国防科技大学学报
JOURNAL OF NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY
第14卷第1期 1992年3月 Vol. 14 No. 1

m序列完备递归采样值的存在条件

李 超

（系统工程与应用数学系）

摘 要 本文用群论方法讨论了 n 级m序列完备递归采样值的存在条件，证明了对任意 n 级 m 序列，其完备递归采样值存在的充要条件是商群 $G=Z_p^*/H$（其中 $p=2^n-1, Z_p^*=\{s|(s,p)=1\}$ ，$H=\{1,2,2^2,\cdots,2^{n-1}\}$）为循环群。在完备递归采样值存在的条件下，求出了完备递归采样值的个数为 $n.\varphi\left(\frac{\varphi(2^n-1)}{n}\right)$ 。最后给出了递归采样值的一个重要性质。

关键词 采样，m序列，循环群

分类号 TN911.72

1 问题的提出

由于m序列具有周期大，伪随机特性好等优点，被广泛应用于保密通信，从已知的m序列构造新的m序列的方法变得重要。唐朝京等[1]引进的m序列递归采样和完备递归采样是一个很好的方法，它克服了普通采样法的所有局限。在文[1]中，对于周期为素数的m序列证明了完备递归采样值的存在性，并求出了所有的完备采样值；但对于周期为合数的m序列，仅给出了完备递归采样值存在的一个必要条件。在文[1]最后提出了三个更为一般的有待解决的问题，即：(1) 当 n 为合数时，完备递归采样值在什么条件下存在？如何计算？(2) 当完备采样值不存在时，如何确定各递归采样值的等价次数？(3) 能否找到 $h(h>1)$ 个不同的递归采样值 $s_1, s_2, \cdots, s_h$（等价次数分别为 $t_1,t_2,\cdots,t_h$）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。本文从群论的观点出发，对上述问题进行讨论，对任意 n 级m序列，不管其周期为素数还是合数，得到了较好的结果。

为方便起见，本文先引进文[1]中一些基本概念：

定义1 设 $\{a_k\}$ 为 n 级m序列，s 为正整数，$(s,2^n-1)=1$，对 $\{a_k\}$ 进行 s 采样得到 n 级m序列 $\{a_{sk}\}$，求出 $\{a_{sk}\}$ 的反馈多项式。然后对 $\{a_{sk}\}$ 进行 s 采样得到 n 级m序列 $\{a_{s^2k}\}$，重复下去，可得多个m序列 $\{a_{sk}\}\{a_{s^2k}\}\{a_{s^3k}\}\cdots$，这样产生m序列的方法称为m序列的递归采样法，$s$ 叫 n 级m序列 $\{a_k\}$ 的递归采样值。

定义2 若某一递归采样值可采得 $\frac{\varphi(2^n-1)}{n}$ 个不平移等价的m序列（即全体 n 级m序列），则称它为完备递归采样值。我们记 S_c 表示所有的完备递归采样值。

定义3 设 s 为递归采样值，若 t_0 是满足 $s^t\equiv 2^\beta(\bmod 2^n-1)$（其中 β 为 $\{0,1,\cdots,n-1\}$

* 1991年3月27日收稿

中任意数)的最小正整数，则称 t_0 为 s 对模 2^n-1 的递归采样的等价次数，简称等价次数。

由上述定义易知，当 s 的等价次数为 t_0 时，$\{a_{sk}\},\{a_{s^2k}\},\cdots,\{a_{s^{t_0}k}\}$ 为互不等价的 m 序列。若 $t_0=\frac{\varphi(2^n-1)}{n}$，则 s 为完备递归采样值。因此，对任意 s，$(s,2^n-1)=1$，s 是否为完备递归采样值关键在于 s 的等价次数为 $\frac{\varphi(2^n-1)}{n}$。下面用群论的方法来讨论 s 的等价次数。

2 主要结果及其证明

设 $\{a_k\}$ 为 n 级 m 序列，$p=2^n-1$ 为 $\{a_k\}$ 的周期。 令：

$$Z_p=\{0,1,2,\cdots,p-1\}$$
$$Z_p^*=\{s\in Zp\,|\,(s,p)=1\}$$
$$H=\{2^i\,|\,0\leqslant 1\leqslant n-1\}$$

由群论易知，Z_p^* 关于模 m 的数的乘法构成 Abel 群。H 为 Z_p^* 的正规子群，从而我们有商群 $G=Z_p^*/H=\{C_0,C_1,\cdots,C_{u-1}\}$，其中 $C_0=H,C_i=S_iH,u=\varphi(2^n-1)/n.\ s_i(i=1,2,\cdots,u-1)$ 为 C_i 中代表元。

由等价次数的定义知，对任意 $s\in Z_p^*$，s 的等价次数即为使 $s^t\in H$ 的最小值 t_0.

下面证明：对任意 $s\in Z_p^*$，s 的等价次数实际上为 s 所在的群元 C_i 在群 G 中的阶。证明了这一点，可推出递归采样值 s 为完备递归采样值的充分必要条件为 C_i 为 G 中 $\varphi(2^n-1)/n$ 阶元。

引理 1 设 $s_1,s_2\in Z_p^*$，若存在 $C_i\in G$ 使 $s_1,s_2\in C_i$，则 s_1 与 s_2 具有相同的等价次数。

证明 设 s_1 与 s_2 的等价次数分别为 t_1,t_2，则 $s_1^{t_1}\in H,s_2^{t_2}\in H$.

由于 $s_1,s_2\in C_i$，于是存在 $\beta\in\{0,1,2,\cdots,n-1\}$，使 $s_1=2^\beta s_2$，从而 $s_1^{t_1}=(2^\beta s_2)^{t_1}=2^{\beta t_1}s_2^{t_1}$. 又 $s_1^{t_1}\in H$，所以 $s_2^{t_1}\in H$，而 t_2 是使 $s_2^{t_2}\in H$ 的最小正整数，于是 $t_2\angle t_1$.

同理可证 $t_1\angle t_2$，所以 $t_1=t_2$.

引理 2 对任意 $s\in C_i$，s 的等价次数等于群元 C_i 在群 G 中阶。

证明 设 s 的等价次数为 V，群元 C_i 在 G 中阶为 W，不妨设 s 为 C_i 的代表元，即 $C_i=SH$. 由于 s 的等价次数为 V，于是 $S^V\in H$，进而 $S^VH=H$.

所以 $$(SH)^V=\overbrace{(SH)(SH)\cdots(SH)}^{V个}=S^VH=H$$

即 $C_i^V=H$. 所以 $W\angle V$.

反之，因为 $C_i^W=H$，即 $S^WH=H$，于是 $S^W\in H$，从而 $V\angle W$. 所以 $W=V$.

推论 1 递归采样值 s 的等价次数一定为 $\varphi(2^n-1)/n$ 的因子。 s 为完备递归采样值的充要条件为 s 所在群元 C_i 为 G 的生成元。即 C_i 为 $\varphi(2^n-1)/n$ 阶元。

定理 1 任意 n 级 m 序列 $\{a_k\}$ 存在完备递归采样值的充要条件为商群 $G=Z_p^*/H$ 系循环群。

证明 (1) 必要性 若存在完备递归采样值 $s\in Z_p^*$，则 s 的等价次数为 $\varphi(2^n-1)/n$. 设 s 所在群元为 C_i，由引理 2 可知，C_i 在 G 中阶为 $\varphi(2^n-1)/n$，而 $|G|=\varphi(2^n-1)/n$，所以 $G=\langle C_i\rangle$ 为循环群。

(2) 充分性　若 G 为循环群，则存在 $C\in G_n$ 使 $G=\langle C_i\rangle$，即 C_i 的阶为 $\varphi(2^n-1)/n$，从而群元 C_i 中每个数的等价次数为 $\varphi(2^n-1)/n$. 即 C_i 中每个数均为完备递归采样值。

推论 2　若 n 级 m 序列 $\{a_k\}$ 存在完备递归采样值，则，$S_c=\bigcup\limits_{C_i\text{为}G\text{中生成元}} Ci$，且 $|S_c|=n\cdot\Phi\left(\dfrac{\varphi(2^n-1)}{n}\right)$.

证明　由定理 1 可知，在完备递归采样值存在的条件下，商群 $G=Z_p^*/H=\{C_0,C_1,\cdots,C_{n-1}\}$ 为循环群，从而 G 中每个生成元内所有的值均为完备递归采样值。即 $S_c=\bigcup\limits_{C_i\in G\text{为生成元}} C_i$. 而有限群 G 中生成元个数为 $\varphi(\varphi(2^n-1)/n)$，于是共有 $n\cdot\varphi(\varphi(2^n-1)/n)$ 个完备递归采样值。

例 1

$$n=4,p=2^4-1=15$$
$$Z_p^*=\{1,2,4,7,8,11,13,14\}$$
$$H=\{1,2,4,8\},G=Z_p^*/H=\{C_0,C_1\}$$

式中，　$C_0=H=\{1,2,4,8\},C_1=\{7,11,13,14\}$

易知　$G=<C_1>$ 为循环群。

所以　$S_c=C_1=\{7,\ 11,\ 13,\ 14\}$.

同例 1 可验证 $n=5$，6 时，可求出全体完备递归采样值。(推导略)

由以上讨论可知，要判定任意 n 级 m 序列 $\{a_k\}$ 是否存在完备递归采样值，关键在于判别 $\varphi(2^n-1)/n$ 阶商群是否为循环群。当 $\varphi(2^n-1)/n$ 比较小时(如 $n=4$、5、6)，可验证 G 是否为循环群。但当 $\varphi(2^n-1)/n$ 很大时，一般难以判定 G 是否为循环群。但我们有以下充分条件。

定理 2　设 $\{a_k\}$ 为任意 n 级 m 序列，若 $\varphi(2^n-1)/n$ 无平方因子，则 $\{a_k\}$ 存在完备递归采样值。

证明　由文献 [3]，若 $\varphi(2^n-1)/n$ 无平方因子，则 $\varphi(2^n-1)/n$ 阶 Abel 群一定为循环群。

补充说明：(1) 当 $n=4$，5，6 时 $\varphi(2^n-1)/n$ 无平方因子，故完备采样值存在。

(2) 本定理只是一个充分条件，如 $n=7$ 时　$\varphi(2^n-1)/n$ 有平方因子，7 级 m 序列同样有完备采样值。

为了给出递归采样值的一个重要性质，首先引进文[3]中两个有关有限 Abel 群的结构定理。

引理 3　如果 Abel 群 A 的阶 $|A|=P_1^{a_1}P_2^{a_2}\cdots P_k^{a_k}$，$P_i\neq P_j$ 为素数，则 $A=A_1\times A_2\times\cdots\times A_k$，其中，$A_i=\{a\in A|a^{P_i^{a_i}}=1\}$，$|A_i|=P_i^{a_i}$，$i=1,2,\cdots,k$.

证明　见文[3](P_{39}).

引理 4　设 Abel 群 A 的阶为 P^a，P 为素数，则 A 为循环群的直积。

证明　见文[3](P_{40}).

由引理 3、4 可得：

引理 5 对任意 u，群 $G=Z_p^*/H=\{C_0,C_1,\cdots,C_{u-1}\}$（其中 $C_0=H,u=\varphi(2^n-1)/n$）为循环群的直积，即存在群元 C_{i1}，C_{i2}，…，$C_{ih}(h>1)$使

$$G=<C_{i1}>\times<C_{i2}>\times\cdots\times<C_{ih}>$$

定理 3 对任意 n 级 m 序列，一定存在正整数 $h(h>1)$，使得可找到 h 个递归采样值 s_1，s_2，…，s_h（等价次数分别为 $t_1,t_2,\cdots,t_h$）使得它们采样到的 $\sum_{i=1}^{h}t_i$ 个 m 序列除原序列外互不相同。

证明 由引理 5 及前面讨论易证，这里从略。

参 考 文 献

1 唐朝京，肖戎.m 序列完备递归采样法.国防科技大学学报，1990，12

2 肖国镇等.伪随机序列及应用.北京：国防工业出版社，1985

3 陈重穆.有限群论基础.重庆出版社，1983

Existence Condition of the Complete Recurrence Sampling Values of m-Sequences

Li Chao

(Department of System Engineering and Applied Mathematics)

Abstract

We discuss the existence condition for the complete recurrence sampling value of m-sequences. It is proved that for m-sequences of order n, the sufficient and necessary conditions that the complete recurrence sampling value exists are that the quotient group $G=Z_p^*/H(p=2^n-1,Z_p^*=\{s|(s,p)=1\},H=1,2^2,2^3,\cdots,2^n-1\})$ is cylcic group, and that the number of the complete recurrence sampling values is $n\cdot\varphi(\varphi(2^n-1)/n)$. In the end, we give some important characteristics of the complete recurrence sampling of m-sequences.

Key words sampling, m-sequeces, cyclic group