第 20 卷 第 6 期 电 子 科 学 学 刊 Vol.20 No.6
1998 年 11 月 JOURNAL OF ELECTRONICS Nov. 1998

关于本原 M 序列的自相关函数 [1]

曾凡鑫

(重庆通信学院电子线路教研室 重庆 400035)

摘 要 本文研究了本原 M 序列的自相关性能，首次获得了部份自相关函数的通解．这些通解的作用在于无需给出序列，只要知道反馈函数就可以获得相应的自相关函数值，大大降低了自相关函数的计算量．此外，还给出了自相关函数 $C(i)$ $(n < i \leq 2n-1)$ 的取值范围．

关键词 本原 M 序列，自相关函数，反馈函数，通解
中图号 TN911.3

1 引 言

当前，由于码分多址技术在通信中的广泛使用和测距、遥控、仿真等领域的需求，导致需要伪随机序列的数量越来越大．这些伪随机序列应具有良好的相关性、便于产生和有较大的等效长度等特性．迄今为止，人们获得的伪随机序列主要有移位寄存器序列 (即 m 和 M 序列)[1,2] 、 Gold 序列 [3] 、二次剩余序列 [4] 、 GMW 序列 [5] 、嵩忠雄序列 [6] 、 Bent 函数序列 [7] 、 No 序列 [8] 、 LZ 序列 [9] 等．在这些序列中，只有 M 序列拥有巨大数量，但是， M 序列又是研究得最不完善的序列．研究 M 序列是一项难度很大的工作，从 1946 年 de Bruijn 证明 M 序列存在以来，人们构造出的 M 序列的数量远远低于实际的数量， M 序列的自相关函数也只知道 [1,2] ： $C(i)=0(i=1,2,\cdots,n-1), C(n)=2^n-4w(f_o)$, 对于本原 M 序列 $C(n)=-4$, 而其余范围的 $C(i)(n<i<2^n-n)$ 完全不清楚，只能对具体序列一一计算来得到，这就巨大地制约了 M 序列的应用．

最近，作者获得了本原 M 序列一些自相关函数的一般性结论 [10,11], 如 $C(n+1)=-4$ 或 0 或 4．本文将对这一问题进一步讨论，获得的结论更多、更具有一般性．

2 理论准备

定义 1 n 级 m 序列 $\underline{a}=(a_1,a_2,\cdots,a_{2^n-1})$ 的反馈函数是 $f(x)=c_1x_n\star c_2x_{n-1}\star\cdots\star c_nx_1$, 如果 $a_k = c_1a_{k-1}\star c_2a_{k-2}\star\cdots\star c_na_{k-n}$ ．这里 " $\star$ " 表示模 2 和， $c_i=0$ 或 $1,(i=1,2,\cdots,n-1), c_n=1$ ．

定义 2 设有二元序列 $\underline{a}=(a_1,a_2,\cdots,a_t)$, $\underline{b}=(b_1,b_2,\cdots,b_t)$, 定义差序列为 $\underline{a}-\underline{b}=(a_1-b_1,\cdots,a_t-b_t)$ ．这里 " $-$ " 为普通减法， $\underline{a}$ 和 $\underline{b}$ 中的元素视为普通整数 0 和 1 ．

定义 3 设有二元序列 $\underline{a}$ 和 $\underline{b}$ 如定义 2, 称 $\underline{b}$ 为 $\underline{a}$ 的变换序列，如果 $b_k=1-2a_k, k=1,2,\cdots,t$ ．记为 $\underline{a}\to\underline{b}$ ．

定义 4 设有二元序列 $\underline{a}$ 和 $\underline{b}$ 如定义 2, $\underline{a}$ 和 $\underline{b}$ 的乘积序列定义为 $\underline{a}\,\underline{b}=(a_1b_1,a_2b_2,\cdots,a_tb_t)$ ．

[1] 1997-03-03 收到， 1998-02-25 定稿
重庆市中青年科技专家基金资助项目

引理 1 设有 $n(\geq 3$, 下同) 级 m 序列 $\underline{a}=(a_1,a_2,\cdots,a_{2^n-1})$, 其中 $a_i=0(i=1,2,\cdots,n-1),a_n=1,a_{2^n-1}=1$, 则 a_i 与反馈函数 $f(x)$ 的系数有如下关系

$$\begin{cases} a_{n+1}=c_1, \\ a_{n+2}=c_1\star c_2, \\ a_{n+3}=c_1\star c_3, \\ a_{n+4}=c_1\star\bar{c}_1c_2\star c_4, \\ \cdots\cdots, \end{cases} \text{和} \begin{cases} a_{2^n-2}=c_{n-1}, \\ a_{2^n-3}=c_{n-1}\star c_{n-2}, \\ a_{2^n-4}=c_{n-1}\star c_{n-3}, \\ a_{2^n-5}=c_{n-1}\star\bar{c}_{n-1}c_{n-2}\star c_{n-4}, \\ \cdots\cdots, \end{cases}$$

其中 $\bar{c}=1\star c$.

证明 $\underline{a}$ 是 n 级 m 序列, 所以满足递推关系式

$$a_k=c_1a_{k-1}\star c_2a_{k-2}\star\cdots\star c_na_{k-n}.$$

又因为序列 $(a_{2^n-5},a_{2^n-4},\cdots,a_{2^n-1},a_1,a_2,\cdots,a_{n-1},a_n,\cdots)$ 是 $\underline{a}$ 的一个等价周期序列, 故也满足这个递推关系式. 所以

$$\begin{aligned} a_{n+1}&=c_1a_n\star c_2a_{n-1}\star\cdots\star c_na_1, \\ a_{n+2}&=c_1a_{n+1}\star c_2a_n\star c_3a_{n-1}\star\cdots\star c_{n-1}a_3\star c_na_2, \\ a_{n-1}&=c_1a_{n-2}\star\cdots\star c_{n-2}a_1\star c_{n-1}a_{2^n-1}\star c_na_{2^n-2}. \end{aligned}$$

注意到 $a_i=0(i=1,2,\cdots,n-1),a_n=1,c_n=1,a_{2^n-1}=1$, 故有

$$\begin{aligned} &a_{n+1}=c_1 \\ &a_{n+2}=c_1a_{n+1}\star c_2=c_1^2\star c_2=c_1\star c_2, \\ &0=c_{n-1}\star a_{2^n-2}, \text{即} a_{2^n-2}=c_{n-1}. \end{aligned}$$

其余关系式同理可得. 证毕

引理 2 设有 n 级 m 序列 $\underline{a}$, $\underline{a}^t$ 和 $\underline{a}^{t+1}$ 是 $\underline{a}$ 的两个左移变换序列, 则差序列 $\underline{a}^t-\underline{a}^{t+1}$ 中的非零项必是 1 和 -1 相间出现.

证明 见文献 [11].

引理 3 设 $\underline{a}^f$ 和 $\underline{a}^t$ 是 n 级 m 序列 $\underline{a}$ 的两个左移序列, 且 $f\not\equiv t \bmod(2^n-1)$, 则存在 $\underline{a}$ 的一个左移序列 $\underline{a}^d$ 满足 $\underline{a}^f\star\underline{a}^t=\underline{a}^d$, 且如果 $\underline{a}^f\to\underline{b}^f,\underline{a}^t\to\bar{\underline{b}}^t,\underline{a}^d\to\underline{b}^d$, 则有 $\underline{b}^f\underline{b}^t=\underline{b}^d$.

证明 见文献 [2].

引理 4 设 $\underline{a}$ 是 n 级 M 序列, 则其自相关函数 $C(t)$ 满足: $4|C(t), C(t)=C(2^n-t)$.

证明 见文献 [12].

引理 5 同一等价类中的 M 序列具有相同的自相关函数.

证明 显然成立.

3 主要结果

根据引理 5, 我们可以不失一般性地将 n 级本原 M 序列表示为如下形式:

$$\underline{a}=(a_1,a_2,\cdots,a_{n-1},a_n,\cdots,a_f,a_{f+1},a_{f+2},\cdots,a_{2^n-1},a_{2^n}), \tag{1}$$

其中 $a_i=0(i=1,2,\cdots,n-1)$, $a_n=1$, $a_{2^n-1}=1$, $a_{2^n}=0$.

由本原 M 序列的构造法知 [1,2]: 序列 $\underline{D}=(a_1,a_2,\cdots,a_{n-1},a_n,\cdots,a_{2^n-1})$ 是 n 级 m 序列. 求二元 M 序列的自相关函数是在变换 $b_k=1-2a_k$ 下考虑下列两组序列对应位的异同数目:

$$\begin{array}{cccccccccc} a_1 & a_2 & \cdots & a_{2^n-t} & a_{2^n-t+1} & a_{2^n-t+2} & a_{2^n-t+3} & \cdots & a_{2^n-1} & a_{2^n} \\ a_t & a_{t+1} & \cdots & a_{2^n-1} & a_{2^n} & a_1 & a_2 & \cdots & a_{t-2} & a_{t-1} \end{array}$$

则自相关函数 $C(t-1)$ 为

$$C(t-1)=\sum_{i=1}^{2^n-t}b_ib_{t+i-1}+\sum_{i=1}^{t-2}b_ib_{2^n-t+i+1}+b_{2^n}b_{2^n-t+1}+b_{2^n}b_{t-1}. \tag{2}$$

又因为 $\underline{D}$ 是 m 序列, 故当 $2\le t\le 2^n$ 时, 其自相关函数为 -1 .

$$\begin{array}{cccccccccc} a_1 & a_2 & \cdots & a_{2^n-t} & a_{2^n-t+1} & a_{2^n-t+2} & a_{2^n-t+3} & \cdots & a_{2^n-1} \\ a_t & a_{t+1} & \cdots & a_{2^n-1} & a_1 & a_2 & a_3 & \cdots & a_{t-1} \end{array}$$

即有

$$\sum_{i=1}^{2^n-t}b_ib_{i+t-1}+\sum_{i=1}^{t-1}b_ib_{2^n-t+1}=-1. \tag{3}$$

将 (3) 式代入 (2) 式, 并注意到 $b_{2^n}=1$(因为 $a_{2^n}=0$), 简化后有

$$C(t-1)=-1-\sum_{i=1}^{t-1}b_ib_{2^n-t+1}+\sum_{i=1}^{t-2}b_ib_{2^n-t+i+1}+b_{2^n-t+1}+b_{t-1}. \tag{4}$$

利用变换 $b_k=1-2a_k$, $a_{2^n}=a_1=0$, 进一步可以将 (4) 式表示为 (5) 式和 (6) 式两种形式.

$$C(t-1)=-1+b_{2^n-t+1}+2\sum_{i=1}^{t-1}b_i(a_{2^n-t+i}-a_{2^n-t+i+1}), \tag{5}$$

$$C(t-1)=-4\sum_{i=1}^{t-1}a_i(a_{2^n-t+i}-a_{2^n-t+i+1}). \tag{6}$$

定理 1　设有 n 级 m 序列的反馈函数 $f(x)=c_1x_n\star c_2x_{n-1}\star\cdots\star c_nx_1$, 则由反馈函数 $f_1(x)=f(x)\star\bar{x}_2\bar{x}_3\cdots\bar{x}_n$ 构成的本原 M 序列的自相关函数 $C(n+i)(1\le i<n)$ 满足下列关系式:

(1) $C(n+1)=-4(c_{n-1}+c_1-1)$. 一般地, $C(n+1)=0$ 或 4 或 -4 .

(2) $C(n+2)=-4[(c_{n-2}\star c_{n-1})+(c_2\star c_1)-(c_1\star c_{n-1})-c_{n-1}c_1]$.

(3) $C(n+3)=-4[(c_{n-1}\star c_{n-3})+c_1(c_{n-1}\star c_{n-2})+c_{n-1}(c_1\star c_2)+(c_1\star c_3)$
$-c_1c_{n-1}-(c_{n-1}\star c_{n-2})-(c_1\star c_2)]$.

(4) $C(n+4)=-4[(c_{n-1}\star\bar{c}_{n-1}c_{n-2}\star c_{n-4})+c_2(1-2c_1)(c_{n-1}\star c_{n-2})$
$+(c_1\star\bar{c}_1c_2\star c_4)-\bar{c}_1(c_{n-1}\star c_{n-3})-\bar{c}_{n-1}(c_1\star c_3)-c_{n-1}(c_1\star c_2)]$.

证明　为节省篇幅, 只给出关系式 (1) 式的证明, 其余关系式同理可得.

将反馈函数 $f_1(x)$ 产生的本原 M 序列表示为 (1) 式，注意到 $a_i=0(i=1,2,\cdots,n-1)$,$a_n=1$, $a_{2^n-1}=1$, $a_{2^n}=0$, 令 $t=n+2$, 代入 (6) 式简化后有 $C(n+1)=-4(a_{2^n-2}+a_{n+1}-1)$. 再由引理 1, 得到 $C(n+1)=-4(c_{n-1}+c_1-1)$. 又因为 $c_i=0$ 或 $1(i=1,2,\cdots,n-1)$ 及引理 4, 故有 $C(n+1)=0$ 或 4 或 -4. 证毕

为了说明问题，我们给出以下三个例题.

例 1 反馈函数 $f_1(x)=x_1\star x_4\star\overline{x}_2\overline{x}_3\overline{x}_4(c_1=1,c_2=c_3=0)$, 产生的 4 级本原 M 序列为 0001111010110010. 计算表明： $C(5)=0$, $C(6)=0$, $C(7)=-4$.

例 2 反馈函数 $f_1(x)=x_1\star x_2\star x_4\star x_5\star\overline{x}_2\overline{x}_3\overline{x}_4\overline{x}_5(c_1=c_2=c_4=1,c_3=0)$, 产生的 5 级本原 M 序列为 00001101010010001011111011001110. 计算表明： $C(6)=-4$, $C(7)=0$, $C(8)=0$, $C(9)=4$.

例 3 反馈函数 $f_1(x)=x_1\star x_4\star\overline{x}_2\overline{x}_3\overline{x}_4\overline{x}_5(c_1=c_3=c_4=0,c_2=1)$, 产生的 5 级本原 M 序列为 00001010111011000111110011010010. 计算表明： $C(6)=4$, $C(7)=-4$, $C(8)=0$, $C(9)=0$.

注记 (1) 令 $t=n+1$ 代入 (6) 式直接有 $C(n)=-4$, 这一证明方法比文献 [1] 的证明过程更简洁、直观. 更重要的是本方法避免了使用权重的概念及其权重的计算.

(2) 三个例题表明： $C(n+1)$ 的值是本原 M 序列该项自相关函数的最紧的一般性结论.

(3) 得到本原 M 序列前必须首先知道反馈函数，定理 1 的作用在于无需给出序列就可以得到自相关函数值. 文献 [11] 也获得了 $C(n+1)=0$ 或 4 或 -4 的结果，但 $C(n+1)$ 具体取何值依赖于序列，而不是反馈函数.

定理 2 设有 n 级本原 M 序列为 (1) 式，如果 $a_fa_{f+1}\cdots a_{f+n-1}$ 是长度为 n 的 1-游程，则有 $C(f)=-4$.

证明 参见文献 [11].

定理 3 设有 n 级本原 M 序列为 (1) 式，如果 $a_fa_{f+1}\cdots a_{f+n-3}$ 是长度为 $n-2$ 的 1-游程，则有 $C(f-1)=0$ 或 -4.

证明 本定理利用引理 3 和引理 4 即可证明，详见文献 [11].

定理 4 任意 n 级本原 M 序列的自相关函数有

$$|C(n+i)|\le\begin{cases}4k, & \text{当}n=2k+1\text{时},\\ 4(k+1), & \text{当}n=2k+2\text{时},\end{cases}\quad 1\le i\le n-1.$$

证明 设有本原 M 序列 $\underline{a}$ 如 (1) 式，令 $t=n+i+1$, 代入 (6) 式后有

$$C(n+i)=-4\sum_{j=1}^{n+i}a_j(a_{2^n-n-i+j-1}-a_{2^n-n-i+j}).$$

又因为 $a_j=0(j=1,2,\cdots,n-1)$, 所以上式再简化为

$$C(n+i)=-4\sum_{j=n}^{n+i}a_j(a_{2^n-n-i+j-1}-a_{2^n-n-i+j}).\tag{7}$$

为节省篇幅，只证明 $n=2k+1$ 情况， $n=2k+2$ 情况同理可证.

(1) 当 $1 \le i \le 2k-1$ 时，根据引理 2, 差序列 $\underline{D}^{2^n-n-i-1} - \underline{D}^{2^n-n-i}$ 中的非零项只能是 1 和 -1 相间出现，而 a_i=0 或 1, 同时 (7) 中只有 $i+1(\le 2k)$ 项求和，故求和项至多出现 k 个 1 或者 -1 . 这个实事表明定理成立.

(2) 当 $i = 2k$ 时，根据引理 2 和 (7) 式中最后一项 $a_{2^n-1} - a_{2^n} = 1$, 故至多可能出现 $k+1$ 个 1 . 假设这种情况发生，(7) 式必定是如下形式：

$$(a_{2^n-i-1} - a_{2^n-i}, \cdots, a_{2^n-1} - a_{2^n}) = (1,-1,1,-1,\cdots,1,-1,1), \quad (k+1\text{个}1, k\text{个}-1);$$

$$(a_n, a_{n+1}, \cdots, a_{n+i}) = (1,0,1,0,\cdots,1,0,1), \qquad (k+1\text{个}1, k\text{个}0).$$

再由 $a_{2^n-1} = 1$, $a_{2^n} = 0$, 可以推出

$$(a_{2^n-i-1}, a_{2^n-i}, \cdots, a_{2^n-1}) = (1,0,1,0,\cdots,1,0,1), \qquad (k+1\text{个}1, k\text{个}0).$$

这说明在 m 序列 $\overline{D}$ 的一个周期中，有两个状态 $(a_n, a_{n+1}, \cdots, a_{n+i})$ 和 $(a_{2^n-i-1}, a_{2^n-i}, \cdots, a_{2^n-1})$ 相同，这是不可能的. 这个矛盾说明 (7) 中的求和项至多出现 k 个 1 或者 -1, 故定理成立. 证毕

注记 本定理的作用在于定出了 $C(n+i)(1 \le i \le n-1)$ 的取值范围.

参 考 文 献

[1] 万哲先，等. 非线性移位寄存器. 北京：科学出版社，1978, 第 2 章.

[2] 肖国镇，等. 伪随机序列及其应用. 北京：国防工业出版社，1985, 第 2 章，第 3 章.

[3] Gold R. Optimal binary sequences for spread spectrum multiplexing. IEEE Trans. on IT, 1967, IT-13(5): 619–621.

[4] Klapper A, *et al.* Cascaded GMW squences. IEEE Trans. on IT, 1993, IT-39(1): 177–183.

[5] Scholtz R A, *et al.* GWM Squences. IEEE Trans. on IT, 1982, IT-30(3): 548–553.

[6] Kasami T. Weight Distribution of Bose-Chaudhuri-Hocquenghen Code. In Combinational Mathematics and Its Applications. Chapel Hill, NC: Univ. of North Carolina Press, 1969.

[7] Olsen J D, *et al.* Bent-function sequences. IEEE Trans. on IT, 1982, IT-28(6): 858–864.

[8] No J S, *et al.* A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span. IEEE Trans. on IT, 1989, IT-35(2): 371–379.

[9] 李世鹏，等. 一类新的性能优越的伪随机序列. 电子学报，1993, 21(1): 41–51.

[10] 曾凡鑫. 一类 M 序列自相关函数的界. 电子学报，1996, 24(4): 127.

[11] 曾凡鑫. 关于本原 M 序列的一些自相关函数取值. 通信学报，1997, 18(9): 26–30.

[12] 章照止. 关于 M 序列的相关函数. 系统科学与数学. 1982, 2(4): 241- 251.

ON AUTOCORRELATION FUNCTIONS OF PRIMITIVE M-SEQUENCES

Zeng Fanxin

(*Chongqing Communication College, Chongqing* 400035)

Abstract In this paper, the self-correlation functions of primitive M-sequences are discussed, the general solutions of some autocorrelation functions are presented. These general solutions result in that the auto-correlation functions can be obtained by the feedback functions of M-sequences and need not to know the M-sequences. Therefore, the calculation for these functions is greatly reduced. Meanwhile, potential values of autocorrelation function $C(i)(n < i < 2n)$ are proposed as well.

Key words Primitive M-sequence, Autocorrelation function, Feedback function, General solution

曾凡鑫： 男，1964 年生，副教授，硕士，从事扩频通信、伪随机序列理论、通信中的差错控制理论、编码理论等的教学和科研工作.