国防科技大学学报
JOURNAL OF NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY
第12卷第4期 1990年12月 Vol.12 No.4

m序列的完备递归采样法

唐朝京 肖戎
(电子技术系)

摘 要 本文提出了m序列递归采样的概念，研究并解决了素数周期m序列的完备递归采样，对周期为合数的情况得到了一些有用的结论。

关键词 保密通信，采样，m序列
分类号 TP918.1

m序列是一类非常有用的伪随机序列，在编码、密码及通信工程中得到了广泛的应用。特别在密码学领域，将m序列进行适当变换产生密码序列是行之有效的办法。若存贮一定数量的m序列，则可以有效地增加密钥量，提高密码的抗破译能力。因此产生多个m序列的问题具有重要的意义。

产生m序列的传统方法是求GF(2)上的本原多项式，这可以直接根据本原多项式的定义来求，也可以利用各种等价的方法求得[1]，但这些方法都不很实用。目前产生m序列的最简单方法是采样法，只要采样间隔选得与序列的周期互素，就能得到一个新的m序列。但是当需要产生的m序列数量很大时，采样法也存在如下的不足之处（设级数为n，采样值为s，要求产生的m序列的个数为l）：

(1) 对每个采样值s，都要求保证$(s, 2^n-1)=1$，这一工作的计算量是不能忽略的；

(2) 为求得一个采样序列的反馈多项式，需要产生$2ns$位m序列。当l比较大时，s的值必然越来越大，则计算量也越来越大；

(3) 对于不同采样值采到的m序列，需要从中排除平移等价的序列，这个工作量为$\frac{1}{2}l(l-1)$；

(4) 不能保证在比较短的时间内采到所有的n级m序列。

针对采样方法的这些不足，作者提出了m序列递归采样和完备递归采样的概念，可

1990年3月16日收稿

weight error-detecting codes. A succinct proof is given for the conclusion made by prof. Wang xinmei (china science, vol.11, 1987) when n is even. The author also gives a proof for the conjecture of the wang xinmei's paper.

Key words code, coding error-detecting code, optimization / constant weight codes

以有效地解决这些问题。

1 定义与引理

首先，将 m 序列采样的有关结论作为本文的一个引理[2]：

引理 1 设$\{a_k\}$为一 n 级 m 序列，$\{a_{sk}\}$为$\{a_k\}$的一个 s 采样，则：

(1) 当$(s,2^n-1)=1$时，$\{a_{sk}\}$也为 n 级 m 序列；

(2) 设$(s_1,2^n-1)=1$，$(s_2,2^n-1)=1$，则 m 序列$\{a_{s_1k}\}$与$\{a_{s_2k}\}$平移等价的充要条件为存在 β 使下式成立：

$$s_2\equiv s_1\cdot 2^\beta(\mathrm{mod}2^n-1),\quad(0\leqslant\beta\leqslant n-1)$$

由引理 1 之(1)知，若$(s,2^n-1)=1$，则$\{a_{sk}\}$为 m 序列。我们可以求出$\{a_{sk}\}$的反馈多项式，并由它产生$2ns$位的$\{a_{sk}\}$序列，再对其作 s 采样，即得$\{a_{s^2k}\}$，显然$\{a_{s^2k}\}$也为 m 序列。重复进行这一过程，即可得到多个 m 序列：$\{a_{sk}\}$，$\{a_{s^2k}\}$，$\{a_{s^3k}\}$，……。这就是本文提出的递归采样的概念。

定义 1 上述产生 m 序列的方法称为 m 序列的递归采样法，称 s 为 m 序列$\{a_k\}$的递归采样值。

用递归采样法求一个 m 序列的反馈多项式只需产生 $2ns$ 位已知的 m 序列，再解一组 GF(2)上的 n 元线性方程。这个计算量很小，且每次都是固定的，这正是递归采样法的优点之一。

定义 2 若某一递归采样值可采得所有 n 级 m 序列，则称它为 n 级 m 序列的完备递归采样值，简称完备采样值，记作s_c. 这种采样过程称为完备递归采样。

显然，完备递归采样可以克服普通采样法的所有局限，本文的工作主要是讨论 m 序列的完备递归采样问题。

若将所有 s_c 的集合记作S_c，则 S_c 中每一个采样值均能采到$\frac{\varphi(2^n-1)}{n}$个 n 级 m 序列。

引理 2 若对 n 级 m 序列$\{a_{sk}\}$作 s 递归采样，则所得序列中出现平移等价序列的充要条件为存在正整数 t，使得下式对某一 β 值成立：

$$s^t\equiv 2^\beta(\mathrm{mod}2^n-1)\qquad(0\leqslant\beta\leqslant n-1)\qquad(1)$$

证明 充分性。若存在$t>0$，使(1)式成立，则由引理 1 之(2)知，$\{a_{s^tk}\}$即与$\{a_k\}$平移等价。

必要性。设$\{a_{s^tk}\}$与$\{a_{s^jk}\}$平移等价，不失一般性，可设 $j>i$，则由引理 1 之(2)知，存在 $\beta(0\leqslant\beta\leqslant n-1)$使下式成立：$s^j\equiv s^t\cdot 2^\beta(\mathrm{mod}2^n-1)$。由于$(s,\ 2^n-1)=1$，则$(s^t,\ 2^n-1)=1$，从而

$$s^{j-t}\equiv 2^\beta(\mathrm{mod}2^n-1)\qquad(0\leqslant\beta\leqslant n-1)$$

记$t=j-i>0$，则得：$s^t\equiv 2^\beta(\mathrm{mod}2^n-1)(0\leqslant\beta\leqslant n-1)$. (证毕)

定义 3 若t_0为满足(1)式的最小的 t，则称t_0为 s 对模2^n-1递归采样的平移等价次数，简称等价次数。

显然，对于任何 s 都有 $0<t_0\leqslant\frac{\varphi(2^n-1)}{n}$，而对完备采样值 s_c 则有 $t_0=\frac{\varphi(2^n-1)}{n}$。引理2的结论及等价次数 t_0 的概念本文将经常用到。

2 周期为素数时的结论

当 m 序列的周期为素数时，本文证明了完备采样值 s_c 的存在性，并找到了所有的 s_c.

定理 1　当 n 取素数 p，且 2^p-1 也为素数，则模 2^p-1 的所有原根都是 n 级 m 序列的完备采样值。

证明　设 g 为模 2^p-1 的任一原根，由于 2^p-1 为素数，故 g 必存在，且 $(g,2^p-1)=1$.

设 g 对模 2^p-1 的等价次数为 t_0，若 g 不是完备采样值，则有 $t_0<\frac{\varphi(2^p-1)}{p}$，由引理2知存在 β 使得：$g^{t_0}\equiv 2^\beta(\mathrm{mod}2^p-1)(0\leqslant\beta\leqslant p-1)$. 上式两边作 p 次乘方得：

$$g^{t_0p}\equiv(2^\beta)^p=(2^p)^\beta\equiv 1^\beta=1(\mathrm{mod}2^p-1) \qquad (2)$$

由于 $t_0p<(\varphi(2^p-1)$，(2)式说明 g 对模 2^p-1 的次数小于 $\varphi(2^p-1)$，这与 g 为原根矛盾，故 $t_0=\frac{\varphi(2^p-1)}{p}$，即 g 为完备采样值，或 $g\in S_c$.　　(证毕)

记 G 为所有原根的集合，则由数论知：

$$G=\{g^\lambda\mid 1\leqslant\lambda<\varphi(2^p-1),\ (\lambda,\ \varphi(2^p-1))=1\}$$

且

$$|G|=\varphi(\varphi(2^p-1)).$$

定理1说明：只要找到 2^p-1 的一个原根，则它一定可以递归采样得到全部的 p 级 m 序列。对于一个不算太大的素数 2^p-1（例如 $p<100$），只要将 $\varphi(2^p-1)$ 化成标准分解式，总能得到它的一个原根。定理2将证明某些不是原根的数也可作为完备采样值。

定理 2　设 g 为素数模 2^p-1 的一个原根，则当 $1\leqslant j<\frac{\varphi(2^p-1)}{p}$ 且 $\left(j,\frac{\varphi(2^p-1)}{p}\right)=1$ 时，g^{pj} 为完备采样值。

证明　设 g^{pj} 对模 2^p-1 的等价次数为 t_0，则 $g^{pjt_0}\equiv 2^\beta(\mathrm{mod}2^p-1)$ 对某一 β 值成立 $(0\leqslant\beta\leqslant p-1)$。上式两边对 g 取指数，得：

$$t_0pj\equiv\beta\mathrm{ln}d_g2(\mathrm{mod}\varphi(2^p-1))\quad(0\leqslant\beta\leqslant p-1) \qquad (3)$$

另一方面，由 $2^p\equiv 1(\mathrm{mod}2^p-1)$ 得：$p\cdot\mathrm{ln}d_g2\equiv 0\ (\mathrm{mod}\varphi(2^p-1))$. 而 $p\mid\varphi(2^p-1)$，故 $\mathrm{ln}d_g2\equiv 0\left(\mathrm{mod}\frac{\varphi(2^p-1)}{p}\right)$，故存在 k 使得下式成立：

$$\mathrm{ln}d_g2=k\cdot\frac{\varphi(2^p-1)}{p} \qquad (4)$$

显然(4)式中 $k\neq 0$，否则 $\mathrm{ln}d_g2=0$，或：

$$2\equiv g^{\mathrm{ln}d_g2}=g^0=1\quad(\mathrm{mod}2^p-1).\qquad 矛盾。$$

由于任何不为1的整数对模 2^p-1 的指数必小于 $\varphi(2^p-1)$，故 $\mathrm{ln}d_g2<\varphi(2^p-1)$，得

$k<p$，故$0<k<p$.（4）式代入（3）式得：

$$t_0 pj \equiv \beta \cdot \frac{k\varphi(2^p-1)}{p} (\mathrm{mod}\varphi(2^p-1)) \tag{5}$$

由于$p|\varphi(2^p-1)$，故（5）式两边必被p整除。由文[3]知，对于奇素数$p<6\times10^9$，且2^p-1也为素数，有$p^2|\varphi(2^p-1)$，又$0<k<p$，$0\leqslant\beta\leqslant p-1$，故必有$\beta=0$，（5）式即化为：$t_0 j\equiv \left(\mathrm{mod}\frac{\varphi(2^p-1)}{p}\right)$。由题设，$\left(j, \frac{\varphi(2^p-1)}{p}\right)=1$，故$t_0\equiv 0\left(\mathrm{mod}\frac{\varphi(2^p-1)}{p}\right)$，又由$0<t_0\leqslant\frac{\varphi(2^p-1)}{p}$，得$t_0=\frac{\varphi(2^p-1)}{p}$。即$g^{pj}$为完备采样值，故$g^{pj}\in S_c$.

（证毕）

显然，由于$(pj, \varphi(2^p-1))=p>1$，故g^{pj}不是模2^p-1的原根。下面讨论这种完备采样值的个数。

定理 3 记 $G'=\left\{g^{pj}\,\middle|\,1\leqslant j<\frac{\varphi(2^p-1)}{p}, \left(j, \frac{\varphi(2^p-1)}{p}\right)=1\right\}$，则

（1）对任一不同原根g_i，都有$g_i^{pj}\in G'$；

（2）$|G'|=\varphi\left(\frac{\varphi(2^p-1)}{p}\right)$。

证明 （1）由于g为原根，故g_i可表示为：

$$g_i=g^{\lambda},\ (\lambda, \varphi(2^p-1))=1,$$

则$g_i^{pj}=g^{pj\lambda}$. 由$(\lambda,\varphi(2^p-1))=1$，当然有$\left(\lambda, \frac{\varphi(2^p-1)}{p}\right)=1$，又$\left(j, \frac{\varphi(2^p-1)}{p}\right)=1$，故$\left(j\lambda, \frac{\varphi(2^p-1)}{p}\right)=1$，故$g^{pj\lambda}\in G'$，也即$g_i^{pj}\in G'$.

（2）由G'的定义知：G'中共有$\varphi\left(\frac{\varphi(2^p-1)}{p}\right)$个元素，下面证明$G'$中元素互不相同。

设j_1、j_2均满足G'中j的条件，则有：$|j_1-j_2|<\frac{\varphi(2^p-1)}{p}$。设$g^{pj_1}\equiv g^{pj_2}(\mathrm{mod}2^p-1)$，上式对$g$取指数得：$pj_1\equiv pj_2(\mathrm{mod}\varphi(2^p-1))$，有$j_1\equiv j_2\left(\mathrm{mod}\frac{\varphi(2^p-1)}{p}\right)$。由于$|j_1-j_2|<\frac{\varphi(2^p-1)}{p}$，故必有$j_1=j_2$，此即说明$G'$中元素各不相同，故

$$|G'|=\varphi\left(\frac{\varphi(2^p-1)}{p}\right)$$

（证毕）

综上所述知：只要$s\in G$或$s\in G'$，则s必为完备采样值。实际上，G和G'已包含了所有的完备采样值，定理4证明了这一结论。

定理 4 设s_c为完备采样值，S_c为所有s_c的集合，g、G、G'的定义如前，则：

（1）当$s_c^{\frac{\varphi(2^p-1)}{p}}\equiv 1(\mathrm{mod}2^p-1)$时，必有$s_c\in G'$；

(2) 当$s_c^{\frac{\varphi(2^p-1)}{p}}\equiv 2^\beta(\mathrm{mod}2^p-1)$对某一$\beta$值成立时$(1\leqslant\beta\leqslant p-1)$，必有$s_c\in G$；

(3) $S_c=G\cup G'$，且$|S_c|=p\cdot\varphi\left(\frac{2^{p-1}-1}{p}\right)$.

证明 (1) 首先证明：s_c一定为g^{up}的形式。

记$s_c=g^\lambda$，则λ可唯一表示为$\lambda=up+v(0\leqslant v<p)$，则

$$1\equiv s_c^{\frac{\varphi(2^p-1)}{p}}=g^{\lambda\cdot\frac{\varphi(2^p-1)}{p}}\equiv g^{up\varphi(2^p-1)}\cdot g^{\frac{v}{p}\varphi(2^p-1)}\equiv g^{\frac{v}{p}\varphi(2^p-1)}(\mathrm{mod}2^p-1)$$

若$v\neq 0$，有$0<\frac{v}{p}\varphi(2^p-1)<\varphi(2^p-1)$，则上式说明$g$对模$2^p-1$的次数小于$\varphi(2^p-1)$. 这与$g$为原根矛盾，所以$v=0$，$\lambda=up$，即$s_c=g^{up}$.

再证$\left(u,\ \frac{\varphi(2^p-1)}{p}\right)=1$. 设$s_c$对模$2^p-1$的等价次数为$t_0$，由题设$s_c^{t_0}\equiv 1(\mathrm{mod}2^p-1)$，或$g^{upt_0}\equiv 1(\mathrm{mod}2^p-1)$，即$upt_0\equiv 0(\mathrm{mod}\varphi(2^p-1))$，故$ut_0\equiv 0\left(\mathrm{mod}\frac{\varphi(2^p-1)}{p}\right)$。设$\left(u,\ \frac{\varphi(2^p-1)}{p}\right)=d$，则上式化为：

$$t_0\equiv 0\left(\mathrm{mod}\frac{\varphi(2^p-1)}{p\cdot d}\right)\qquad(6)$$

由于t_0为满足(6)式的最小正整数，故$t_0=\frac{\varphi(2^p-1)}{p\cdot d}$. 又$s_c$为完备采样值，故必有$t_0=\frac{\varphi(2^p-1)}{p}$，$d=1$，即$\left(u,\ \frac{\varphi(2^p-1)}{p}\right)=1$，从而$s_c=g^{up}\in G'$.

(2) 首先证明：若s_c对模2^p-1的次数为λ，则必有$\lambda=u\cdot\frac{\varphi(2^p-1)}{p}$ $(0<u\leqslant p)$.

设$\lambda=u\cdot\frac{\varphi(2^p-1)}{p}+v$，$0\leqslant v<\frac{\varphi(2^p-1)}{p}$，则

$$1\equiv s_c^\lambda=s_c^{u\frac{\varphi(2^p-1)}{p}+v}\equiv(2^\beta)^u\cdot s_c^v(\mathrm{mod}2^p-1)\quad(1\leqslant\beta\leqslant p-1)$$

即：
$$2^{\beta u}\cdot s_c^v\equiv 1(\mathrm{mod}2^p-1)\quad(1\leqslant\beta\leqslant p-1)\qquad(7)$$

由于$(2^{\beta u},\ 2^p-1)=1$，故同余式(7)有唯一解[8]：

$$s_c^v\equiv(2^{\beta u})^{\varphi(2^p-1)-1}\equiv 2^{\beta'}(\mathrm{mod}2^p-1)\quad(0\leqslant\beta'\leqslant p-1).$$

若$v\neq 0$，由于$v<\frac{\varphi(2^p-1)}{p}$，则上式表明，$s_c$的等价次数小于$\frac{\varphi(2^p-1)}{p}$. 这与$s_c$为完备采样值矛盾，故$v=0$，即$\lambda=u\cdot\frac{\varphi(2^p-1)}{p}$. 显然$0<u\leqslant p$.

再证s_c为原根，即$\lambda=\varphi(2^p-1)$。据：

$$1\equiv s_c^{\lambda}=s_c^{u\frac{\varphi(2^p-1)}{p}}\equiv(2^{\beta})^u(\mathrm{mod}2^p-1)\quad(1\leqslant\beta\leqslant p-1)$$

得： $2^{\beta u}\equiv 1(\mathrm{mod}2^p-1)\quad(1\leqslant\beta\leqslant p-1)$

即$(2^p-1)\mid(2^{\beta u}-1)$，或$(2^{\beta u}-1,\ 2^p-1)=2^p-1=2^{(\beta u,p)}-1$[8]，故$(\beta u,p)=p$，$p\mid\beta u$. 由于$(\beta,p)=1$，故$p\mid u$. 又$0<u\leqslant p$，故$u=p$，$\lambda=\varphi(2^p-1)$，故$s_c$为原根，即$s_c\in G$.

(3) 由于(1)与(2)的讨论已包括了β的所有可能取值，故$S_c=G\cup G'$.

又由于G中元素都是原根，G'中元素都不是原根，显然$G\cap G'$为空，故$|S_c|=|G|+|G'|$. 而$|G|=\varphi(\varphi(2^p-1))=\varphi\left(p\cdot\frac{\varphi(2^p-1)}{p}\right)$，因$\left(p,\ \frac{\varphi(2^p-1)}{p}\right)=1$，故

$$|G|=\varphi(p)\cdot\varphi\left(\frac{\varphi(2^p-1)}{p}\right)=(p-1)\cdot\varphi\left(\frac{\varphi(2^p-1)}{p}\right)$$

又$|G'|=\varphi\left(\frac{\varphi(2^p-1)}{p}\right)$，故

$$|S_c|=|G|+|G'|=p\cdot\varphi\left(\frac{\varphi(2^p-1)}{p}\right)=p\cdot\varphi\left(\frac{2^p-2}{p}\right)$$

$$=p\cdot\varphi\left(2\cdot\frac{2^{p-1}-1}{p}\right)=p\cdot\varphi(2)\cdot\varphi\left(\frac{2^{p-1}-1}{p}\right)=p\cdot\varphi\left(\frac{2^{p-1}-1}{p}\right)\qquad\text{(证毕)}$$

至此，素数周期m序列的完备递归采样问题已解决。下面以一个例子加以说明。

例 取$n=p=5$，$2^p-1=31$为素数，$\frac{\varphi(2^p-1)}{p}=6$，$p\cdot\varphi\left(\frac{2^{p-1}-1}{p}\right)=10$，此时有：$G=\{3,\ 11,\ 12,\ 13,\ 17,\ 21,\ 22,\ 24\}$；$G'=\{6,\ 26\}$；$S_c=G\cup G'$，$|S_c|=10$.

如取$s_c=6\in S_c$，则s_c的各次采样值s_c^i依次为：

i：	1， 2， 3， 4， 5， 6
$s_c^i(\mathrm{mod}31)$：	6， 5， 30， 25， 26， 1

显然，$s_c=6$可递归采得全部5级m序列。

3 周期为合数时的结论

合数周期的m序列是更为普通的，对它们的讨论也更有意义。

定理 5 设$2^n-1=\prod_{i=1}^{k}q_i^{a_i}$为$2^n-1$的标准分解式，则当$[\varphi(q_1^{a_1}),\ \cdots,\ \varphi(q_k^{a_k})]<\frac{\varphi(2^n-1)}{n}$时，$n$级$m$序列不存在完备采样值。

证明 设s为n级m序列的任一递归采样值，由$(s,\ 2^n-1)=1$知，$(s,\ q_i^{a_i})=1$ $(1\leqslant i\leqslant k)$. 由欧拉定理：

$$s^{\varphi(q_i^{a_i})}\equiv 1(\mathrm{mod}q_i^{a_i})(1\leqslant i\leqslant k)\qquad(8)$$

设$\varphi(q_i^{a_i})\cdot m_i=[\varphi(q_1^{a_1}),\ \cdots,\ \varphi(q_k^{a_k})]$，(8)式两边作$m_i$次乘方，得：

$$s^{[\varphi(q_1^{a_1}),\cdots,\varphi(q_k^{a_k})]}\equiv 1(\mathrm{mod}q_i^{a_i})\quad(1\leqslant i\leqslant k)$$

所以　$s^{[\varphi(q_1^{a_1}),\cdots,\varphi(q_k^{a_k})]}\equiv 1\left(\mathrm{mod}\prod_{i=1}^{k}q_i^{a_i}\right)$

即　$s^{[\varphi(q_1^{a_1}),\cdots,\varphi(q_k^{a_k})]}\equiv 1\ (\mathrm{mod}2^n-1)$

显然，当$[\varphi(q_1^{a_1}),\cdots,\varphi(q_k^{a_k})]<\frac{\varphi(2^n-1)}{n}$时，$s$的等价次数$t_0<\frac{\varphi(2^n-1)}{n}$，即此时$n$级$m$序列不存在完备采样值。　（证毕）

定理5可以用来判断某一级数的m序列是否存在完备采样值s_c。利用定理5，命题1得出了当2^p-1为合数时p级m序列不存在完备采样值的结论（p为素数）。

引理3　若p为素数，q为2^p-1的任一素因数，则必有$2p|q-1$.

证明　若$q|2^p-1$，则$2^p\equiv 1\ (\mathrm{mod}q)$。设2对于模$q$的次数为$d$，则有$d|p$，由于$p$为素数，故$d=p$. 由于$q|2^p-1$，故$q$为奇数，故$(2,q)=1$. 由费尔马定理：$2^{q-1}\equiv 1\ (\mathrm{mod}q)$，得$d|q-1$，即$p|q-1$. 又$q-1$为偶数，故$2|q-1$. $2p|q-1$.　（证毕）

命题1　当n取素数p，而2^p-1为合数，则n级m序列不存在完备采样值。

证明　下述数论猜想尚未解决[8]：不存在素数q使得$q^2|2^p-1$.可以认为，当p取值在实际应用的数量级时上述猜想成立，即2^p-1无平方因子，故可设2^p-1的标准分解式为

$$2^p-1=\prod_{i=1}^{k}q_i\ (k\geqslant 2)，则\varphi(2^p-1)=\prod_{i=1}^{k}\varphi(q_i)$$

由引理5知$2p|q_i-1$，即$2p|\varphi(q_i)$，则

$$[\varphi(q_1),\cdots,\varphi(q_k)]=2p\cdot\left[\frac{\varphi(q_1)}{2p},\cdots,\frac{\varphi(q_k)}{2p}\right]$$

$$\leqslant 2p\cdot\prod_{i=1}^{k}\frac{\varphi(q_i)}{2p}=\frac{1}{(2p)^{k-1}}\prod_{i=1}^{k}\varphi(q_i)$$

$$=\frac{1}{(2p)^{k-1}}\varphi(2^p-1)<\frac{\varphi(2^p-1)}{p}$$

由定理5知，此时p级m序列不存在完备采样值。　（证毕）

4　进一步的讨论

对于周期为素数的m序列，本文已证明了完备采样值s_c的存在性，并找到了所有的s_c. 这种情况下的完备递归采样问题已经解决。对于级数为素数而周期为合数的m序列，命题1证明了s_c不存在。对于级数n为合数的m序列，本文只得到了s_c存在的必要条件，这一问题有待于进一步探讨。事实上，当$n=6$时，s_c是存在的，且$s_c\in S_c=\{5,10,13,17,19,20,26,34,38,40,42,52\}$。

此外，对于s_c不存在的m序列，也有必要研究它们的不完备递归采样问题。本文尚未解决的问题可以归结为：

（1）当n为合数时s_c在什么条件下存在？如何计算？

（2）当s_c不存在时，如何确定各递归采样值s的等价次数？

（3）能否找到h个（$h>1$）不同的递归采样值$s_1,\cdots,s_h$（等价次数分别为t_1，

…, t_h)，使得它们采得的 $\sum_{i=1}^{h} t_i$ 个 m 序列除原序列外互不相同？

上述问题的解决将使递归采样的方法更为实用。

利用普通采样法产生多个 m 序列存在许多不足。利用本文所提出的递归采样方法，这些不足都可克服。递归采样法的应用价值是比较大的。本文从一个新的角度来考察 m 序列的产生问题，所得的结论丰富了 m 序列采样的理论。

本文得到了国防科技大学电子技术系青年教师研究基金的资助。

杨述明老师对本文进行了认真的审阅，谨表示深切的感谢。

参 考 文 献

[1] 倪世鹏.寻找二进制本原多项式的一种新方法.国防科技大学学报，1987，(3)

[2] 肖国镇等.伪随机序列及其应用.国防工业出版社，1985：94

[3] 柯召、孙琦.数论讲义.高等教育出版社，1986.16～40

[4] 李复中.初等数论选讲.东北师范大学出版社，1984

[5] 蒋增荣.数论变换.国防科技大学出版社，1978

On Complete Recurrence Sampling of m-Sequences

Tang Chaojing Xiao Rong

(Department of Electronic Technology)

Abstract

This paper presents the concept of recurrence sampling of m-sequences. The complete recurrence sampling of the m-sequence with a prime number period is studied and solved. In the case of composite number period, some useful conclusions are achieved.

Key words: secret communication, sampling, m-sequence