数字语音编码、密码分析,E-mail:cdh@ahut.edu.cn;刘梅(1987-),女,硕士研究生,研究方向:信息安全。