关于M序列*：
有限域中本原元的升幂序列与M序列的关系

欧阳景正
（华南工学院）

〔提要〕本文提出了M序列的一个新定义，即利用有限域中本原元的升幂序列来定义M序列。用这种方法，很容易推导出M序列的性质。本文还给出一个用模2加法器合成M序列一个平移等价类中的全部M序列（即不同相位的M序列）的计算方法。它在设计不同相位的M序列时是有用的。本文还推导出用于M序列设计的一些关系式，并指出最多只要（n－2）个模2加法器便可得到任一相位的M序列。

* * *

二元M序列是一种伪随机码。由于它产生容易，并具有良好的自相关特性等优点，因而在数字通信、测距、定位技术、自动控制等方面都很有用。人们对M序列作过不少研究。过去都是把M序列定义为满足某些线性递归关系的线性反馈移位寄存器序列。按此，很难推导出M序列的性质。笔者经过全面研究后，提出下述新定义。

§1 M序列的定义

设F_q是有限域，它有q个元素。$f(x)$是F_q上的n阶不可约多项式。再设F_{q^n}是由$f(x)$构成的有限域。α是F_{q^n}的本原元。它可以由一个低于n阶的多项式表示，

$$\alpha = a_0 + a_1 x + a_2 x^2 + \cdots\cdots a_{n-1} x^{n-1},$$

系数a_0，a_1，……a_{n-1}是F_q中的元素。

显然，F_{q^n}可以看作是F_q上的n维向量空间。F_{q^n}的元素都可以用n维向量表示。例如α可以表成向量$(a_0, a_1, \cdots\cdots, a_{n-1})$。

设本原元α的升幂序列为$A_i(\alpha)$，

$$A_i(\alpha): \quad \alpha^{i+1}, \alpha^{i+2}, \cdots\cdots \alpha^{i+q^n-1}, \cdots\cdots \qquad (1)$$

其中 $i = 0, 1, 2, \cdots\cdots q^n - 2$。

由于α是本原元，它是q^n-1阶元素（即$\alpha^{q^n-1}=1$），因此向量序列$A_i(\alpha)$是周期序列，它的周期为q^n-1。而一周期内的元素均相异。由$A_i(\alpha)$序列的第一分量组成的序列称为对应于$A_i(\alpha)$序列的q元M序列$M_{A\alpha}(i)$，或简称q元M序列。

$$M_{A\alpha}(i): a_0^{(i+1)}, a_0^{(i+2)}, \cdots\cdots, a_0^{(i+q^n-1)} \cdots\cdots \qquad (2)$$

其中 $a_0^{(i+j)}$是向量α^{i+j}的第一个分量。

由于F_{q^n}只有q^n-1个非零元素，因此只有q^n-1种α的升幂序列。我们称这q^n-1个$A_i(\alpha)$序列（$A_0(\alpha)$，$A_1(\alpha)$，……$A_{q^n-2}(\alpha)$）为α的平移等价类。它们对应的M序列

* 本文于1977年11月上旬交给华南工学院学报编辑部，后来，又于1977年12月26日转寄到本刊编辑部。

也称为平移等价类。显然，它们是一些初相位不同的同一类M序列。

§2 M序列的主要特征

M序列的主要特征是它的移位相加性。即不同相位的M序列相加仍然是M序列。对于二元M序列，还有一个基本特点，就是一个周期内，零的个数比1的个数少一。根据这两个特点就可以马上推出二元M序列相关函数为二值函数。而二元M序列的一个主要优点也就在于它的相关函数只取两个差异较大的值。

1．M序列的移位相加性 设有两个A序列$A_i(\alpha)$、$A_j(\alpha)$，它们对应的M序列为$M_{A_\alpha}(i)$、$M_{A_\alpha}(j)$。把$A_i(\alpha)$和$A_j(\alpha)$对应的项两两相加，得到新序列$A_{i+j}(\alpha)$，

$$A_{i+j}(\alpha):\quad \alpha^{i+1}+\alpha^{j+1},\ \alpha^{i+2}+\alpha^{j+2},\ \cdots\cdots,\ \alpha^{i+q^n-1}+\alpha^{j+q^n-1}\cdots\cdots \quad (3)$$

可以改写成

$$A_{i+j}(\alpha):\quad (\alpha^i+\alpha^j)\alpha,\ (\alpha^i+\alpha^j)\alpha^2,\ \cdots\cdots,\ (\alpha^i+\alpha^j)\alpha^{q^n-1},\ \cdots\cdots\cdots \quad (4)$$

由于α是F_{q^n}的本原元，假定$i\neq j \bmod (q^n-1)$，因此元素$\alpha^i+\alpha^j$必可表成α的某一幂。设$\alpha^i+\alpha^j=\alpha^K$，$(0\leqslant K\leqslant q^n-2)$。于是$A_{i+j}(\alpha)$可以写成 $\alpha^{K+1},\alpha^{K+2},\cdots,\alpha^{K+q^n-1},\cdots$

或
$$A_{i+j}(\alpha)=A_K(\alpha) \quad (5)$$

于是$A_K(\alpha)$仍为α的升幂序列，它对应的M序列为$M_{A_\alpha}(K)$。它是由$M_{A_\alpha}(i)$与$M_{A_\alpha}(j)$相加而得到的。这就是M序列的移位相加性。

2．M序列的平均值 下面我们证明在$A_i(\alpha)$的一周期内(即q^n-1)，M序列零的个数为$q^{n-1}-1$，λ_K的个数为q^{n-1}（$K=1,2,\cdots\cdots,q-1$；λ_K是F_q的$q-1$个非零元素。）

由于α是本原元，所以$A_i(\alpha)$的一周期内q^n-1个元素均为F_{q^n}上的不同的元素。而这q^n-1个元素正好用q^n-1个F_q上的n维非零向量表示。显然F_q上的n维向量共有q^n个。第一分量为某一固定元素λ_K的向量共有q^{n-1}个。因此在一周期内，$A_i(\alpha)$对应的M序列$M_{A_\alpha}(i)$共有q^{n-1}个λ_K（$K=1,2,\cdots\cdots,q-1$），由于零向量不是A_i序列的元素，因此一周期内，$M_{A_\alpha}(i)$共有$q^{n-1}-1$个零。

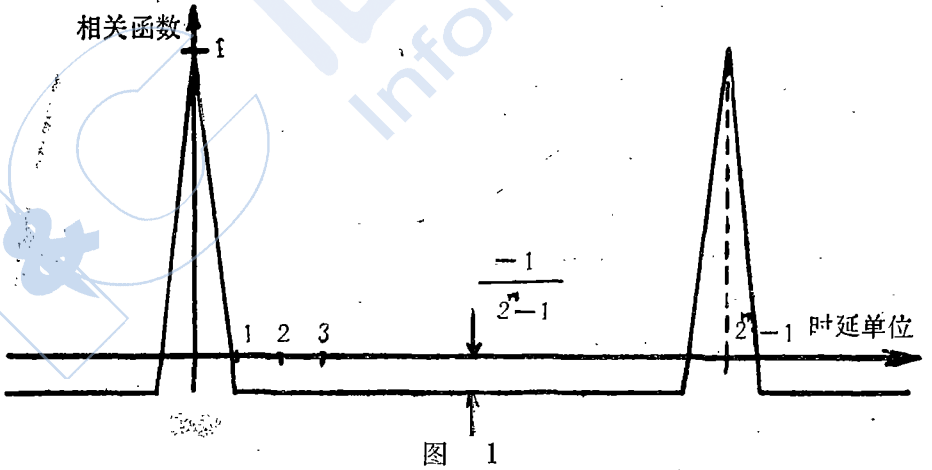

图 1

对于二元M序列，一周期内（即2^n-1）共有2^n-1个1，2^n-1个零。

由上述两个特性，很容易推出二元M序列的自相关函数如图1所示。〔1〕

§3 M序列的产生

当f(x)是本原多项式，产生M序列最容易。它可以用反馈移位寄存器产生。

假设本原多项式为

$$f(x)=b_0+b_1x+\cdots\cdots+b_nx^n\cdots\cdots \qquad (6)$$

图2就是产生$A_i(\alpha)$序列的反馈移位寄存器[2]。n个q元移位寄存器的状态正好代表F_q上的一个n－1阶多项式$\alpha(x)$的n个系数（$\alpha(x)=a_0+a_1x+\cdots\cdots+a_{n-1}x^{n-1}$）。亦即代表$F_{q^n}$中的一个元素。假定图2的移位寄存器初态为$\alpha_0(x)\neq 0$。每移一位相当于乘上一个$x_0$于是得到一个状态序列

$$A_0(\alpha):\ \alpha_0(x),\ \alpha_0(x)x,\ \alpha_0(x)x^2,\ \cdots\cdots,\ \alpha_0(x)x^{q^n-1}\cdots\cdots, \qquad (7)$$

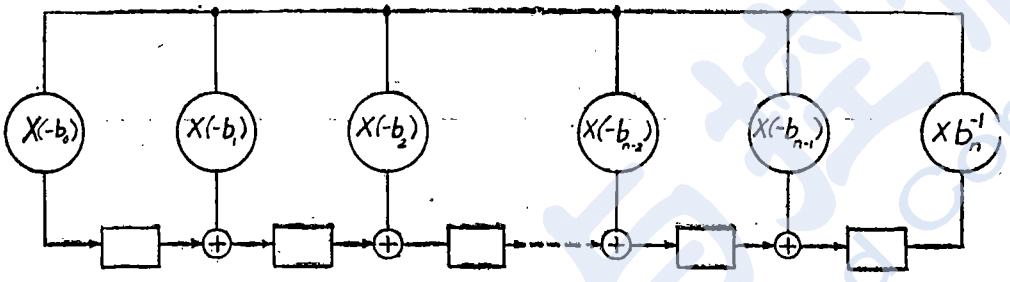

图 2

由于f(x)是本原多项式，其根x必为本原元，故$A_0(x)$是本原元x的升幂序列，而最左一个移位寄存器的状态就是对应的M序列的状态。图2的电路实际上是一个有限域计算器，它能够用移位的办法产生所有F_{q^n}中的非零元素。对二元M序列，图2可简化为图3的电路。

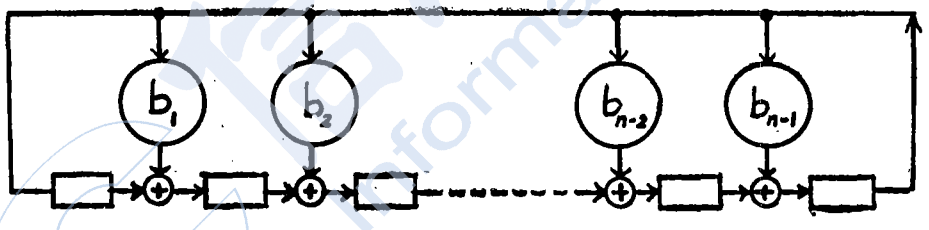

图 3

当f(x)是不可约多项式，但不是本原的，产生M序列的电路较复杂。因为此时x不再是本原元。例如，对于F_2上的四阶不可约多项式$f(x)=x^4+x^3+x^2+x+1$。它不是本原多项式，因为它的根x是五阶元素。故用图2不能产生M序列。但是1＋x是本原元。因此，用图4的电路可以产生1＋x的升幂序列。

先看图4a的实线部分，它是按图3的方法连成的电路。因此对于初态$\alpha_0(x)\neq 0$，每移一位相当于乘上一个x。虚线的反馈相当于每移一位加上一个移位前的元素。于是两者合起来（得到图4b）的作用，相当于每移一位乘上一个(1＋x)。所以，对初态为$\alpha_0(x)$的情况，得到一个(1＋x)的升幂序列

$$A_0(x):\ \alpha_0(x),\alpha_0(x)+x\alpha_0(x),\ [\alpha_0(x)+x\alpha_0(x)]\,x+\alpha_0(x)+x\alpha_0(x),\cdots\cdots$$

可以改写成：

$$A_0(\alpha):\quad \alpha_0(x),\ \alpha_0(x)(1+x),\ \alpha_0(x)(1+x)^2,\ \cdots\cdots \tag{8}$$

$A_0(\alpha)$对应的二元序列是M序列。

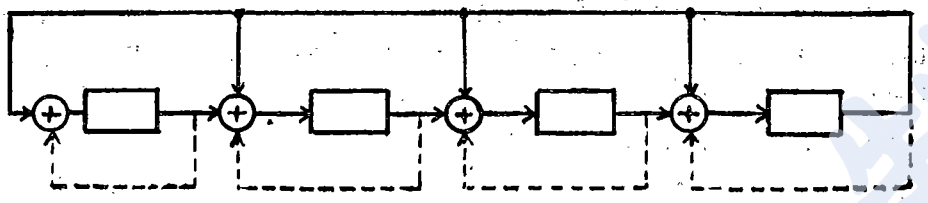

图 4a

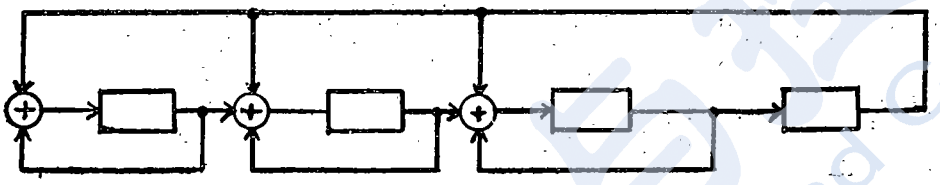

图 4b

§4 M序列的线性递归关系式

设$f(x)=b_0+b_1x+\cdots\cdots b_nx^n$是$F_q$上的n阶本原多项式。本原元$\alpha$是f(x)的根。于是有

$$f(\alpha)=0,$$

或

$$\alpha^{i+1}f(x)=0 \qquad (i=0,\ 1,\ \cdots\cdots q^n-2)。$$

即

$$\sum_{j=0}^{n} b_j\alpha^{i+j+1}=0 \tag{9}$$

因为α^{i+j+1}是一个n维向量，故(9)式实际上是一个方程组。以向量形式表示α^{i+j+1}得

$$\alpha^{i+j+1}=(\alpha_0^{(i+j+1)},\ \alpha_1^{(i+j+1)},\ \cdots\cdots,\ \alpha_{n-1}^{(i+j+1)}) \tag{10}$$

于是(9)式可以写成

$$\sum_{j=0}^{n} b_j a_K^{(i+j+1)}=0$$

其中 $K=0,1,2,\cdots\cdots n-1$，

当 $K=0$时有

$$\sum_{j=0}^{n} b_j \alpha_0^{(i+j+1)}=0$$

或

$$a_0^{(i+1+n)}=\frac{-1}{b_n}\sum_{j=0}^{n} b_j\, a_0^{(i+j+1)} \tag{12}$$

于是M序列(2)满足线性递归关系(12)。这就是通常定义M序列的线性递归关系式。这个关系式可用图5a的移位寄存器电路实现。对于二元情况，得到图5b的电路。

于是用递归关系式定义的M序列也就可以由(2)式的定义得到。

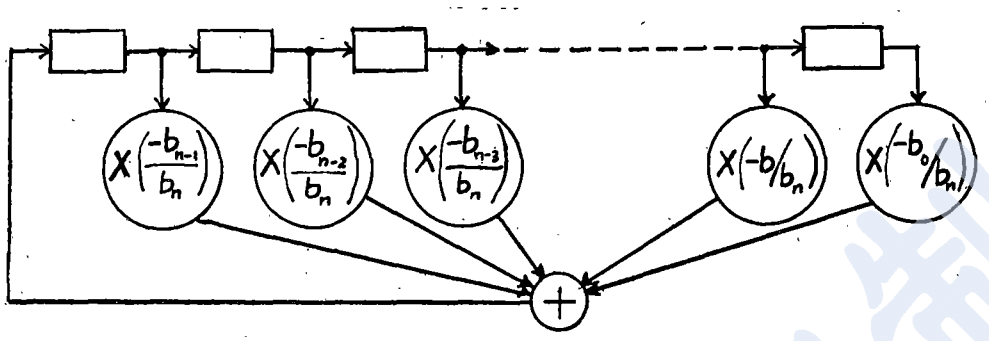

图 5a

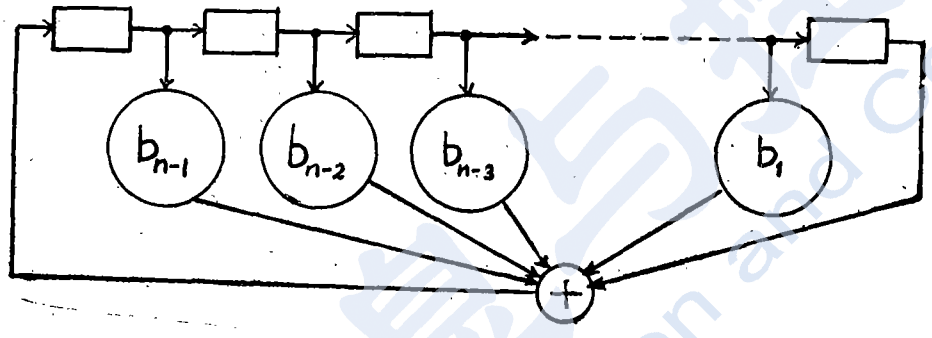

图 5b

§5 F_{qn}上的M序列的数目

从有限域的理论可知，F_{q^n}上共有$\phi(q^n-1)$个本原元。其中$\phi(m)$是欧拉函数，它等于与m互素而又小于m的正整数的个数。表面上看来，根据定义式(1)和(2)，似乎有$\phi(q^n-1)$类M序列。但是事实上，这$\phi(q^n-1)$种M序列中有些是平移等价的。亦即这$\phi(q^n-1)$种M序列中每几种都属于同一平移等价类。下面证明这一点。

设α是F_{q^n}的本原元。它的极小多项式必为n阶本原多项式$f_\alpha(x)$。$f_\alpha(x)$的n个根组成了α的共轭组：α，α^q，α^{q^2}，……$\alpha^{q^{n-1}}$。它们都是本原元。于是根据(1)式，由α的n个共轭根构成了n种升幂序列。它们对应n种M序列(2)。我们证明这n种M序列是平移等价的。

设
$$f_\alpha(x)=b_0+b_1x+b_2x^2+\cdots\cdots+b_nx^n \tag{13}$$
于是$f_\alpha(\alpha)=0$，由此可推出α升幂序列$A_i(\alpha)$所对应的M序列$M_{A_\alpha}(i)$满足递归关系式(12)。对于 $r_m=\alpha^{q^m}(1\leqslant m\leqslant n-1)$，它的极小多项式也是$f_\alpha(x)$。因此有
$$r_m^{i+1}f_\alpha(r_m)=0 \tag{14}$$
或
$$\sum_{j=0}^{n}b_jr_m^{i+j+1}=0 \tag{15}$$
用向量形式表示r^{i+j+1}

$$r^{i+j+1}=(C_0^{(i+j+1)}C_1^{(i+j+1)},\ \cdots\cdots,\ C_{n-1}^{(i+j+1)})。$$

从(15)式可得

$$C_0^{(i+n+1)}=\frac{-1}{b_n}\sum_{j=0}^{n-1}b_jC_0^{(i+j+1)} \tag{16}$$

显然，r_m的升幂序列$A_i(r_m)$对应的M序列$M_{A_r}(i)$满足(16)式。它与$M_{A_\alpha}(i)$序列满足同一个递归关系式。因此，$M_{A_r}(i)$与$M_{A_\alpha}(i)$属同一类M序列。亦即它们是初相位不同的同一种M序列。于是证明了α的共轭组构成的n个M序列互相平移等价。

对于不是共轭组的本原元，显然对应于不同的极小多项式。因此，每一共轭组的几个本原元对应于一类M序列。于是F_{q^n}上共有$\phi(q^n-1)/n$类M序列。它等于F_{q^n}上的本原多项式的数目。

§6 M序列的采样

设有(2)式所示的$M_{A_\alpha}(i)$序列，它是由(1)式的$A_i(\alpha)$产生的M序列。对$M_{A_\alpha}(i)$进行采样，可以得到一些新序列。设采样周期为$d(d<q^n-1)$，采样得到的新序列为

$$M_d(i):\ a_0^{(i+1)},a_0^{(i+1+d)},\ a_0^{(i+1+2d)},\ \cdots\cdots \tag{17}$$

我们证明当d与q^n-1互素，(17)式仍为M序列。而且当$d=q^m$ $(0\leqslant m<n-1)$时，所得的采样序列(17)均平移等价。更进一步，周期为q^n-1的不同类的M序列均可由采样的办法，从一个M序列$M_{A_\alpha}(i)$得到。

考察F_{q^n}的元素α^d的升幂序列（α是本原元）$A_k(\alpha^d)$，

$$A_k(\alpha^d):\ (\alpha^d)^{k+1},\ (\alpha^d)^{k+2},\ \cdots\cdots \tag{18}$$

如果d与q^n-1互素，则α^d是本原元。于是根据M序列的定义可知，$A_k(\alpha^d)$对应于M序列$M_{A_{\alpha^d}}(k)$。

$$M_{A_{\alpha^d}}(k):\ a_0^{(dk+d)},\ a_0^{(dk+2d)}\cdots\cdots$$

由于α和α^d都是本原元。α^{i+1}是F_{q^n}中的非零元素。而F_{q^n}中的任一非零元素均可以表成本原元α^d的某一幂。这就是说总可以找到一个$k(1\leqslant k\leqslant q^n-1)$，使

$$\alpha^{i+1}=(\alpha^d)^{k+1} \tag{19}$$

把(19)代入(18)得

$$A_k(\alpha^d):\ \alpha^{i+1},\ \alpha^{i+1+d},\ \alpha^{i+1+2d},\ \cdots\cdots \tag{20}$$

(20)式对应的M序列$M_{A_{\alpha^d}}(k)$可以写成

$$M_{A_{\alpha^d}}(k):\ a_0^{(i+1)},\ a_0^{(i+1+d)},\ a_0^{(i+1+2d)},\ \cdots\cdots \tag{21}$$

它与(17)式完全相同。这就证明了当采样周期d与q^n-1互素，M序列的采样序列仍为M序列。

当$d=q^m$ $(0\leqslant m\leqslant n-1)$，$\alpha^d$是$\alpha$的共轭元素。由§5的分析可知序列(18)的M序列与序列(2)平移等价。

最后，由于F_{q^n}上对应的全部M序列均由F_{q^n}上的全部本原元产生。而全部本原元均可由α^d（d与q^n-1互素）表示。因此全部不同类的M序列均可由一个M序列$M_{A_\alpha}(i)$采样产生。

§7 不可约非本原多项式的反馈移位寄存器

由图2可知，当移位寄存器的反馈按照本原多项式的系数来连接，如果初态不为零，移位寄存器就能产生F_{q^n}上的全部非零元素。或者每级移位寄存器都产生一个周期为q^n-1的M序列。但是，如果连接反馈的多项式是不可约的非本原多项式，那就不能产生M序列。下面我们证明，只要初态不为零，它产生的序列的周期都相同，而且是b^n-1的因子。

设图2的反馈连接多项式为

$$f(x)=b_0+b_1x+\cdots\cdots+b_nx^n。$$

它是不可约的非本原多项式。于是它的根X不是本原元。亦即它的阶$p\neq q^n-1$。设初态为α^i（α是本原元）。于是，移位寄存器得到的序列为

$$A_{xi}:\ \alpha^i,\ \alpha^ix,\ \alpha^ix^2,\ \cdots\cdots,\ \alpha^ix^p,\ \alpha^ix^{p+1},\ \cdots\cdots。\tag{22}$$

由于x的阶是p，故$x^p=1$，所以

$$A_{xi}:\ \alpha^i,\ \alpha^ix,\ \alpha^ix^2,\ \cdots\cdots\alpha^ix^{p-1},\ \alpha^i,\ \alpha^ix\cdots\cdots。\tag{23}$$

于是得到的序列以p为周期。对于初态为1，得到的序列为

$$A_{x1}:\ 1,\ x,\ x^2,\ \cdots\cdots x^{p-1},\ 1,\ \cdots\cdots。\tag{24}$$

易知，A_{x1}一周期内的元素(p个)构成$F^*_{q^n}$（$F^*_{q^n}$表示F_{q^n}中的全部非零元素，它是一个乘法群的一个乘法子群H。不难看出，不同初态产生的序列的元素均可构成H的陪集。根据有限群理论中的拉格朗日（Lagrange）定理，这些乘法子群（或陪集）的数目正好是$(q^n-1)/p$。它们都是不相交的。并且p一定是q^n-1的因子。

§8 同时产生q^n-1个平移等价的M序列的办法

在工程实际中，往往希望同时产生q^n-1个（或其中若干个）不同相位的M序列。最直接的办法是把M序列送到q^n-2级移位寄存器中，每经一级移位寄存器就得到一个相移一位的M序列（图6）。但是这种方法不经济，因为它需要q^n-2级移位寄存器。当我们只要其中一部份M序列时（例如只要$M_{A_\alpha}(i-1)$和$M_{A_\alpha}(i-q^n-2)$），如果用q^n-2个移位寄存器来产生这两个序列就有点浪费了。下面介绍一个办法，它只需要$n-2$个模q加法器就能得到全部q^n-1个M序列。如果只要其中一部份，则不一定要用$(n-2)$个模q加法器。

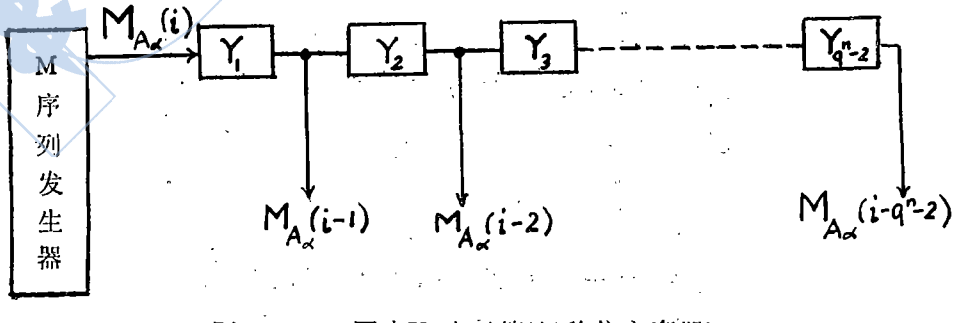

图 6 （图中Y_i表示第i级移位寄存器）

1．反馈移位寄存器各级产生不同相位的M序列 假定本原多项式f(x)的首项系数为1。

$$f(x)=x^n+b_{n-1}x^{n-1}+\cdots\cdots+b_1x+b_0 \tag{25}$$

按图2.的方法接成反馈移位寄存器如图7。把移位寄存器从左至右按顺序编号为第0级、第一级、…第n－1级。在§3已证明第0级移位寄存器的输出是M序列$M_{A_\alpha}(i_0)$，下面我们证明第1级至第n－1级移位寄存器也产生平移等价的M序列$M_{A_\alpha}(i_1)$，$M_{A_\alpha}(i_2)$，……$M_{A_\alpha}(i_{n-1})$，并求出它们的关系。

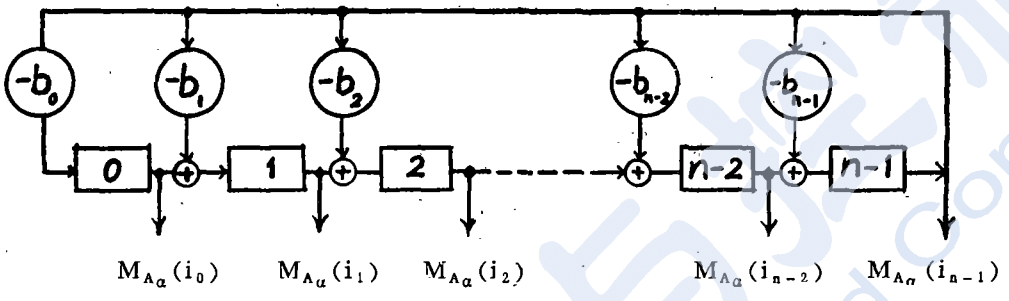

图 7

由于F_q中任一非零元素均可以由α的某一幂表示，因此$A_i(\upsilon)$序列逐项乘以F_q中的任一非零元素β以后，所得的序列$\beta\cdot A_i(\alpha)$仍为υ的升幂序列，它所对应的M序列与$A_i(\alpha)$对应的M序列平移等价。亦即任何M序列$M_{A_\alpha}(i)$乘以F_q中的非零元素仍然是同一类的M序列。

写出$M_{A_\alpha}(i_0)$序列和(n－1)级移位寄存器的状态序列$M_{A_\alpha}(i_{n-1})$如下，

$$M_{A_\alpha}(i_0):\ a_0^{(i_0+1)},\ a_0^{(i_0+1)},\ \cdots\cdots,$$

$$M_{A_\alpha}(i_{n-1}):\ a_{n-1}^{(i_0+1)},\ a_{n-1}^{(i_0+2)},\ \cdots\cdots。$$

由移位寄存器的反馈（图7）可得如下的关系

$$\left.\begin{aligned} a_0^{(i_0+2)} &= -b_0 a_{n-1}^{(i_0+1)} \\ a_0^{(i_0+3)} &= -b_0 a_{n-1}^{(i_0+2)} \\ &\vdots \end{aligned}\right\} \tag{26}$$

亦即

$$\left.\begin{aligned} a_{n-1}^{(i_0+1)} &= -a_0^{(i_0+2)}/b_0 \\ a_{n-1}^{(i_0+2)} &= -a_0^{(i_0+3)} \\ &\vdots \end{aligned}\right\} \tag{27}$$

由此可见，$M_{A_\alpha}(i_0)$序列向前移一位再乘$(-1/b_0)$就得到$M_{A_\alpha}(i_{n-1})$序列。所以$M_{A_\alpha}(i_{n-1})$是与$M_{A_\alpha}(i_0)$平移等价的M序列。

由M序列的移位M相加性以及上面的特性可知，图7的$M_{A_\alpha}(i_1)$、$M_{A_\alpha}(i_2)$、……$M_{A_\alpha}(i_{n-2})$均为同一类的M序列。也就是说它们都是由初态不同的α升幂序列$A_{i_j}(\alpha)$产生的$(i=0, 4, \cdots\cdots n-1)$。由于$A_{i_j}(\alpha)$序列完全取决于初态$\alpha^{i_j+1}$。根据图7的移位寄存器，我们可以列出各级所对应的$A_{i_j}(\alpha)$序列。

第n－1级 $A_{i_{n-1}}(\alpha)$: $\alpha^{i_{n-1}+1}$, $\alpha^{i_{n-1}+2}$, $\alpha^{i_{n-1}+3}$, ……,

第 0 级 $A_{i_0}(\alpha)$: $-b_0\alpha^{i_{n-1}}$, $-b_0\alpha^{i_{n-1}+1}$, $-b_0\alpha^{i_{n-1}+2}$, ……,

$\qquad = \alpha^{i_0+1}$, α^{i_0+2}, α^{i_0+3},

第一级 $A_{i_1}(\alpha)$: $\alpha^{i_0}-b_1\alpha^{i_{n-1}+1}$, $\alpha^{i_0+1}-b_1\alpha^{i_{n-1}+1}$, $\alpha^{i_0+2}+b_1\alpha^{i_{n-1}+2}$, ……,

$\qquad = \alpha^{i_1+1}$, α^{i_1+2}, α^{i_1+3}, ……。

由此可得出α^{i_j}与α^{i_j+1}之间的递推关系式：

$$\left.\begin{aligned}
\alpha^{i_0+1} &= -b_0\alpha^{i_{n-1}} \\
\alpha^{i_1+1} &= \alpha^{i_0}-b_1\alpha^{i_{n-1}} \\
\alpha^{i_2+1} &= \alpha^{i_1}-b_2\alpha^{i_{n-1}} \\
&\vdots \\
\alpha^{i_{n-2}+1} &= \alpha^{i_{n-3}}-b_{n-2}\alpha^{i_{n-1}} \\
\alpha^{i_{n-1}+1} &= \alpha^{i_{n-2}}-b_{n-1}\alpha^{i_{n-1}}
\end{aligned}\right\} \tag{28}$$

由这些递推关系式可以求出i_0、i_1、i_2、……i_{n-1}之间的关系。

2．向量α^{i_0}，α^{i_1}，……$\alpha^{i_{n-1}}$是F_q上的n维向量空间的一组基由线性代数的理论可知，要证明由这几个向量分量构成的n行n列矩阵A非奇异即可。

$$A=\begin{vmatrix}
a_0^{(i_0)}, & a_1^{(i_0)}, & a_2^{(i_0)}, & \cdots\cdots a_{n-1}^{(i_0)} \\
a_0^{(i_1)}, & a_1^{(i_1)}, & a_2^{(i_1)}, & \cdots\cdots a_{n-1}^{(i_1)} \\
\vdots & & & \\
a_0^{(i_{n-1})}, & a_1^{(i_{n-1})}, & a_2^{(i_{n-1})}, & \cdots\cdots a_{n-1}^{(i_{n-1})}
\end{vmatrix} \tag{29}$$

其中第j行为向量α^{i_j}；$\alpha^{i_j}=(a_0^{(i_j)}, a_1^{(i_j)}, \cdots\cdots a_{n-1}^{(i_j)})$。

不失一般性，可以假定$\alpha^{i_0}=1$，本原元α可以用多项式x代表，于是α的向量形式为

$$\alpha=(0, 1, 0, \cdots\cdots 0) \tag{30}$$

根据（28）式有

$$\alpha^{i_{n-1}}=-1/b_0\alpha=(0, -1/b_0, 0, \cdots\cdots 0) \tag{31}$$

用多项式表示α^{ij}得

$$\alpha^{ij}=a_0^{(ij)}+a_1^{(ij)}x+\cdots\cdots+a_{n-1}^{(ij)}x^{n-1}。$$

于是

$$\alpha^{ij+1}=\alpha^{ij}\cdot\alpha=a_0^{(ij)}x+a_1^{(ij)}x^2+\cdots\cdots a_{n-2}^{(ij)}x^{n-1}+a_{n-1}^{(ij)}x^n。$$

但是

$$x^n=-\sum_{k=0}^{n-1}b_kx^k$$

故

$$\alpha^{ij+1}=-a_{n-1}^{(ij)}b_0+(a_0^{(ij)}-a_{n-1}^{(ij)}b_1)x+(a_1^{(ij)}-a_{n-1}^{(ij)}b_2)x^2+\cdots\cdots$$
$$+(a_{n-2}^{(ij)}-a_{n-1}^{(ij)}b_{n-1})x^{n-1}\qquad(32)$$

从(28)式可得

$$\alpha^{ij+1}=\alpha^{ij-1}-b_j\alpha^{in-1}。$$

把(32)式代入上式可得

$$\left.\begin{aligned}-a_{n-1}^{(ij)}b_0&=a_0^{(ij-1)}\\ a_k^{(ij)}-a_{n-1}^{(ij)}b_{k+1}&=a_{k+1}^{(ij-1)}+S(k)\,bj/b_0\end{aligned}\right\}\qquad(33)$$

其中 $S(k)=\begin{cases}1 & \text{当}k=0\\ 0 & \text{当}k\neq0\end{cases}$；　$j\geqslant1$；　$k=0,1,\cdots\cdots n-1$。

有了上述的关系式，我们可以用矩阵的初等变换来证明(29)非奇异，即A是满秩矩阵。

根据$\alpha^{i_0}=1$及(31)式，

$$A=\begin{vmatrix}1, & 0, & \cdots\cdots & 0\\ a_0^{(i_1)}, & a_1^{(i_1)}, & \cdots\cdots & a_{n-1}^{(i_1)}\\ \cdot & & & \cdot\\ \cdot & & & \cdot\\ \cdot & & & \cdot\\ 0, & -1/b_0, & 0, \cdots\cdots & 0\end{vmatrix}\qquad(34)$$

把$-a_1^{(i_1)}$乘第一行加到第二行；　把$b_0a_1^{(i_1)}$乘第n行加到第二行；

〃 $-a_0^{(i_2)}$ 〃 〃 〃 〃 〃 〃 〃 三 〃；　〃 $b_0a_1^{(i_2)}$ 〃 〃 〃 〃 〃 〃 〃 三 〃；

〃 $a_0^{(i_{n-2})}$ 〃 〃 〃 〃 〃 〃 (n-1)行；　〃 $b_0a_1^{(i_{n-2})}$ 〃 〃 〃 〃 〃 〃 (n-1)行。

然后把第n行调到第二行并顺次把各行向下推一行，得到

$$A'=\begin{vmatrix}1, & 0, & \cdots\cdots & 0\\ 0 & -1/b_0, & 0\cdots\cdots & 0\\ \cdot & 0, & a_2^{(i_1)}\cdots\cdots & a_{n-1}^{(i_1)}\\ \cdot & \cdot & a_2^{(i_2)}, \cdots\cdots & a_{n-1}^{(i_2)}\\ \cdot & \cdot & \cdot & \cdot\\ \cdot & \cdot & \cdot & \cdot\\ 0, & 0, & a_2^{(i_{n-2})}, \cdots\cdots & a_{n-1}^{(i_{n-2})}\end{vmatrix}\qquad(35)$$

把 $(-b_3)$ 乘第n列加到第 三 列；

〃 $(-b_4)$ 〃 〃 〃 〃 〃 〃 四 〃；

⋮ ⋮

〃$(-b_{n-1})$〃 〃 〃 〃 〃 〃$(n-1)$〃；

然后把第n列调到第三列，并顺次把各列向右推一列。再注意到$a_k^{(i_0)}=0$(当$k>0$)就得到

$$A''=\begin{vmatrix} 1, & 0, & 0, & \cdots\cdots\cdots, & 0 \\ 0, & -1/b_0, & 0 & \cdots\cdots\cdots, & 0 \\ 0, & 0, & a_{n-1}^{(i_1)}, & 0\cdots\cdots, & 0 \\ \vdots & \vdots & a_{n-1}^{(i_2)}, & a_3^{(i_1)}, \cdots\cdots, & a_{n-1}^{(i_1)} \\ \vdots & \vdots & \vdots & & \\ \vdots & \vdots & \vdots & & \\ \vdots & \vdots & \vdots & & \\ 0, & 0, & a_{n-1}^{(i_{n-2})}, & a_3^{(i_{n-3})}, \cdots, & a_{n-1}^{(i_{n-3})} \end{vmatrix} \tag{36}$$

把 $(-b_4)$ 乘第n列加到第 四 列；

〃 $(-b_5)$ 〃 〃 〃 〃 〃 〃 五 〃；

⋮

〃$(-b_{n-1})$〃 〃 〃 〃 〃 〃 〃$(n-1)$〃。

然后把第n列调到第四列，并顺次把各列向右推一列得到：

$$A'''=\begin{vmatrix} 1, & 0, & 0, & \cdots\cdots\cdots\cdots, & 0 \\ 0, & -1/b_0, & 0, & \cdots\cdots\cdots\cdots, & 0 \\ 0, & 0, & a_{n-1}^{(i_1)}, & 0, \cdots\cdots\cdots, & 0 \\ 0, & 0, & a_{n-1}^{(i_2)}, & a_{n-1}^{(i_1)}, 0\cdots\cdots, & 0 \\ \vdots & \vdots & \vdots & a_{n-1}^{(i_2)}, a_4^{(i_1)}\cdots\cdots, & a_{n-1}^{(i_1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0, & 0, & a_{n-1}^{(i_{n-2})}, & \cdots\cdots\cdots\cdots & a_{n-1}^{(i_{n-3})} \end{vmatrix} \tag{37}$$

重复上述的初等变换就可把A变成三角矩阵$A^{(n-1)}$。它的行列式为$(-1/b_0)\left[a_{n-1}^{(i_1)}\right]^{n-2}$。从(33)式可知

$$a_{n-1}^{(i_1)}=-1/b_0\neq 0,$$

因此矩阵$A^{(n-1)}$非奇异，是满秩矩阵。而$A^{(n-1)}$是由A经初等变换得来的，因而两者的秩相等。亦即A满秩。这就证明了α^{i_0}，α^{i_1}，$\cdots\cdots\alpha^{i_{n-1}}$是$F_q$上的n维向量空间的一组基。

3．**M序列的合成** 由于α^{i_0}，α^{i_1}，$\cdots\cdots\alpha^{i_{n-1}}$是一组基。因此$F_{q^n}$上的任意矢量均可由$\alpha^{i_0}$，$\alpha^{i_1}$，$\cdots\cdots\alpha^{i_{n-1}}$的线性组合得到。亦即所有的$\alpha$升幂序列$A_j(\alpha)$均可由$A_{i_0}(\alpha)$，$A_{i_1}(\alpha)$，$\cdots\cdots A_{i_{n-1}}(\alpha)$线性组合得到。实际上，M序列$M_{A_\alpha}(j)$只是对应于$A_j(\alpha)$的第一分量。故$M_{A_\alpha}(j)$可由$M_{A_\alpha}(i_0)$，$M_{A_\alpha}(i_1)$，$\cdots M_{A_\alpha}(i_{n-1})$线性组合得到。

设 $$\alpha^{j}=C_0\alpha^{i_0}+C_1\alpha^{i_1}+\cdots\cdots+C_{n-1}\alpha^{i_{n-1}},$$

其中C_0，…C_{n-1}是F_q的元素。于是M序列$M_{A\alpha}(j)$可由图8的电路产生。

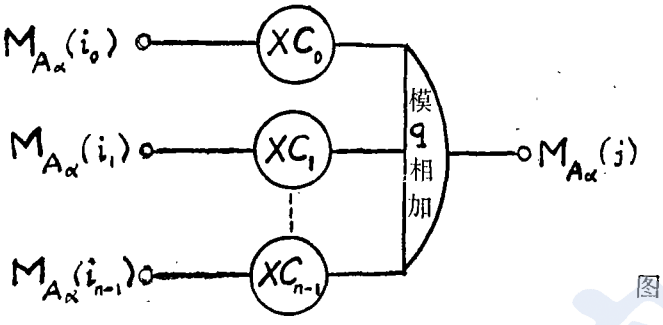

图 8

从图8可见，任意的$M_{A\alpha}(j)$序列最多只要n－1个二输入端的模q加法器便可产生。对于二元M序列，由于系数C_i只取0和1两个值，因此最多只要（n－2）个二输入端的模2加法器便够了。因为图7的电路至少都有一个模2加法器，它可以用在图8的电路上。

§9 应用举例

在多地址通信中，可以用不同类的二元M序列作地址码。也可以用两类优选的M序列（所谓Gold优选对）移位相加得到的新序列作为地址码〔4〕。在这种通信系统中，每一个通信台均需要同时产生两种序列。一种是本机的地址码，另一种是与它通信的另一电台的地址码。如果用移位寄存器产生，需要2^n-1个移位寄存器（因为码长为2^n-1）。但是用模2加法器合成的办法，最多只要n－2个模2加法器就够了。

例如，对于n＝5。优选对所对应的两个本原多项式为：

$$f_1(x)=1+x^2+x^3+x^4+x^5 \tag{38}$$

$$f_2(x)=1+x^3+x^5 \tag{39}$$

由这两个多项式产生的M序列分别为$M_{A\alpha}(i)$、$M_{A\beta}(j)$（α、β分别是它们的本原元）。由它们构成的新序列是$M_{A\alpha}(i)+M_{A\beta}(j)$不难看出，新序列只与差值i－j有关。因而可以写成$M_{A\alpha}(i)+M_{A\beta}(j)=S(i-j)$。又因为$M_{A\alpha}(i)=M_{A\alpha}(i+2^n-1)$，所以$S(i-j)=S(2^n-1+i-j)$。因此有$S(-k)=S(2^n-1-k)$。所以S(k)的k只取值0，1，2，…即可。图9就是产生$M_{A\alpha}(i)$及$M_{A\beta}(j)$的电路。

假定$i_0=0$，利用(28)式可知

$$\left.\begin{aligned}
&\alpha=\alpha^{i_{n-1}} && \text{或 } i_{n-1}=i_4=1;\\
&\alpha^{i_1+1}=\alpha^{i_0} && \text{或 } i_1=-1\text{或}30(\because \alpha^{-1}=\alpha^{30});\\
&\alpha^{i_2+1}=\alpha^{30}+\alpha;\\
&\alpha^{i_2}=\alpha^{29}+1;\\
&\alpha^{i_3+1}=\alpha^{i_2}+\alpha && \text{或}\alpha^{i_3}=\alpha^{i_2-1}+1;
\end{aligned}\right\} \tag{40}$$

$$\left.\begin{aligned}
&\beta=\beta^{j_4} && \text{或 } j_4=1;\\
&\beta^{j_1+1}=\beta^{j_0} && \text{或 } j_1=-1(\text{或}30);\\
&\beta^{j_2+1}=\beta^{j_1} && \text{或 } j_2=-2(\text{或}29);\\
&\beta^{j_4+1}=\beta^{j_3} && \text{或 } j_3=j_4+1=2。
\end{aligned}\right\} \tag{41}$$

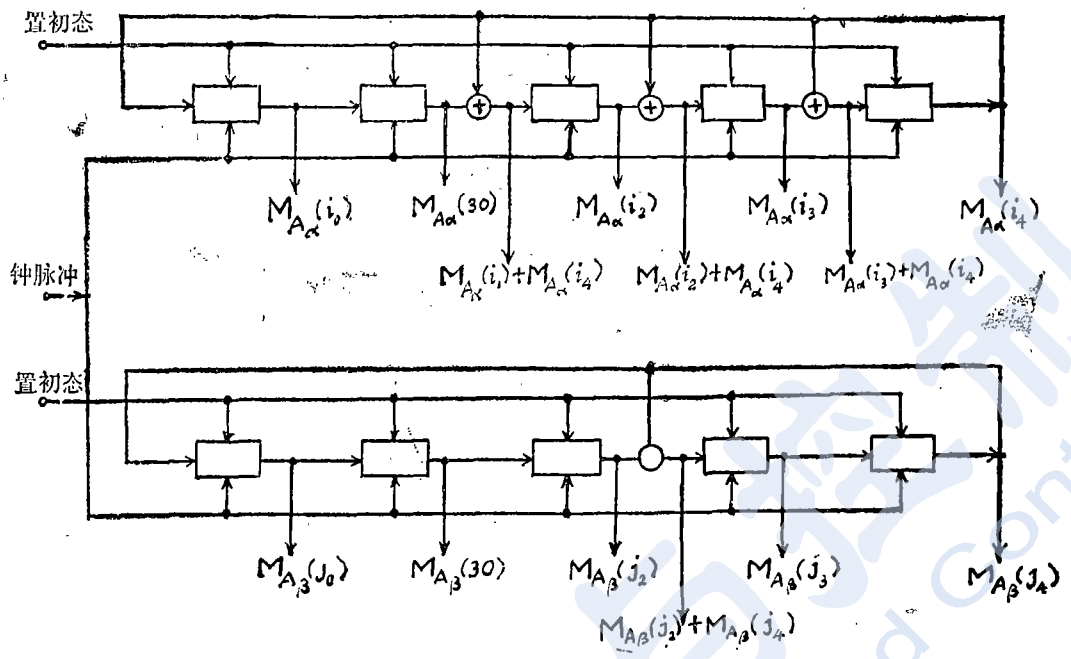

图　9

把α及β的各次幂列于表 1。

α^0	1	α^{16}	$1+\alpha+\alpha^3$	β^5	$1+\beta^3$	β^{21}	$1+\beta+\beta^2+\beta^4$
α^1	α	α^{17}	$\alpha+\alpha^2+\alpha^4$	β^6	$\beta+\beta^4$	β^{22}	$1+\beta+\beta^2$
α^2	α^2	α^{18}	$1+\alpha^4$	β^7	$1+\beta^2+\beta^3$	β^{23}	$\beta+\beta^2+\beta^3$
α^3	α^3	α^{19}	$1+\alpha+\alpha^2+\alpha^3+\alpha^4$	β^8	$\beta+\beta^3+\beta^4$	β^{24}	$\beta^2+\beta^3+\beta^4$
α^4	α^4	α^{20}	$1+\alpha$	β^9	$1+\beta^2+\beta^3+\beta^4$	β^{25}	$1+\beta^4$
α^5	$1+\alpha^2+\alpha^3+\alpha^4$	α^{21}	$\alpha+\alpha^2$	β^{10}	$1+\beta+\beta^4$	β^{26}	$1+\beta+\beta^3$
α^6	$1+\alpha+\alpha^2$	α^{22}	$\alpha^2+\alpha^3$	β^{11}	$1+\beta+\beta^2+\beta^3$	β^{27}	$\beta+\beta^2+\beta^4$
α^7	$\alpha+\alpha^2+\alpha^3$	α^{23}	$\alpha^3+\alpha^4$	β^{12}	$\beta+\beta^2+\beta^3+\beta^4$	β^{28}	$1+\beta^2$
α^8	$\alpha^2+\alpha^3+\alpha^4$	α^{24}	$1+\alpha^2+\alpha^3$	β^{13}	$1+\beta^2+\beta^4$	β^{29}	$\beta+\beta^3$
α^9	$1+\alpha^2$	α^{25}	$\alpha+\alpha^3+\alpha^4$	β^{14}	$1+\beta$	β^{30}	$\beta^3+\beta^4$
α^{10}	$\alpha+\alpha^3$	α^{26}	$1+\alpha^3$	β^{15}	$\beta+\beta^2$		
α^{11}	$\alpha^2+\alpha^4$	α^{27}	$\alpha+\alpha^4$	β^{16}	$\beta^2+\beta^3$		
α^{12}	$1+\alpha^2+\alpha^4$	α^{28}	$1+\alpha^3+\alpha^4$	β^{17}	$\beta^3+\beta^4$		
α^{13}	$1+\alpha+\alpha^2+\alpha^4$	α^{29}	$1+\alpha+\alpha^2+\alpha^3$	β^{18}	$1+\beta^3+\beta^4$		
α^{14}	$1+\alpha+\alpha^4$	α^{30}	$\alpha+\alpha^2+\alpha^3+\alpha^4$	β^{19}	$1+\beta+\beta^3+\beta^4$		
α^{15}	$1+\alpha+\alpha^3+\alpha^4$			β^{20}	$1+\beta+\beta^2+\beta^3+\beta^4$		

表　1

从上表可知

$$\alpha^{30}+\alpha=\alpha^2+\alpha^3+\alpha^4=\alpha^8;$$

于是从（40）式得

$$i_2+1=8 \quad 或\ i_2=7\ 。$$

$$\alpha^7+\alpha=\alpha^2+\alpha^3=\alpha^{22};$$

于是

$$i_3+1=22, \quad 或\ i_3=21。$$

从图9可知这两个电路还可以产生其他一些序列：

$$M_{A\alpha}(30)+M_{A\alpha}(1)=M_{A\alpha}(8);$$

$$M_{A\alpha}(7)+M_{A\alpha}(1)=M_{A\alpha}(22);$$

$$M_{A\alpha}(21)+M_{A\alpha}(1)=M_{A\alpha}(2);$$

$$M_{A\beta}(29)+M_{A\beta}(1)=M_{A\beta}(3)。$$

把它们产生的序列写于下：

$M_{A\alpha}(0)$, $M_{A\alpha}(1)$, $M_{A\alpha}(2)$, $M_{A\alpha}(7)$, $M_{A\alpha}(8)$, $M_{A\alpha}(21)$, $M_{A\alpha}(22)$,

$M_{A\beta}(30)$, $M_{A\beta}(0)$, $M_{A\beta}(1)$, $M_{A\beta}(2)$, $M_{A\beta}(3)$, $M_{A\beta}(29)$, $M_{A\beta}(30)$,

用一个模2加法器把上面的$M_{A\alpha}(i)$序列和$M_{A\beta}(j)$序列相加，并注意到$S(-k)=s(31-k)$，于是可以产生以下22种$S(j)$序列。见表2。

$S(j)=M_{A\alpha}(i)+M_{A\beta}(k)$																					
j	0	1	2	3	4	5	6	7	8	9	10	18	19	20	21	22	23	24	27	28	29	30
i	0	1	2	1	2	7	7	7	7	7	8	21	21	21	21	21	21	22	30	0	0	0
k	0	0	0	29	29	2	1	0	30	29	29	3	2	1	0	30	29	29	3	3	2	1

表　2

还差9种S序列，它们可以用$M_{A\alpha}(18)$、$M_{A\alpha}(14)$、$M_{A\alpha}(26)$产生，而这三种$M_{A\alpha}$序列可以由一组基α^0，α，α^{34}，α^7，α^{21}合成。把余下的9种S序列列于表3

j	11	12	13	14	15	16	17	25	26
i	14	14	14	14	18	18	18	26	26
k	3	2	1	0	3	2	1	1	0

表　3

利用 $\alpha^j=C_0\alpha^0+C_1\alpha+C_2\alpha^{30}+C_3\alpha^7+C_4\alpha^{21}$ 以及表1可得

$$\alpha^{18}=\alpha^0+\alpha^{30}+\alpha^7;$$

$$\alpha^{14}=\alpha^0+\alpha+\alpha^{30}+\alpha^7;$$

$$\alpha^{26}=\alpha^0+\alpha^{30}+\alpha^{21}。$$

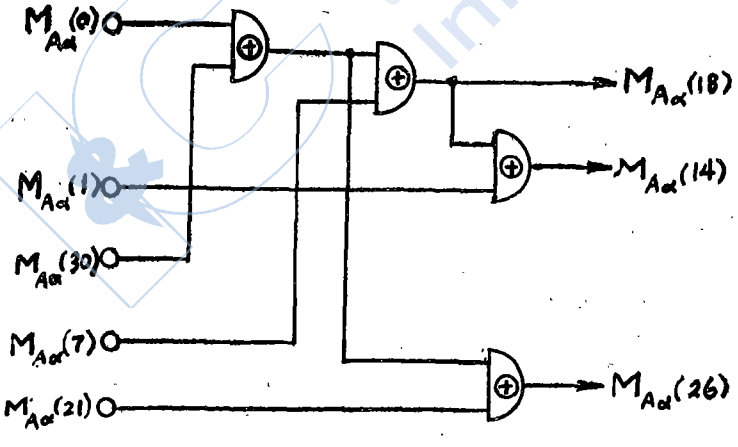

图　10

于是利用图10的电路便可产生$M_{A\alpha}(18)$、$M_{A\alpha}(14)$、$M_{A\alpha}(26)$。由此可见，要产生31种$S(j)$序列中的任意一个序列，最多只要3个$(n-2=3)$模2，加法器用来合成$M_{A\alpha}$序列，用一个模2加法器合成$S(j)$序列就够了。

（下转10页）

息信号看成是确定性的周期信号或瞬态信号。然而越来越多的通讯实践证明，系统内的消息和噪声在大多数情况下，既非周期性，也非瞬态性，而实质上是一种具有概率性的随机函数或随机过程。后来由于使用了统计力学中的概念，把概率论随机过程理论以及广义谐波分析的数学方法应用到信息系统的研究中，才得出概括性很高的一些结论，从而把通讯工程提高到统计科学的高度，因而对工程实践具有长远而深刻的指导意义。

应该看到：信息论虽然发展很快，但不少学者还认为，这一理论的基本结构不能算很完整，直到现在还缺乏象守恒定律类型的基本定律系，而这些定律是衡量各学科是否奠定理论基础的特征。

可能有部分不熟悉信息论的同志，以为信息论包含任何具体问题的解答，这是一种误解。信息论只建立明确的概念体系，预指实践活动的途径，而不直接给出结果。

信息论的研究，与很多近代学科是密切相关的；如通讯、雷达、声纳、导航、遥测、遥控、遥感、自动控制、计算机、信息处理技术、控制论以及应用数学、物理学、逻辑学、生物学、心理学、语言学、语音学、仿生学等。由此可见，通讯和控制等领域的科技工作者，确实需要掌握信息论有关方面的理论。本文仅仅是信息论的一个简单导引，仅供参考。

（上接26页）

文 献

〔1〕万哲先，代数和编码，科学出版社，1976.

〔2〕Peterson W. W., E. J. Weldon Jr., Error-Correcting Codes, 2nd ed., MIT Press, Mas., USA, 1971.

〔3〕Carmichael R. D., Introduction to The Theory of Groups of Finite Order, Boston, Ginu and Company.

〔4〕Gold R., Optimal Binary sequences for Spread Spectrum multiplexing, Trans. IEEE, Vol. IT pp.619—621, 1967.