第 22 卷 第 3 期 电子科学学刊 Vol.22 No.3
2000 年 5 月 JOURNAL OF ELECTRONICS May 2000

本原 de Bruijn 序列的几个性质 [1]

曾凡鑫

(重庆通信学院电子线路教研室 重庆 400035)

摘 要 本文讨论了二元本原 M 序列，证明了二元互反本原 M 序列具有相等的自相关函数和相等的线性复杂度，并给出了二元互反本原 M 序列的结构.

关键词 M 序列，本原多项式，自相关函数，线性复杂度

中图号 TN911.25

1 引 言

M 序列 (也称为 de Bruijn 序列) 以拥有巨大码字数量和高的线性复杂度而引人注目，它对于扩展频谱通信系统、码分多址通信系统、跳频通信系统和保密通信系统等存在着巨大的潜在应用价值．但由于缺乏强有力的数学工具，多年来， M 序列的研究进展缓慢．对于本原 M 序列 (即由 m 序列添加全零状态 $(0,0,\cdots,0)$ 构成的 M 序列) 来说，人们的认识相对多一些，自相关性能方面的研究成果可以参阅文献 [1–7]．特别地，文献 [1, 2] 给出了部份自相关函数的一般性定论，突破了多年来相应研究停滞不前的状态；线性复杂度方面的研究成果可以参阅文献 [7–9]; M 序列的构造与性质方面的研究成果可以参阅文献 [10–13]．

本原 M 序列是 M 序列家族中非常重要的子类，它是沟通其它 M 序列的桥梁，有许多 M 序列的构造都是建立在这个子类之上，因此，研究本原 M 序列自身固有性质更显得意义重大． 本文获得了本原 M 序列的互反等价性.

2 几个引理

定义 1 设有反馈多项式 $f(x)=1+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}+x^n$ ，则多项式 $\overline{f}(x)=x^nf(1/x)=1+c_{n-1}x+c_{n-2}x^2+\cdots+c_1x^{n-1}+x^n$ 称为 $f(x)$ 的互反多项式.

定义 2 设序列 $\underline{a}$ 由多项式 $f(x)$ 生成，序列 $\underline{b}$ 由 $\overline{f}(x)$ 产生，则称 $\underline{a}$ 与 $\underline{b}$ 为互反序列且 $\underline{b}$ 是 $\underline{a}$ 的互反序列。

引理 1 $f(x)$ 与 $\overline{f}(x)$ 同时为本原多项式或者同时不是本原多项式 [6]．

引理 2 任意一个本原多项式产生唯一一个 m 序列 (平移等价序列视为相等)[6]．

引理 3 设 $\underline{a}=(a_1a_2\cdots a_{n-1}a_n\cdots a_{2^n-1})$ 是一个由多项式 $f(x)$ 产生的 n 级 m 序列，其中 $a_j=0(j=1,2,\cdots,n-1)$, 则 $\underline{b}=(a_oa_1a_2\cdots a_{n-1}a_n\cdots a_{2^n-1})$ 是一本原 M 序列 [5]．这里 $a_o=0$ 并称 M 序列 $\underline{b}$ 是由本原多项式 $f(x)$ 产生的本原 M 序列.

这三个引理说明了任一本原 M 序列必对应着一个互反本原 M 序列，从互反角度来说，本原 M 序列只有 $\phi(2^n-1)/(2n)$ 个序列是非互反序列 ($\phi(\cdot)$ 为欧拉函数， n 为本原 M 序列

[1] 1998-08-19 收到， 1999-06-26 定稿
重庆市中青年科技专家基金资助项目

的阶)．互反 m 序列间更深入的内在关系由引理 4 给出，它是确定互反本原 M 序列间内在关系的基础．

引理 4 设本原多项式 $f(x)$ 产生的 $n(\geq 3)$ 级 m 序列为 $\underline{a}=(a_1a_2\cdots a_{2^n-2}a_{2^n-1})$, 则互反多项式 $\overline{f}(x)$ 产生的的 n 级 m 序列为 $\underline{b}=(a_{2^n-1}a_{2^n-2}\cdots a_2a_1)$．

证明 由引理 1 和引理 2, $\overline{f}(x)$ 也产生一个 m 序列．

设 $(a_j,a_{j+1},\cdots,a_{j+n-1})$ 为序列 $\underline{a}$ 的任意一个状态，则该状态的后继状态为 $(a_{j+1},\cdots,a_{j+n-1},a_{j+n})$, 即有

$$a_{j+n}=c_1a_{j+n-1}+c_2a_{j+n-2}+\cdots+c_{n-1}a_{j+1}+a_j. \tag{1}$$

再设 $(a_k,a_{k-1},\cdots,a_{k-n+1})$ 是任意一个状态，将其代入多项式 $\overline{f}(x)$ 有

$$c_{n-1}a_{k-n+1}+c_{n-2}a_{k-n+2}+\cdots+c_1a_{k-1}+a_k\triangleq W. \tag{2}$$

由 (1) 式

$$a_k=c_1a_{k-1}+c_2a_{k-2}+\cdots+c_{n-1}a_{k-n+1}+a_{k-n}, \tag{3}$$

将 (3) 式代入 (2) 式，并注意这里的运算“+”是模 2 加，故得到： $W=a_{k-n}$．这说明状态 $(a_k,a_{k-1},\cdots,a_{k-n+1})$ 的后继状态是 $(a_{k-1},a_{k-2},\cdots,a_{k-n+1},a_{k-n})$, 即序列 $\underline{b}$ 满足互反多项式 $\overline{f}(x)$．再由引理 2, 序列 $\underline{b}$ 由多项式 $\overline{f}(x)$ 生成． 证毕

例 1 本原多项式 $f(x)=1+x^2+x^5$ 和其互反本原多项式 $\overline{f}(x)=1+x^3+x^5$ 产生的 5 级 m 序列分别为

$\underline{a}$: 0000101011101100011111001101001．

$\underline{b}$: 1001011001111100011011101010000．

例 2 本原多项式 $f(x)=1+x+x^2+x^4+x^5$ 和其互反本原多项式 $\overline{f}(x)=1+x+x^3+x^4+x^5$ 产生的 5 级 m 序列分别为

$\underline{h}$: 0000110101001000101111101100111．

$\underline{r}$: 1110011011111010001001010110000．

3 本原 M 序列的性质

定理 1 设本原多项式 $f(x)$ 产生的 $n(\geq 3)$ 级 M 序列为 $\underline{a}=(a_0a_1a_2\cdots a_{2^n-2}a_{2^n-1})$, 则互反多项 $\overline{f}(x)$ 产生的本原 n 级 M 序列 $\underline{b}=(a_{2^n-1}a_{2^n-2}\cdots a_2a_1a_0)$．

证明 由引理 3 和引理 4 直接得到． 证毕

注 1: 本定理反映了互反本原 M 序列的内在结构关系，其关系为互为倒序排列．

定理 2 设本原 M 序列 $\underline{a}$ 和 $\underline{b}$ 分别由本原多项式及其互反多项式生成，则 $\underline{a}$ 和 $\underline{b}$ 的自相关函数相同．

证明 设本原 M 序列为 $\underline{a}=(a_0a_1a_2\cdots a_{2^n-2}a_{2^n-1})$, 则由定理 1, 本原 M 序列 $\underline{b}=(a_{2^n-1}a_{2^n-2}\cdots a_2a_1a_o)$．再设 $\underline{a}$ 的自相关函数为 $C_a(t)$ $(0\leq t\leq 2^n-1)$, 则自相关函数

$C_a(t)=A(t)-B(t)$[5]．其中 $A(t)$ 为下面两序列对应位相同的个数，$B(t)$ 为下面两序列对应位不同的个数．

$$\begin{matrix} a_0 & a_1 & a_2 & \cdots & a_{2^n-t-1} & a_{2^n-t} & a_{2^n-t+1} & \cdots & a_{2^n-1} \\ a_t & a_{t+1} & a_{t+2} & \cdots & a_{2^n-1} & a_0 & a_1 & \cdots & a_{t-1} \end{matrix} \tag{4}$$

相应地，$\underline{b}$ 的自相关函数为 $C_b(t)=A_1(t)-B_1(t)$ $(0\le t\le 2^n-1)$．其中 $A_1(t)$ 为下面两序列对应位相同的个数，$B_1(t)$ 为下面两序列对应位不同的个数．

$$\begin{matrix} a_{2^n-1} & a_{2^n-2} & \cdots & a_{t+1} & a_t & a_{t-1} & a_{t-2} & \cdots & a_1 & a_0 \\ a_{2^n-t-1} & a_{2^n-t-2} & \cdots & a_1 & a_0 & a_{2^n-1} & a_{2^n-2} & \cdots & a_{2^n-t+1} & a_{2^n-t} \end{matrix} \tag{5}$$

注意到两序列对应位相同与不同的个数与对应位排列的次序无关，将 (5) 式上下两行交换后有

$$\begin{matrix} a_{2^n-t-1} & a_{2^n-t-2} & \cdots & a_1 & a_0 & a_{2^n-1} & a_{2^n-2} & \cdots & a_{2^n-t+1} & a_{2^n-t} \\ a_{2^n-1} & a_{2^n-2} & \cdots & a_{t+1} & a_t & a_{t-1} & a_{t-2} & \cdots & a_1 & a_0 \end{matrix} \tag{6}$$

再交换 (6) 式中的对应项次序，显然可以将 (6) 式化为 (4) 式，这就意味着 $A(t)=A_1(t)$，$B(t)=B_1(t)$，即 $C_a(t)=C_b(t)$．　　证毕

例 3　例 1 中两 m 序列构成的本原 M 序列的自相关函数计算结果，见表 1．

例 4　例 2 中两 m 序列构成的本原M序列的自相关函数计算结果，见表 2．

注 2：本定理反映了互反本原 M 序列的自相关函数间关系，在求自相关函数时计算量可以减少一半．

表 1　自相关函数取值比较

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	$t>16$
$C_a(t)$	32	0	0	0	0	−4	4	−4	0	0	−8	4	0	−4	−4	4	−8	$C_a(32-t)$
$C_b(t)$	32	0	0	0	0	−4	4	−4	0	0	−8	4	0	−4	−4	4	−8	$C_b(32-t)$

表 2　自相关函数取值比较

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	$t>16$
$C_h(t)$	32	0	0	0	0	−4	−4	0	0	4	−8	0	4	−4	−4	0	0	$C_h(32-t)$
$C_r(t)$	32	0	0	0	0	−4	−4	0	0	4	−8	0	4	−4	−4	0	0	$C_r(32-t)$

线性复杂度是度量一个序列使用是否安全的一个重要度量指标，低的线性复杂度意味着高的破译能力．已证明：M 序列的线性复杂度满足关系 $2^{n-1}+n\le C(\underline{a})\le 2^n-1$[8,9]．下述定理给出了互反本原 M 序列线性复杂度的一个重要性质．

定义 3　设有多项式 $g(x)=1+\sum_{j=1}^{m}h_jx^j$(其中 $h_m=1$) 和序列 $\underline{a}=(a_1a_2\cdots a_p)$，并设 $\underline{a}$ 满足多项式 $g(x)$，即 $a_{i+m}+\sum_{j=1}^{m}h_ja_{i+m-j}=0$(序列下标模 p)．则 $\underline{a}$ 的线性复杂度 $C(\underline{a})$ 为 $\underline{a}$ 所满足的多项式中最小的多项式次数[8]．

定理 3　设本原 M 序列 $\underline{a}$ 和 $\underline{b}$ 分别由本原多项式及其互反多项式生成，则 $C(\underline{a})=C(\underline{b})$．

证明　(1) $C(\underline{b})\le C(\underline{a})$

设 $\underline{a}=(a_0a_1a_2\cdots a_{2^n-2}a_{2^n-1})$ 则由定理 1 有 $\underline{b}=(a_{2^n-1}a_{2^n-2}\cdots a_2a_1a_0)$ 。再设 $C(\underline{a})=m$, 由定义 3 有

$$a_{i+m}+\sum_{j=1}^{m}h_ja_{i+m-j}=0 \quad (\text{序列下标模 } 2^n). \tag{7}$$

为了便于讨论，记 $\underline{b}=(b_ob_1b_2\cdots b_{2^n-1})$ 。显然 $b_k=a_{2^n-1-k}$ $(k=0,1,2,\cdots,2^n-1)$ 。

取多项式 $g_1(x)=1+\sum_{j=1}^{m-1}h_jx^{m-j}+x_m$, 将序列 $\underline{b}$ 代入后得到

$$b_{i+m}+\sum_{j=1}^{m-1}h_jb_{i+m-(m-j)}+b_{i+m-m}=b_{i+m}+\sum_{j=1}^{m-1}h_jb_{i+j}+b_i,$$

代入 $b_i=a_{2^n-1-i}$ 后并应用 (7) 式得到

$$\begin{aligned}&a_{2^n-1-i-m}+\sum_{j=1}^{m-1}h_ja_{2^n-1-i-j}+a_{2^n-1-i}\\&=a_{2^n-1-i}+\sum_{j=1}^{m}h_ja_{2^n-1-i-j}=0.\end{aligned}$$

这个关系表明序列 $\underline{b}$ 满足多项式 $g_1(x)$, 即 $C(\underline{b})\le m=C(\underline{a})$ 。

(2) $C(\underline{a})\le C(\underline{b})$

因为 $\underline{a}$ 也是 $\underline{b}$ 的互反序列，所以同理于 (1) 必有该不等式成立。

综上所述，定理成立。 证毕

注 3：本定理给出了互反本原 M 序列的线性复杂度间的关系，使线性复杂度的分析量减少了一半。

例 5 用文献 [7] 所提供的周期为 2^n 的序列的线性复杂度快速算法验证例 1 和例 2 中 m 序列构成的本原 M 序列，其结果为

$$C(\underline{a})=C(\underline{b})=31,\quad C(\underline{h})=C(\underline{r})=31.$$

4 结束语

互反本原 M 序列不仅自相关函数、线性复杂度相等，而且两序列在结构上也互为倒序排列，知道其中一个，另一个也就清楚了，所以我们可以认为互反本原 M 序列在互反意义下是“相等”的，为简便，称之为“互反等价性”。从而本原 M 序列只有 $\phi(2^n-1)/(2n)$ 个序列不同。

参考文献

[1] 曾凡鑫. 关于本原 M 序列的自相关函数. 电子科学学刊, 1998, 20(6): 775–780.

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

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

[4] 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.

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

[6] 万哲先. 代数与编码. 北京: 科学出版社, 1976, 第 3 章.

[7] 杨先义, 等. 编码密码学. 北京: 人民邮电出版社, 1992, 第 18 章, 第 19 章.

[8] Etzion T, *et al.* Construction of de Bruijn sequences of minimal complexity. IEEE Trans. on IT., 1984, IT-30(5): 705–709.

[9] Chan A H, *et al.* On the complexities of de Bruijn sequences. J. Combin. Theory, Ser. A, 1982, 33(2): 233–246.

[10] 康庆德. 关于 de Bruijn 序列. 通信学报, 1991, 12(6): 69–76.

[11] 康庆德. 求 GF(q) 上全部 M 序列的剪接方法. 应用数学学报, 1984, 7(1): 78–85.

[12] 高鸿勋. 求全部 n 级 M 序列及其反馈函数的一个方法与证明. 应用数学学报, 1979, 2(4): 316–324.

[13] 苏驷希, 等. 从非奇异布尔函数对产生 M 序列. 电子学报, 1997, 25(1): 106–109.

SOME PROPERTIES ON PRIMITIVE de Bruijn SEQUENCES

Zeng Fanxin

(*Chongqing Communication Institute*, *Chongqing* 400035)

Abstract The binary primitive M-sequences are discussed in this paper. It is shown that arbitrary two reciprocal primitive M-sequences have the same auto-correlation function and the equal linear complexity, meanwhile, the configuration of the two M-sequences is proposed.

Key words M-sequence, Primitive polynomial, Auto-correlation function, Linear complexity

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、编码理论等的教学与科研工作.