一类稀疏序列的最小周期

胡予濮
(西安电子科技大学 ISN 国家重点实验室,信息安全研究所,陕西西安 710071)

摘 要: 稀疏序列用于数字信号处理技术.针对作者所给出的一类稀疏序列,本文给出此类序列的若干有实用价值的构造方法,这些构造方法使得其最小周期达到最大.

关键词: 稀疏序列; 信息隐藏; 最小周期; 线性复杂度
中图分类号: TN918.1 **文献标识码**: A **文章编号**: 0372-2112 (2003) 04-0616-04

The Least Period of a Class of Sparse-Sequences

HU Yu-pu
(*ISPI, ISN National Key Lab., Xidian University, Xi'an, Shaanxi* 710071, *China*)

Abstract: For a class of sparse-sequences presented by Yupu Hu, this paper gives several methods of construction which have practical application value, to maximize the least period.

Key words: sparese sequence; information hiding; the least period; linear complexity

1 引言

稀疏序列[1]在数字信号处理,特别是在隐藏技术[2]中有广泛的应用.稀疏序列的伪随机性仍然包括极大的周期、高线性复杂度、良好的游程分布等[3].文献[1]给出了一类稀疏序列,并指出此类序列的绝大多数具有很大的最小周期(由于此类序列的最小周期是 2 的幂,因此大的最小周期也意味着大的线性复杂度),但没有说明如何得到最小周期大的序列.本文给出此类序列的若干实用构造方法,使得其最小周期达到最大.

定义 1[1] 设 $a = a_0 a_1 a_2 \cdots$ 是 $GF(2)$ 上的序列,最小周期为 P,在一个最小周期内 1 的个数为 M,称 $D = M/P$ 是序列 a 的密度.若 $D \ll 1/2$,则称 a 为稀疏序列.

定义 2[1] 设有 $GF(2)$ 上的 n 级 m 序列 $a_0 a_1 a_2 \cdots$.取集合 $\{1,2,\cdots,n-1\}$.对于子集 $J \subset \{1,2,\cdots,n-1\}$,若 $a_t = 1$,则输出乘积 $\prod_{j\in J} a_{t+j}$(当子集 J 是空集时,定义 $\prod_{j\in J} a_{t+j} = 1$);否则放弃输出; $t = 0,1,2,\cdots$.如此得到输出序列 $b_0 b_1 b_2 \cdots$ 记为 $b(J)$,称其为基于 m 序列 a 的自缩乘积序列.

定理 1[1] 设自缩乘积序列族 $\{b(J), J \subset \{1,2,\cdots,n-1\}\}$.则有

(1) 每个序列的最小周期都形如 $2^l (0 \le l \le n-1)$,因此线性复杂度大于 2^{l-1}.

(2) 任意固定 $k = 1,2,\cdots,n-2$,最小周期小于 2^{n-k} 的自缩乘积序列所占的比例不多于 2^{-k}.

(3) 固定 m,从 $\{1,2,\cdots,n-1\}$ 中随机地取出 m 个元素组成子集 J, $b(J)$ 的最小周期小于 2^l 的概率记为 $Pr(m,l)$.则当 $m \ge l$ 时 $Pr(m,l) \ge l$ 时 $Pr(m,l) = 1$;当 $m < l$ 时 $Pr(m,l) \ge (C_{n-1}^{m} - C_{l-1}^{m})/C_{n-1}^{m}$.

本文以下将通过设计集合 J 来构造最小周期达到最大的自缩乘积序列.

2 情形一($J = \{1,2,\cdots,k\}$)

引理 1 取定序列 $b(J)$,取定一个 j,设 $b_j = a_{l+1} a_{l+2} \cdots a_{l+k}$(注意到此时有 $a_l = 1$).则 $b_j b_{j+1} = 11$ 当且仅当 $a_{l+1} a_{l+2} \cdots a_{l+k} a_{l+k-1} = 11\cdots11$.

证明 由定义 2 可知充分性是显然的.如果 $b_j b_{j+1} = 11$,则 $b_{j+1} = a_{l+2} a_{l+3} \cdots a_{l+k+1}$,因此必要性也为真.引理 1 得证.

引理 2 取定序列 $b(J)$.取定一个 j,设 $b_j = a_{l+1} a_{l+2} \cdots a_{l+k}$(此时有 $a_l = 1$),则

$$b_{j-1} b_j \cdots b_{j+m-1} b_{j+m} = 01\cdots10$$

当且仅当 $a_{l-1} a_l \cdots a_{l+m+k-1} a_{l+m+k} = 011\cdots10$.

证明 这是引理 1 的自然推论.引理 2 得证.

定理 2 取定序列 $b(J)$,其中 $J = \{1,2,\cdots,k\}$.则在其连续的 2^{n-1} 个输出比特中, $b(J)$ 具有如下的"1"游程分布:

"1"游程的长度	$n-k$	$n-k-2$	$n-k-3$	$n-k-4$	$\cdots$	1
"1"游程的个数	1	1	2	2^2	$\cdots$	2^{n-k-3}

因此 $b(J)$ 的最小周期为 2^{n-1}.

证明 根据引理 2 以及 m-序列的游程分布,本定理的结论是显然的.定理 2 得证.

收稿日期:2001-09-17;修回日期:2002-04-03
基金项目:国家自然科学基金(No. 60273084);受 ISN 国家重点实验室开放课题基金(No. 5-03)

3　情形一的第一种推广

为了统一起见,以下所说的"m-序列 a 的极小多项式 $f(x)=1+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}+x^n$"总是指 m-序列 a 满足线性递归关系:$a_t=c_1a_{t-1}+c_2a_{t-2}+\cdots+c_{n-1}a_{t-n+1}+a_{t-n}$. 对于集合 J,以下总记 $J(m)=\{u\mid u-m\in J\}$. 对于 $j_1\in J$, $j_2\in J$, $j_1<j_2$ 如果不存在 $j_3\in J$ 使得 $j_1<j_3<j_2$,则称 j_1 与 j_2 在 J 内是相邻的,并且称 j_2-j_1 为 j_1 与 j_2 在 J 内的距离.

在本节中总设集合 J 满足以下两个条件:

条件 1　设 k 是集合 J 中的最大的元素. 对任何 J 内是相邻的元素 j_1 与 j_2,它们的距离 j_2-j_1 小于 $n-k$.

条件 2　$1\in J$.

引理 3　取定序列 $b(J)$,取定一个 j,设 $b_j=\prod_{u\in J}a_{l+u}$(此时有 $a_l=1$). 则 $b_jb_{j+1}=11$ 当且仅当 $a_{l+u}=1$ 对每一个 $u\in J\cup J(1)$ 成立.

证明　如果 $b_jb_{j+1}=11$,则 $b_j=\prod_{u\in J}a_{l+u}=1$,说明 $a_{l+1}=1$,因此 $b_{j+1}=\prod_{u\in J(1)}a_{l+u}$,必要性为真. 反之如果 $a_{l+u}=1$ 对每一个 $u\in J\cup J(1)$ 成立,则 $b_j=1$, $a_{l+1}=1$,因此 $b_{j+1}=\prod_{u\in J}a_{l+1+u}=\prod_{u\in J(1)}a_{l+u}=1$,充分性为真. 引理 3 得证.

引理 4　取定序列 $b(J)$,取定一个 j,设 $b_j=\prod_{u\in J}a_{l+u}$(此时有 $a_l=1$). 则:$b_jb_{j+1}\cdots b_{j+n-k-1}b_{j+n-k}=11\cdots10$,当且仅当 $a_la_{l+1}\cdots a_{l+n-1}a_{l+n}=11\cdots10$

证明　根据本情形的条件 1～条件 2 以及引理 3, $b_jb_{j+1}\cdots b_{j+n-k-1}b_{j+n-k}=11\cdots10$ 当且仅当:对于 $u\in J\cup J(1)\cup J(2)\cup\cdots\cup J(n-k-1)$ 总有 $a_{l+u}=1$ 成立,且对于 $u\in J(n-k)$ 不总有 $a_{l+u}=1$. 但

$$J\cup J(1)\cup J(2)\cup\cdots\cup J(n-k-1)=\{1,2,\cdots,n-1\}$$

$$J(n-k)-\{J\cup J(1)\cup J(2)\cup\cdots\cup J(n-k-1)\cup\}=\{n\}$$

因此 $b_jb_{j+1}\cdots b_{j+n-k-1}b_{j+n-k}=11\cdots10$,当且仅当 $a_la_{l+1}\cdots a_{l+n-1}a_{l+n}=11\cdots10$. 引理 4 得证.

定理 3　取定序列 $b(J)$,其中集合 J 满足条件 1 和条件 2. 则在其连续的 2^{n-1} 个输出比特中, $b(J)$ 具有唯一长度为 $n-k$ 的"1"游程. 因此 $b(J)$ 的最小周期为 2^{n-1}.

证明　设 $b_j=\prod_{u\in J}a_{l+u}$(注意到此时有 $a_l=1$). 由引理 4, $b_jb_{j+1}\cdots b_{j+n-k-1}b_{j+n-k}=11\cdots10$,当且仅当 $a_la_{l+1}\cdots a_{l+n-1}a_{l+n}=11\cdots10$. 注意到 m-序列 a 在其一个最小周期内有唯一的最长"1"游程,长度为 n. 这就是说,当 $a_la_{l+1}\cdots a_{l+n-1}a_{l+n}=11\cdots10$ 时,必有 $a_{l-1}=0$. 此时 b_{j-1} 只能为 0,否则与引理 3 矛盾. 故当 j 跑遍 $\{0,1,2,\cdots2^{n-1}-1\}$ 时,有唯一的 j 使得 $b_{j-1}b_jb_{j+1}\cdots b_{j+n-k-1}b_{j+n-k}=011\cdots10$. 定理 3 得证

此外不难证明,长度为 $n-k$ 的"1"游程是序列 $b(J)$ 最长的"1"游程.

4　情形一的第二种推广

设集合 J 满足以下两个条件:

条件 4.1　$J=J_0\cup\{m+1\}$,设 k 是集合 J_0 中的最大的元素,对任何 J_0 内相邻的元素 j_1 与 j_2,它们的距离 j_2-j_1 小于 $m-k$,且 $m-k=n-m$.

条件 4.2　$1\in J$.

引理 5　取定序列 $b(J)$,其中集合 J 满足条件 4.1 和条件 4.2. 则 $b(J)$ 的输出比特不会有连续 $m-k+1$ 个"1".

证明　取定一个 j,设 $b_j=\prod_{u\in J}a_{l+u}$(注意到此时有 $a_l=1$). 则类似于引理 3 和引理 4 的证明容易得到:$b_jb_{j+1}\cdots b_{j+m-k-1}b_{j+m-k}=11\cdots11$ 当且仅当 $a_{l+u}=1$ 对每一个 $u\in J(1)\cup J(2)\cup\cdots\cup J(m-k)$ 成立. 但

$$J\cup J(1)\cup J(2)\cup\cdots\cup J(m-k)=(J_0\cup J_0(1)\cup J_0(2)\cup\cdots\cup J_0(m-k)\cup\{m+1,m+2,\cdots,m+1+m-k\}=\{1,2,\cdots,m\}\cup\{m+1,m+2,\cdots,n+1\}=\{1,2,\cdots,n+1\}$$

这说明 m-序列 a 有长度大于 n 的"1"游程,矛盾. 引理得证.

引理 6　取定序列 $b(J)$,其中集合 J 满足条件 4.1 和条件 4.2. 取定一个 j,设 $b_j=\prod_{u\in J}a_{l+u}$(此时有 $a_l=1$). 则 $b_jb_{j+1}\cdots b_{j+m-k-1}=11\cdots1$ 当且仅当:$a_{l+u}=1$ 对每一个 $u\in\{1,2,\cdots,m-1\}\cup\{m+1,m+2,\cdots,n\}$ 成立;且 $a_{l+m}=0$.

证明　注意到 $\{1,2,\cdots,m-1\}\cup\{m+1,m+2,\cdots,n\}=J\cup J(1)\cup J(2)\cup\cdots\cup J(m-k-1)$. 类似于引理 3 和引理 4 的证明,充分性为真. 如果 $b_jb_{j+1}\cdots b_{j+m-k-1}=11\cdots1$,则显然 $b_{j+1}=\prod_{u\in J(1)}a_{l+u}$, $b_{j+2}=\prod_{u\in J(2)}a_{l+u}$, $\cdots$, $b_{j+m-k-1}=\prod_{u\in J(m-k-1)}a_{l+u}$; $a_{l+u}=1$ 对每一个 $u\in\{1,2,\cdots,m-1\}\cup\{m+1,m+2,\cdots,n\}$ 成立. 此时必须有 $a_{l+m}=0$,不然 $a_{l+u}=1$ 对每一个 $u\in\{0,1,2,\cdots,n\}$ 成立,即 m-序列 a 有长度大于 n 的"1"游程. 必要性为真. 引理 6 得证.

定理 4　取定序列 $b(J)$,其中集合 J 满足条件 4.1 和条件 4.2. 又设 m-序列 a 的极小多项式 $f(x)=1+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}+x^n$ 满足 $c_{n-m}=1$. 则在其连续的 2^{n-1} 个输出比特中, $b(J)$ 具有唯一的最长"1"游程,其长度为 $m-k$. 因此 $b(J)$ 的最小周期为 2^{n-1}.

证明　因为 $c_{n-m}=1$,所以 m-序列 a 存在这样的 l,使得:$a_{l+u}=1$ 对每一个 $u\in\{0,1,2,\cdots,m-1\}\cup\{m+1,m+2,\cdots,n\}$ 成立;且 $a_{l+m}=0$. 又显然这样的 l 在 $\{0,1,2,\cdots,2^n-2\}$ 中是唯一的. 取定此 l,设 $b_j=\prod_{u\in J}a_{l+u}$. 由引理 6, $b_jb_{j+1}\cdots b_{j+m-k-1}=11\cdots1$, $b_{j-1}=0$, $b_{j+m-k}=0$,且这样的 j 在 $\{0,1,2,\cdots,2^{n-1}-1\}$ 中是唯一的. 定理 4 得证

定理 4 还可以进一步推广. 有如下的

推论 1　取定序列 $b(J)$,其中集合 J 满足以下两个条件:

(1) $J=J_0\cup\{m+1\}$,设 k 是集合 J_0 中的最大的元素,对任何 J_0 内相邻的元素 j_1 与 j_2,它们的距离 j_2-j_1 小于 $m-k$,且 $m-k=n-1-m+M$,其中 M 为正整数;

(2) $1\in J$.

又设 m-序列 a 的极小多项式 $f(x)=1+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}+x^n$ 满足 $c_{n-m}c_{n-m+1}\cdots c_{n-m-1+M}=11\cdots1$. 则在

其连续的 2^{n-1} 个输出比特中，$b(J)$ 具有唯一的最长“1”游程，其长度为 $m-k$. 因此 $b(J)$ 的最小周期为 2^{n-1}.

证明 类似于引理 5，$b(J)$ 的输出比特不会有连续 $m-k+1$ 个“1”.

类似于引理 6，我们有：设 $b_j=\prod_{u\in J}a_{l+u}$（此时有 $a_l=1$），则 $b_jb_{j+1}\cdots b_{j+m-k-1}=11\cdots1$ 当且仅当：$a_{l+u}=1$ 对每一个 $u\in\{1,2,\cdots,m-1\}\cup\{m+1,m+2,\cdots,n-1+M\}$ 成立；且 $a_{l+m}=0$.

因为 $c_{n-m}c_{n-m+1}\cdots c_{n-m-1+M}=11\cdots1$，所以 m-序列 a 存在这样的 l，使得：

$a_{l+u}=1$ 对每一个 $u\in\{0,1,2,\cdots,m-1\}\cup\{m+1,m+2,\cdots,n-1+M\}$ 成立，且 $a_{l+m}=0$. 又显然这样的 l 在 $\{0,1,2,\cdots,2^n-2\}$ 中是唯一的. 取定此 l，设 $b_j=\sum_{u\in J}a_{l+u}$. 由以上的讨论得知，$b_jb_{j+1}\cdots b_{j+m-k-1}=11\cdots1$，$b_{j-1}=0$，$b_{j+m-k}=0$，且这样的 j 在 $\{0,1,2,\cdots,2^{n-1}-1\}$ 中是唯一的. 推论 2 得证.

5 情形二（$J=\{2,3,\cdots,k\}$，$k\geq3$）

引理 7 取定序列 $b(J)$，取定一个 j，设 $b_j=a_{l+2}a_{l+3}\cdots a_{l+k}$（注意到此时有 $a_l=1$）. 则 $b_jb_{j+1}b_{j+2}=111$ 当且仅当以下两种情况之一发生：

(1) $a_{l+1}a_{l+2}\cdots a_{l+k}a_{l+k+1}a_{l+k+2}=11\cdots111$；

(2) $a_{l+1}=0$，$a_{l+2}\cdots a_{l+k+1}a_{l+k+2}a_{l+k+3}=1\cdots111$.

证明 由定义 2 可知，情况(1)发生时 $b_jb_{j+1}b_{j+2}=111$；情况(2)发生时 $b_{j+1}=a_{l+4}a_{l+5}\cdots a_{l+k+2}$，$b_{j+2}=a_{l+5}a_{l+6}\cdots a_{l+k+3}$，因此也有 $b_jb_{j+1}b_{j+2}=111$；充分性为真.

设 $b_jb_{j+1}b_{j+2}=111$. 此时必有 $a_{l+2}a_{l+3}=11$. 当 $a_{l+1}=1$ 时，$b_{j+1}=a_{l+3}a_{l+4}\cdots a_{l+k+1}$，$b_{j+2}=a_{l+4}a_{l+5}\cdots a_{l+k+2}$，因此 $a_{l+1}a_{l+2}\cdots a_{l+k}a_{l+k+1}a_{l+k+2}=11\cdots111$，当 $a_{l+1}=0$ 时，$b_{j+1}=a_{l+4}a_{l+5}\cdots a_{l+k+2}$，$b_{j+2}=a_{l+5}a_{l+6}\cdots a_{l+k+3}$，因此 $a_{l+2}\cdots a_{l+k+1}a_{l+k+2}a_{l+k+3}=1\cdots111$. 必要性为真. 引理 7 得证.

引理 8 取定序列 $b(J)$，取定一个 j，设 $b_j=a_{l+2}a_{l+3}\cdots a_{l+k}$（此时有 $a_l=1$）. 则对于任何固定的 $m\geq3$，$b_jb_{j+1}\cdots b_{j+m-1}b_{j+m}=11\cdots10$ 当且仅当以下两种情况之一发生：

(1) $a_{l+1}a_{l+2}\cdots a_{l+k+m-2}a_{l+k+m-1}=11\cdots11$，$a_{l+k+m}=0$；

(2) $a_{l+1}=0$，$a_{l+2}\cdots a_{l+k+m-2}a_{l+k+m-1}a_{l+k+m}=1\cdots111$，$a_{l+k+m+1}=0$；

证明 由引理 7 的证明可知充分性是显然的.

设 $b_jb_{j+1}\cdots b_{j+m-1}b_{j+m}=11\cdots10$. 此时 $a_{l+1}a_{l+2}a_{l+3}$ 的取值只有两种可能：$a_{l+1}a_{l+2}a_{l+3}=111$ 或 $a_{l+1}a_{l+2}a_{l+3}=011$.

当 $a_{l+1}a_{l+2}a_{l+3}=111$ 时，由递推过程容易得：

$b_{j+1}=a_{l+3}a_{l+4}\cdots a_{l+k+1}$，$b_{j+2}=a_{l+4}a_{l+5}\cdots a_{l+k+2}\cdots b_{j+m-1}=a_{l+m+1}a_{l+m+2}\cdots a_{l+k+m-1}$，$b_{j+m}=a_{l+m+2}a_{l+m+3}\cdots a_{l+k+m}$.

因此 $a_{l+1}a_{l+2}\cdots a_{l+k+m-2}a_{l+k+m-1}=11\cdots11$，$a_{l+k+m}=0$.

当 $a_{l+1}a_{l+2}a_{l+3}=011$ 时，由递推过程容易得：

$b_{j+1}=a_{l+4}a_{l+5}\cdots a_{l+k+2}$，$b_{j+2}=a_{l+5}a_{l+6}\cdots a_{l+k+3}$，$\cdots$，$b_{j+m-1}=a_{l+m+2}a_{l+m+3}\cdots a_{l+k+m}$，$b_{j+m}=a_{l+m+3}a_{l+m+4}\cdots a_{l+k+m+1}$.

必要性为真. 引理 8 得证.

定理 5 取定序列 $b(J)$，其中 $J=\{2,3,\cdots,k\}$，$k\geq3$. 设 m-序列 a 的极小多项式为 $f(x)=1+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}+x^n$.

(1) 如果 $c_{n-1}=0$，则 $b(J)$ 在连续 2^{n-1} 个输出比特中有唯一的最长“1”游程，长度为 $n-k$；

(2) 如果 $c_{n-1}=1$，则 $b(J)$ 在连续 2^{n-1} 个输出比特中有唯一的最长“1”游程，长度为 $n-k+1$. 而无论如何，$b(J)$ 的最小周期均为 2^{n-1}.

证明 取定一个 j，设 $b_j=a_{l+2}a_{l+3}\cdots a_{l+k}$.

(1) 由引理 8 得，$b_jb_{j+1}\cdots b_{j+n-k-1}b_{j+n-k}=11\cdots10$，当且仅当以下两种情况之一发生：

① $a_la_{l+1}a_{l+2}\cdots a_{l+n-2}a_{l+n-1}=111\cdots11$，$a_{l+n}=0$；

② $a_l=1$，$a_{l+1}=0$，$a_{l+2}\cdots a_{l+n-2}a_{l+n-1}a_{l+n}=1\cdots111$，$a_{l+n+1}=0$.

注意到 a 是 n 级 m-序列. 因此当 l 跑遍 $\{0,1,2,\cdots,2^n-2\}$ 时情况②不会出现，而情况①只出现唯一一次，且此时必须有 $a_{l-1}=0$. 又注意到 $c_{n-1}=0$，故必须有 $a_{l-2}=0$. 再根据引理 8，$b_{j-1}=0$.

(2) 由引理 8 得，$b_jb_{j+1}\cdots b_{j+n-k}b_{j+n-k+1}=11\cdots10$ 当且仅当以下两种情况之一发生：

① $a_la_{l+1}a_{l+2}\cdots a_{l+n-1}a_{l+n}=111\cdots11$，$a_{l+n+1}=0$；

② $a_l=1$，$a_{l+1}=0$，$a_{l+2}\cdots a_{l+n-1}a_{l+n}a_{l+n+1}=1\cdots111$，$a_{l+n+2}=0$.

注意到 a 是 n 级 m-序列，因此当 l 跑遍 $\{0,1,2,\cdots,2^n-2\}$ 时情况①不会出现，又注意到 $c_{n-1}=1$，故情况②只出现唯一一次，再根据引理 8，$b_{j-1}=0$. 定理 5 得证.

6 情形二的推广

在本节中总设集合 J 满足以下两个条件：

条件 1 设 k 是集合 J 中的最大的元素，对任何 J 内是相邻的元素 j_1 与 j_2，它们的距离 j_2-j_1 小于 $n-k$.

条件 6.2 $1\notin J$，$2\in J$，$3\in J$.

以下引理 9 和引理 10 的证明类似于引理 7 和引理 8.

引理 9 取定序列 $b(J)$，取定一个 j，设 $b_j=\prod_{u\in J}a_{l+u}$，则 $b_jb_{j+1}b_{j+2}=111$ 当且仅当以下两种情况之一发生：

① $a_l=1$，$a_{l+1}=1$，且 $a_{l+u}=1$ 对每一个 $u\in J\cup J(1)\cup J(2)$ 成立；

② $a_l=1$，$a_{l+1}=0$，且 $a_{l+u}=1$ 对每一个 $u\in J\cup J(1)\cup J(2)$ 成立；

引理 10 取定序列 $b(J)$，取定一个 j，设 $b_j=\prod_{u\in J}a_{l+u}$. 则 $b_jb_{j+1}\cdots b_{j+m-1}b_{j+m}=11\cdots10$，当且仅当以下两种情况之一发生：

① $a_l=1$，$a_{l+1}=1$，$a_{l+u}=1$ 对每一个 $u\in J\cup J(1)\cup J(2)\cup\cdots\cup j(m-1)$ 成立，$a_{l+m+k}=0$；

② $a_l=1$，$a_{l+1}=0$，$a_{l+u}=1$ 对每一个 $u\in J\cup J(2)\cup J(3)$

$\cup\cdots\cup J(m)$ 成立, $a_{l+m+k+1}=0$.

定理 6　取定序列 $b(J)$, 其中 J 满足条件 6.1 和条件 6.2. 设 m-序列 a 的极小多项式为 $f(x)=1+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}+x^n$.

(1) 如果 $c_{n-1}=0$, 则 $b(J)$ 在连续 2^{n-1} 个输出比特中有唯一的最长"1"游程, 长度为 $n-k$;

(2) 如果 $c_{n-1}=1$, 则 $b(J)$ 在连续 2^{n-1} 个输出比特中有唯一的最长"1"游程, 长度为 $n-k+1$; 而无论如何, $b(J)$ 的最小周期均为 2^{n-1}.

证明　取定一个 j, 设 $b_j=\prod_{u\in J}a_{l+u}$.

(1) 由引理 10 得, $b_jb_{j+1}\cdots b_{j+n-k-1}b_{j+n-k}=11\cdots10$ 当且仅当以下两种情况之一发生.

① $a_{l+u}=1$ 对每一个 $u\in\{0,1\}\cup J\cup J(1)\cup J(2)\cup\cdots\cup J(n-k-1)=\{0,1,2,\cdots,n-1\}$ 成立, $a_{l+n}=0$;

② $a_{l+u}=0$, $a_{l+u}=1$ 对每一个 $u\in\{0\}\cup J\cup J(2)\cup J(3)\cup\cdots\cup J(n-k)=\{0,2,3,\cdots,n\}$ 成立, $a_{l+n+1}=0$. n 级 m-序列 a 使得情况 ②不会出现, 而情况 ①只出唯一一次, 且此时必须有 $a_{l-1}=0$. 又注意到 $c_{n-1}=0$, 故必须有 $a_{l-2}=0$. 再根据引理 8, $b_{j-1}=0$.

(2) 由引理 10 得, $b_jb_{j+1}\cdots b_{j+n-k}b_{j+n-k+1}=11\cdots10$, 当且仅当以下两种情况之一发生:

① $a_{l+u}=1$ 对每一个 $u\in\{0,1\}\cup J\cup J(1)\cup J(2)\cup\cdots\cup J(n-k)=\{0,1,2,\cdots,n\}$ 成立, $a_{l+n+1}=0$;

② $a_{l+u}=0$, $a_{l+u}=1$ 对每一个 $u\in\{0\}\cup J\cup J(2)\cup J(3)\cup\cdots\cup J(n-k+1)=\{0,2,3,\cdots,n\}$ 成立, $a_{l+n+2}=0$.

n 级 m-序列 a 使得情况 ①不会出现, 又注意到 $c_{n-1}=1$, 故情况 ②只出现唯一一次. 再根据引理 8, $b_{j-1}=0$. 定理 6 得证.

7　结论

本文给出了自缩乘积的若干构造方法, 使得其最小周期达到最大. 这些构造方法是简单实用的. 此外我们看到, 在密度相同的前提下, 情形一的"1"游程分布比较偏向于长游程, 而将情形一推广以后, 以及情形二, "1"游程分布则更加发散. 情形一和情形二还可以进一步推广, 使得最小周期达到最大的同时使得游程分布更加发散.

参考文献:

[1] 胡予濮, 杨波. 伪随机稀疏序列的研究 [J]. 电子学报, 2002, 30(1): 142 - 144.

[2] Stefan Katzenbeisser, Fafien A P Petitcolas, ed, Information Hiding Techniques for Steganography and Digital Watermarking [C]. Boston, USA. Artech House, Inc, 2000.

[3] 丁存生, 肖国镇. 流密码学及其应用 [M]. 北京: 国防工业出版社, 1994, §3.3～§3.6, 49 - 69.