广义自缩序列的游程长度

孙红波, 胡予濮, 高军涛
(1. 北京电子科技学院, 北京 100010; 2. 西安电子科技大学通信工程学院, 陕西西安 710071;
3. 西安电子科技大学计算机网络与信息安全教育部重点实验室, 陕西西安 710071)

摘 要: 广义自缩序列是一类新型的序列密码. 游程长度是衡量序列伪随机性质的一个重要指标, 一个好的伪随机序列应该具有短的游程长度. 本文利用 m 序列的伪随机性质, 研究了广义自缩序列的游程长度, 得到如下结果: 广义自缩序列族中除两个序列(全 0 序列和全 1 序列)外, 其余序列的游程长度不超过 $n\times n-2.5n+3$, 在 n 为偶数的情况下, 游程长度不超过 $n\times n/2-1.25n+3$.

关键词: m-序列; 游程长度; 自缩生成器; 互缩生成器; 流密码
中图分类号: TN918 文献标识码: A 文章编号: 0372-2112 (2007) 04-0679-06

Run-Lengths of Generalized Self-Shrinking Sequences

SUN Hong-bo, HU Yu-pu, GAO Jun-tao
(1. *Beijing Electronic Science and Technology Institute, Beijing 100010, China;*
2. *Telecommunication Engineering College, Xidian University, Xi'an, Shaanxi 710071, China;*
3. *Key Laboratory of CNIS, Xidian University, Xi'an, Shaanxi 710071, China*)

Abstract: Generalized self-shrinking sequences are a novel class of stream ciphers. Run-lengths is an important criterion to measure the pseudorandom property of sequences. A good pseudorandom sequence should have short run-lengths. In this paper, by using some pseudorandom properties of m-sequences, we obtain a new result about family of the generalized self-shrinking sequences. It is that the run-lengths of each sequence in the sequences family, with the exception of two sequences(000… and 111…), are no greater than $n*n-2.5n+3$, and no greater than $n*n/2-1.25n+3$ if n is even.

Key words: m-sequence; run-length; self-shrinking generator; shrinking generator; stream cipher

1 引言

伪随机序列在密码技术(如流密码)和通信技术(如 CDMA)中有广泛的应用. 衡量一个周期序列的伪随机性有很多的指标, 比如最小周期, 自相关性质, 均衡性质, 游程分布性质等等. 在密码应用中, 要考虑的一个重要方面就是序列生成的简洁性, 基于上述的考虑, D. Coppersmith 等提出了"互缩生成器[1]". Meier 和 Staffelbach 提出了"自缩生成器[2]", 该生成器可以看作是互缩生成器的一个特例, 其生成的自缩序列具有较好的性质: 最小周期为 2 的幂次, 生成简单, 且序列是均衡的, 因此提出之后受到了广泛的关注[3~7]. 但是自缩序列的密钥选择范围太小, 并不适合直接作为密钥序列. 作为互缩生成器的特例和自缩生成器的推广, 我们提出了"广义自缩生成器[8,9]", 其定义如下:

定义 1 设 $GF(2)$ 上的 m 序列 $a=\cdots a_{-2}a_{-1}a_0a_1\cdots$, 周期为 2^n-1, 向量 $\boldsymbol{G}=(g_0, g_1, \cdots, g_{n-1})\in GF(2)^n$, 定义序列 $v=v_0v_1v_2\cdots$, 其中

$$v_k=g_0a_k+g_1a_{k-1}+\cdots+g_{n-1}a_{k-n+1},\ k=0,1,2,\cdots$$

若 $a_k=1$, 则输出 v_k, 否则放弃输出. 这样得到的输出序列 $b(\boldsymbol{G})=b_0b_1b_2\cdots$, 称为基于 m 序列 a 的广义自缩序列. 称序列族 $B(a)=\{b(\boldsymbol{G}), \boldsymbol{G}\in GF(2)^n\}$ 为基于 m 序列 a 的广义自缩序列族.

该生成器的结构仍然非常简单, 且序列族 $B(a)$ 具有良好的互相关性质, 均衡性质, 其中大部分序列的最小周期达到最大等等[8,9]. 下面给出关于序列族 $B(a)$ 的两个平凡的性质, 这两个性质在本文中将会用到:

(1) 序列 000…和 111…都属于 $B(a)$;

(2) 对于 $B(a)$ 中任意一个序列 $b_0b_1b_2\cdots$, 其补序列 $(1+b_0)(1+b_1)(1+b_2)\cdots$ 也属于 $B(a)$.

本文我们主要研究广义自缩序列的游程长度, 结

收稿日期: 2005-11-17; 修回日期: 2006-09-09
基金项目: 国家自然科学基金(No. 60673072); 武器装备预研基金(No. 51436030105DZ0105)

果表明, 除了两个序列 000…和 111…外, 序列族 $B(a)$ 中其它序列的游程长度不超过 $n^2-2.5n+3$, 当 n 为偶数时, 游程长度不超过 $n^2/2-1.25n+3$. 为了得到这个结果, 我们需要证明两个关于 m-序列的命题. 从现在开始, 设 m-序列 a 的极小多项式为: $f(x)=c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}+c_nx^n$, 这里 $c_0=c_n=1$, 为证明简单起见, 总是假设 $n\geqslant 5$, m-序列的 n 长串记为 $\bar{a}_k=(a_ka_{k+1}\cdots a_{k+n-1})$.

2 族 $B(a)$ 中序列的游程长度

设序列 $b(\boldsymbol{G})=b_0b_1b_2\cdots$, 称序列的一个 T 长串 $b_jb_{j+1}b_{j+2}\cdots b_{j+T-1}=11\cdots1$ 为长度为 T 的 1 游程, 称 T 长串 $b_jb_{j+1}b_{j+2}\cdots b_{j+T-1}=00\cdots0$ 为长度为 T 的 0 游程. 序列的游程长度 T 是衡量序列伪随机性质的一个重要指标, 人们希望所得序列的游程长度不要太长. 下面的定理 1 和推论指出除了 000…和 111…两个序列之外, 广义自缩序列族中所有序列的游程长度有一个非常好的上界:

定理 1 对于任意的 $b(\boldsymbol{G})\in B(a)$, $b(\boldsymbol{G})\neq 0000\cdots$, $b(\boldsymbol{G})\neq 1111\cdots$, $b(\boldsymbol{G})$ 的游程长度不超过 $n^2-2.5n+3$.

推论 设 n 为偶数, 对于任意的 $b(\boldsymbol{G})\in B(a)$, $b(\boldsymbol{G})\neq 0000\cdots$, $b(\boldsymbol{G})\neq 1111\cdots$, $b(\boldsymbol{G})$ 的游程长度不超过 $n^2/2-1.25n+3$.

本文后面的部分主要用来推导定理 1 和推论, 第 3 部分证明了两个所需的命题, 第四部分证明定理 1 和推论.

3 关于 m 序列的两个命题

定义 2 设 $\{t_j\mid j=0,1,2,\cdots\}$, 其中 $0\leqslant t_0<t_1<t_2<\cdots$, 对于每一个 j, $a_{t_j}=1$, 对于每一个 $t\notin\{t_j\mid j=0,1,2,\cdots\}$, $a_t=0$. 称 t_j 为序列族 $B(a)$ 的第 j 个输出时刻, $\{t_0,t_1,t_2,\cdots\}$ 为序列族 $B(a)$ 的输出时刻序列.

设 m-序列 a 的 n 长串记为 $\bar{\boldsymbol{a}}_k=(a_ka_{k+1}\cdots a_{k+n-1})$, 则 m-序列 a 的极小多项式系数 $(c_1c_2\cdots c_n)$ 满足下面的线性方程:

$$\begin{bmatrix}\bar{a}_1\\ \bar{a}_2\\ \vdots\\ \bar{a}_n\end{bmatrix}\begin{bmatrix}c_n\\ c_{n-1}\\ \vdots\\ c_2\\ c_1\end{bmatrix}=\bar{a}_{n+1}^{\mathrm{T}} \tag{1}$$

且 $n\times n$ 矩阵 $\begin{bmatrix}\bar{a}_1\\ \bar{a}_2\\ \vdots\\ \bar{a}_n\end{bmatrix}$ 是可逆的.

命题 1 设 $(a_{i+1}a_{i+2}\cdots a_{i+2n})$, $i\in\{0,1,\cdots,2^n-2\}$ 是 m-序列 a 的一个 $2n$ 长的比特串, 则 m-序列 a 中不包含下面类型的 $(a_{i+1}a_{i+2}\cdots a_{i+2n})$:

(1) $(a_{i+1}a_{i+2}\cdots a_{i+2n})$ 的 Hamming 重量为 0;

(2) $(a_{i+1}a_{i+2}\cdots a_{i+2n})$ 的 Hamming 重量为 1;

(3) $(a_{i+1}a_{i+2}\cdots a_{i+2n})$ 的 Hamming 重量为 $2n-1$;

(4) $(a_{i+1}a_{i+2}\cdots a_{i+2n})$ 的 Hamming 重量为 $2n$;

证明: 由 m 序列的性质, 可知上述命题成立. 证毕.

命题 2 m-序列 a 中不包含 Hamming 重量为 2 的串 $(a_{i+1}a_{i+2}\cdots a_{i+2n})$, $i\in\{0,1,\cdots,2^n-2\}$.

首先来看下面的 7 个引理:

引理 1 假设 m-序列 a 中 $2n$ 长的比特串 $(a_1a_2\cdots a_{2n})$ 的 Hamming 重量为 2, 则两个 n 长的比特串 $(a_1a_2\cdots a_n)$ 和 $(a_{n+1}a_{n+2}\cdots a_{2n})$ 的 Hamming 重量都为 1, 比特串 $(a_1a_2\cdots a_{2n})$ 必定是下面的三种情况之一:

(1) $a_n=1$, $a_{n+j}=1$, 这里 $1<j\leqslant n/2$;

(2) $a_i=1$, $a_{n+1}=1$, 这里 $n/2+1\leqslant i<n$;

(3) $a_i=1$, $a_{n+j}=1$, 这里 $1\leqslant i<n$, $1<j\leqslant n$, $(i-j)\geqslant n/2$.

证明: 设比特串 $(a_1a_2\cdots a_{2n})$ 的 Hamming 重量为 2, 则

第一, 比特串 $(a_1a_2\cdots a_n)$ 和 $(a_{n+1}a_{n+2}\cdots a_{2n})$ 的 Hamming 重量都为 1, 因为 n 级 m 序列中不包含长度超过 n 的 0 串.

第二, $a_i=1$, $a_{n+j}=1$, 这里 $1\leqslant i\leqslant n$, $1\leqslant j\leqslant n$. 如果 $i<j$, 则 $(a_{i+1}a_{i+2}\cdots a_{i+n})=(00\cdots0)$, 矛盾; 如果 $i=j$, 则 $(a_1a_2\cdots a_n)=(a_{n+1}a_{n+2}\cdots a_{2n})$, 矛盾; 因此必有 $i>j$.

第三, $a_i=1$, $a_{n+j}=1$, 这里 $n\geqslant i>j\geqslant 1$. 定义 $\bar{a}_k$ 为 $\bar{\boldsymbol{a}}_k=(a_ka_{k+1}\cdots a_{k+n-1})$, 这里 $k=1,2,\cdots,n+1$

当 $k\in\{1,2,\cdots,j\}$, $\bar{\boldsymbol{a}}_k$ 的 Hamming 重量为 1, $\bar{\boldsymbol{a}}_k$ 的分量等于 1 的位置分别为 $\{i,i-1,\cdots,i-j+2,i-j+1\}$;

当 $k\in\{j+1,j+2,\cdots,i\}$, $\bar{\boldsymbol{a}}_k$ 的 Hamming 重量为 2;

当 $k\in\{i+1,i+2,\cdots,n+1\}$, $\bar{\boldsymbol{a}}_k$ 的 Hamming 重量为 1, $\bar{\boldsymbol{a}}_k$ 的分量等于 1 的位置分别为 $\{j+n-i,j+n-i-1,\cdots,j+1,j\}$;

假设 $2(i-j)<n$, 即 $i-j+1\leqslant j+n-i$, 这意味着集合 $\{i,i-1,\cdots,i-j+2,i-j+1\}\cap\{j+n-i,j+n-i-1,\cdots,j+1,j\}$ 非空. 现在假设 $u\in\{i,i-1,\cdots,i-j+2,i-j+1\}\cap\{j+n-i,j+n-i-1,\cdots,j+1,j\}$. 则存在 $k_1\in\{1,2,\cdots,j\}$ 和 $k_2\in\{i+1,i+2,\cdots,n+1\}$ 使得向量 $\bar{\boldsymbol{a}}_{k_1}$ 和 $\bar{\boldsymbol{a}}_{k_2}$ 的分量等于 1 的位置都是 u, 因此 $\bar{\boldsymbol{a}}_{k_1}=\bar{\boldsymbol{a}}_{k_2}$, 矛盾. 所以有 $2(i-j)\geqslant n$.

第四, 设 $a_i=1$, $a_{n+j}=1$, 这里 $n\geqslant i>j\geqslant 1$ 并且 $2(i$

$-j) \geqslant n$. 假设 $i=n, j=1$, 则 $(a_1a_2\cdots a_n)=(0\cdots01)$, $(a_{n+1}a_{n+2}\cdots a_{2n})=(10\cdots0)$. 在这种情况下, $f(x)$ 等于它的互反多项式, 因此序列 a 不是 $m-$ 序列, 矛盾.

综上所述, 我们得到下面的结论:

若 $i=n$, 则 $1<j\leqslant n/2$;

若 $j=1$, 则 $n/2+1\leqslant i<n$;

若 $1\leqslant i<n$ 且 $1<j\leqslant n$, 则 $(i-j)\geqslant n/2$. 证毕.

引理 **2**　m-序列 a 中不包含长为 $2n$ 的比特串 $(a_1a_2\cdots a_{2n})$ 使得串 $(a_1a_2\cdots a_n)$ 和 $(a_{n+1}a_{n+2}\cdots a_{2n})$ 的 Hamming 重量都为 1 且 $a_n=1, a_{n+j}=1$, 这里 $1<j\leqslant n/2$.

证明: 用反证法, 假设存在满足上述条件的长为 $2n$ 的比特串 $(a_1a_2\cdots a_{2n})$, 注意到系数 $(c_1c_2\cdots c_n)$ 满足等式 (1).

设 $n=(u+1)j-v$, 这里 $0\leqslant v<j$. 若 $v=0$, 则等式 (1) 的解必定为

$(c_1c_2\cdots c_j)=(00\cdots01), (c_{j+1}c_{j+2}\cdots c_{2j})=(00\cdots01), \cdots, (c_{uj+1}c_{uj+2}\cdots c_n)=(00\cdots01)$.

因此 $f(x)=1+x^j+x^{2j}+\cdots+x^n$, 其互反多项式与其相等. 矛盾.

若 $0<v<j$, 则等式 (1) 的解必定为:

$(c_1\cdots c_j)=(00\cdots01), (c_{j+1}\cdots c_{2j})=(00\cdots01), \cdots, (c_{(u-1)j+1}\cdots c_{uj})=(00\cdots01), (c_{uj+1}\cdots c_n)=(00\cdots0)$.

因此 $c_n=0\neq1$, 矛盾. 所以 m-序列 a 中不包含这样的比特串 $(a_1a_2\cdots a_{2n})$. 证毕.

引理 **3**　m-序列 a 中不包含长为 $2n$ 的比特串 $(a_1a_2\cdots a_{2n})$ 使得串 $(a_1a_2\cdots a_n)$ 和 $(a_{n+1}a_{n+2}\cdots a_{2n})$ 的 Hamming 重量都为 1 且 $a_i=1$, 这里 $n/2+1\leqslant i<n$, $a_{n+1}=1$.

证明: m-序列 a 的逆序列 a^* 也是一个 m 序列, 由引理 2, 序列 a^* 中不含有上述串的逆串, 因此序列 a 中不包含长为 $2n$ 的比特串 $(a_1a_2\cdots a_{2n})$ 使得串 $(a_1a_2\cdots a_n)$ 和 $(a_{n+1}a_{n+2}\cdots a_{2n})$ 的 Hamming 重量都为 1 且 $a_i=1$, 这里 $n/2+1\leqslant i<n$, $a_{n+1}=1$. 证毕.

现在假设 $2n$ 长的比特串 $(a_1a_2\cdots a_{2n})$ 满足下面的条件: $(a_1a_2\cdots a_n)$ 和 $(a_{n+1}a_{n+2}\cdots a_{2n})$ 的 Hamming 重量都为 1, 且 $a_i=1, a_{n+j}=1$, 这里 $1\leqslant i<n, 1<j\leqslant n, (i-j)\geqslant n/2$. 在这个假设条件下, 等式 (1) 可以表示为:

$$(c_{n-i+1}, c_{n-i+2}, \cdots, c_{n-i+j})=(0,0,\cdots,0,1) \quad (2)$$

$$(c_1+c_{n-i+j+1}, c_2+c_{n-i+j+2}, \cdots, c_{i-j}+c_n)=(0,0,\cdots,0) \quad (3)$$

$$(c_{i-j+1}, c_{i-j+2}, \cdots, c_{n-j})=(0,0,\cdots,0) \quad (4)$$

下面引理 4~7 的证明都基于上述的假设

引理 **4**　如果 $n-i+j$ 是 n 的一个因子, 那么等式 (2)~(4) 的解必为下面的形式: $(0,0,\cdots,0,1)=(c_1,c_2,\cdots,c_{(n-i+j)})=(c_{(n-i+j)+1}, c_{(n-i+j)+2}, \cdots, c_{2(n-i+j)})=\cdots=(c_{(i-j)+1}, c_{(i-j)+2}, \cdots, c_n)$.

证明: 假设 $n=u\times(n-i+j)$, 则 $i-j=n-(n-i+j)=(u-1)\times(n-i+j)$. 把等式 (2)~(4) 中的项分为两部分: 第一部分为:

$(c_{n-i+1}, c_{n-i+2}, \cdots, c_{n-i+j})=(0,0,\cdots,0,1)$,

$(c_{(k-1)\times(n-i+j)+n-i+1}+c_{k\times(n-i+j)+n-i+1}, c_{(k-1)\times(n-i+j)+n-i+2}+c_{k\times(n-i+j)+n-i+2}, \cdots, c_{k\times(n-i+j)}+c_{(k+1)\times(n-i+j)})=(0,0,\cdots,0)$, $k=1,2,\cdots,u-1$,

$(c_{(u-1)\times(n-i+j)+1}, c_{(u-1)\times(n-i+j)+2}, \cdots, c_{(u-1)\times(n-i+j)+n-i})=(0,0,\cdots,0)$.

其中第一部分包含的系数集合为:

$$\bigcup_{k=1}^{u}\{c_{(k-1)\times(n-i+j)+n-i+1}, c_{(k-1)\times(n-i+j)+n-i+2}, \cdots, c_{k\times(n-i+j)}\},$$

第二部分包含的系数集合为:

$$\bigcup_{k=1}^{u}\{c_{(k-1)\times(n-i+j)+1}, c_{(k-1)\times(n-i+j)+2}, \cdots, c_{(k-1)\times(n-i+j)+n-i}\}.$$

上述两个集合没有交叠, 且

$$\bigcup_{k=1}^{u}\{c_{(k-1)\times(n-i+j)+n-i+1}, c_{(k-1)\times(n-i+j)+n-i+2}, \cdots, c_{k\times(n-i+j)}\} \bigcup_{k=1}^{u}\{c_{(k-1)\times(n-i+j)+1}, c_{(k-1)\times(n-i+j)+2}, \cdots, c_{(k-1)\times(n-i+j)+n-i}\}=\{c_1, c_2, \cdots, c_n\}$$

由第一部分, 我们可以得到

$\bigcup_{k=1}^{u}\{c_{(k-1)\times(n-i+j)+n-i+1}, c_{(k-1)\times(n-i+j)+n-i+2}, \cdots, c_{k\times(n-i+j)}\}$ 的值.

$$\begin{aligned}(0,0,\cdots,0,1)&=(c_{n-i+1}, c_{n-i+2}, \cdots, c_{(n-i+j)})\\&=(c_{(n-i+j)+n-i+1}, c_{(n-i+j)+n-i+2}, \cdots, c_{2(n-i+j)})\\&=\cdots\\&=(c_{(u-1)\times(n-i+j)+n-i+1}, c_{(u-1)\times(n-i+j)+n-i+2}, \cdots, c_n).\end{aligned}$$

由第二部分, 我们可以得到 $\bigcup_{k=1}^{u}\{c_{(k-1)\times(n-i+j)+1}, c_{(k-1)\times(n-i+j)+2}, \cdots, c_{(k-1)\times(n-i+j)+n-i}\}$ 的值.

$$\begin{aligned}(0,0,\cdots,0)&=(c_{(u-1)\times(n-i+j)+1}, c_{(u-1)\times(n-i+j)+2}, \cdots, c_{(u-1)\times(n-i+j)+n-i})\\&=(c_{(u-2)\times(n-i+j)+1}, c_{(u-2)\times(n-i+j)+2}, \cdots, c_{(u-2)\times(n-i+j)+n-i})\\&=\cdots\\&=(c_1, c_2, \cdots, c_{n-i}).\end{aligned}$$

证毕.

引理 **5**　如果 $n=u\times(n-i+j)-1$, 那么 $n\times n$ 矩阵 $\begin{bmatrix}\overline{a_1}\\ \overline{a_2}\\ \vdots\\ \overline{a_n}\end{bmatrix}$ 的秩为 $n-1$.

证明 $n = u \times (n - i + j) - 1$, 则有下面的两个等式:

$i - j + 1 = (u - 1) \times (n - i + j) + 1 = (u - 1) \times (n - i + j)$,

$n - j = u \times (n - i + j) - (j + 1) = (u - 1) \times (n - i + j) + (n - i)$

将等式 (4)分成四部分

第一部分为:

$(0, 0, \cdots, 0, 1)$,

$j) + n - i + 1$,

$c_{(k-1)\times(n-i+j)+n-i+2} + c_k \times (n-i+j)+n-i+2, \cdots, c_k \times (n-i+j) + c_{(k+1)\times(n-i+j)} = (0, 0, \cdots, 0)$, 其中 $k = 1, 2, \cdots, u - 2$,

$(c_{(u-2)\times(n-i+j)+n-i+1} + c_{(u-1)\times(n-i+j)+n-i+1}, c_{(u-2)\times(n-i+j)+n-i+2} + c_{(u-1)\times(n-i+j)+n-i+2}, \cdots, c_{(u-1)\times(n-i+j)-1} + c_n) = (0, 0, \cdots, 0)$.

第二部分为:

$(c_{(k-1)\times(n-i+j)+1} + c_k \times (n-i+j)+1, c_{(k-1)\times(n-i+j)+2} + c_k \times (n-i+j)+2, \cdots, c_{(k-1)\times(n-i+j)+n-i-1} + c_k \times (n-i+j)+n-i-1) = (0, 0, \cdots, 0)$, 其中 $k = 1, 2, \cdots, u - 1$,

$(c_{(u-1)\times(n-i+j)+1}, c_{(u-1)\times(n-i+j)+2}, \cdots, c_{(u-1)\times(n-i+j)+n-i-1}) = (0, 0, \cdots, 0)$.

第三部分为:

$c_{(k-1)\times(n-i+j)+n-i} + c_k \times (n-i+j)+n-i = 0$, 其中 $k = 1, 2, \cdots, u - 1$.

第四部分为:

$$c_{(u-1)\times(n-i+j)} = 0.$$

注意到以下的事实:

(1) 第一部分包含的系数集合为:

$\bigcup_{k=1}^{u} \{c_{(k-1)\times(n-i+j)+n-i+1}, c_{(k-1)\times(n-i+j)+n-i+2}, \cdots, c_k \times (n-i+j)\} \cup \{c_{(u-1)\times(n-i+j)+n-i+1}, c_{(u-1)\times(n-i+j)+n-i+2}, \cdots, c_n\}$.

(2) 第二部分包含的系数集合为:

$\bigcup_{k=1}^{u} \{c_{(k-1)\times(n-i+j)+1}, c_{(k-1)\times(n-i+j)+2}, \cdots, c_{(k-1)\times(n-i+j)+n-i-1}\}$

(3) 第三部分包含的系数集合为:

$$\bigcup_{k=1}^{u} \{c_{(k-1)\times(n-i+j)+n-i}\}.$$

(4) 第四部分包含的系数集合为:

$$\{c_{(u-1)\times(n-i+j)}\}.$$

(5) 前三个集合没有交叠, 即它们之间交集为空集; 三个集合的并为 $\{c_1, c_2, \cdots, c_n\}$.

(6) 由第一部分, 我们可以获得下面唯一的值:

$\bigcup_{k=1}^{u-1} \{c_{(k-1)\times(n-i+j)+n-i+1}, c_{(k-1)\times(n-i+j)+n-i+2}, \cdots, c_k \times (n-i+j)\} \cup \{c_{(u-1)\times(n-i+j)+n-i+1}, c_{(u-1)\times(n-i+j)+n-i+2}, \cdots, c_n\}$

(7) 由第二部分, 我们可以获得下面唯一的值:

$\bigcup_{k=1}^{u} \{c_{(k-1)\times(n-i+j)+1}, c_{(k-1)\times(n-i+j)+2}, \cdots, c_{(k-1)\times(n-i+j)+n-i-1}\}$.

(8) 由第三部分, 我们可以获得下面的两个值:

$\bigcup_{k=1}^{u} \{c_{(k-1)\times(n-i+j)+n-i}\}$,

$(c_{n-i}, c_{(n-i+j)+n-i}, c_{2\times(n-i+j)+n-i}, \cdots, c_{(u-1)\times(n-i+j)+n-i}) = (0, 0, \cdots, 0)$ or $(1, 1, \cdots, 1)$.

这意味着相应于第三部分, $\begin{bmatrix} \bar{a}_1 \\ \bar{a}_2 \\ \vdots \\ \bar{a}_n \end{bmatrix}$ 只存在一个线性

关系. 上面所有这些都证明矩阵

等式(2)~(4)中包含下面的方程:

$c_{k-(u-2)\times(n-i+j)}=0$ or 1,

$(c_{k-(u-2)\times(n-i+j)}+c_{k-(u-3)\times(n-i+j)}, c_{k-(u-3)\times(n-i+j)}+c_{k-(u-4)\times(n-i+j)}, \cdots, c_{k-(n-i+j)}+c_k)=(0,0,\cdots,0)$,

$c_k=0$.

$c_{l-(u-2)\times(n-i+j)}=0$ or 1,

$(c_{l-(u-2)\times(n-i+j)}+c_{l-(u-3)\times(n-i+j)}, c_{l-(u-3)\times(n-i+j)}+c_{l-(u-4)\times(n-i+j)}, \cdots, c_{l-(n-i+j)}+c_l)=(0,0,\cdots,0)$,

$c_l=0$.

注意到下面两个不同的线性关系:

$c_{k-(u-2)\times(n-i+j)}+(c_{k-(u-2)\times(n-i+j)}+c_{k-(u-3)\times(n-i+j)})+(c_{k-(u-3)\times(n-i+j)}+c_{k-(u-4)\times(n-i+j)})+\cdots+(c_{k-(n-i+j)}+c_k)+c_k=0$,

$c_{l-(u-2)\times(n-i+j)}+(c_{l-(u-2)\times(n-i+j)}+c_{l-(u-3)\times(n-i+j)})+(c_{l-(u-3)\times(n-i+j)}+c_{l-(u-4)\times(n-i+j)})+\cdots+(c_{l-(n-i+j)}+c_l)+c_l=0$.

因此矩阵 $\begin{bmatrix}\bar{a}_1\\ \bar{a}_2\\ \vdots\\ \bar{a}_n\end{bmatrix}$ 的秩不超过 $n-2$. 证毕.

引理 **7**　m-序列 a 中不包含长为 $2n$ 的比特串 $(a_1a_2\cdots a_{2n})$ 使得串 $(a_1a_2\cdots a_n)$ 和 $(a_{n+1}a_{n+2}\cdots a_{2n})$ 的 Hamming 重量都为 1 且 $a_i=1$, $a_{n+j}=1$, 这里 $1\leqslant i<n$, $1<j\leqslant n$, $(i-j)\geqslant n/2$.

证明: 用反证法证明, 假定存在满足上述条件的 $2n$ 长的比特串 $(a_1a_2\cdots a_{2n})$, 如果 $n-i+j$ 是 n 的一个因子, 由引理 4:

$$f(x)=1+x^{(n-i+j)}+x^{2(n-i+j)}+\cdots+x^n$$

等于互反多项式, 因此 a 不是 m 序列, 矛盾. 如果 $n-i+j$ 不是 n 的一个因子, 由引理 5 和引理 6, 矩阵 $\begin{bmatrix}\bar{a}_1\\ \bar{a}_2\\ \vdots\\ \bar{a}_n\end{bmatrix}$ 的秩小于 n, 即矩阵是不可逆的, 矛盾. 证毕.

命题 2 的证明: 由引理 1, 引理 2, 引理 3 和引理 7 可知命题 2 是正确的. 证毕.

4　定理 1 和推论的证明

由 m 序列的性质, 下面的引理 8 是平凡的.

引理 **8**　取序列 $v=v_0v_1v_2\cdots$ 为 m 序列 a 的移位序列且 $v\neq a$. 取序列 $h=h_0h_1h_2\cdots$ 为序列 a 和序列 v 的乘积序列, $h_k=a_kv_k$, $k=0,1,2,\cdots$, 则序列 h 的线性复杂度不超过 n^2. 因此序列 h 中的串"$00\cdots0$"的长度不超过 n^2-1. 如果 n 为偶数, 则序列 h 的线性复杂度不超过 $n^2/2$. 因此序列 h 中的串"$00\cdots0$"的长度不超过 $n^2/2-1$.

定理 1 和推论的证明: 设广义自缩序列 $b(\boldsymbol{G})=b_0b_1b_2\cdots$, 序列 $h=h_0h_1h_2\cdots$ 满足 $h_k=a_kv_k$, $k=0,1,2,\cdots$, 则 $b_0b_1b_2\cdots b_{L-1}=00\cdots0$ 当且仅当

$$v_{t_0}=v_{t_1}=v_{t_2}=\cdots=v_{t_{L-1}}=0;$$

当且仅当

$$h_t=0, \text{这里 } t_0\leqslant t\leqslant t_{L-1};$$

当且仅当

$$h_t=0, \text{这里 } 0\leqslant t\leqslant t_{L-1}.$$

现在假设 T 长串 $h_0h_1h_2\cdots h_{T-1}=00\cdots0$. 定义 $e=e_0e_1e_2\cdots$, 满足 $e_k=a_k+v_k$. 则 a, e 和 v 都是不同的 m 序列, 且有相同的极小多项式. 设 $T=2n\times S+W$, $0\leqslant W<2n$. 由命题 1 和命题 2, 我们知道:

(1) $e_0e_1e_2\cdots e_{2n\times S-1}$ 的 Hamming 重量不多于 $(2n-2)\times S$;

(2) $v_0v_1v_2\cdots v_{2n\times S-1}$ 的 Hamming 重量不少于 $3S$.

因此序列 $a_0a_1a_2\cdots a_{2n\times S-1}$ 的 Hamming 重量不多于 $(2n-2)\times S-3S=(2n-5)\times S$.

假设 $n<W<2n$, 由 m 序列的性质, $e_{2n\times S}e_{2n\times S+1}\cdots e_{2n\times S+W-1}$ 的 Hamming 重量不超过 $W-1$, $v_{2n\times S}v_{2n\times S+1}\cdots v_{2n\times S+W-1}$ 的 Hamming 重量不少于 1. 因此 $a_{2n\times S}a_{2n\times S+1}\cdots a_{2n\times S+W-1}$ 的 Hamming 重量不超过 $W-2$. 因此 $a_0a_1a_2\cdots a_{T-1}$ 的 Hamming 重量不超过 $(2n-5)\times S+(W-2)$.

但

$$\begin{aligned}&(2n-5)\times S+(W-2)\\&=(2n-5)\times S+(W-5)+3\\&=((2n-5)/(2n))\times 2nS+((W-5)/(2n))\times 2n+3\\&<((2n-5)/(2n))\times 2nS+((2n-5)/(2n))\times W+3\\&=((2n-5)/(2n))\times T+3.\end{aligned}$$

因此 $a_0a_1a_2\cdots a_{T-1}$ 的 Hamming 重量不超过 $((2n-5)/(2n))\times T+3$.

假设 $0\leqslant W\leqslant n$, 则 $a_{2n\times S}a_{2n\times S+1}\cdots a_{2n\times S+W-1}$ 的 Hamming 重量不超过 W, $a_0a_1a_2\cdots a_{T-1}$ 的 Hamming 重量不超过 $(2n-5)\times S+W$.

但

$$\begin{aligned}&(2n-5)\times S+W\\&=((2n-5)/(2n))\times 2nS+((2n-5)/(2n))\times W+(5/(2n))\times W\\&<((2n-5)/(2n))\times 2nS+((2n-5)/(2n))\times W+3\\&=((2n-5)/(2n))\times T+3.\end{aligned}$$

$a_0a_1a_2\cdots a_{T-1}$ 的 Hamming 重量不超过 $((2n-5)/(2n))\times T+3$.

可以看出串 $a_0a_1a_2\cdots a_{T-1}$ 的 Hamming 重量不超过 $((2n-5)/(2n))\times T+3$, 由引理 8, $T\leqslant n^2-1$, 且 $T\leqslant$

$n^2/2-1$ 如果 n 是偶数. 所以串 $a_0a_1a_2\cdots a_{T-1}$ 的 Hamming 重量不超过

$((2n-5)/(2n))\times(n^2-1)+3<((2n-5)/(2n))\times n^2+3=n^2-2.5n+3$,

如果 n 是偶数, 串 $a_0a_1a_2\cdots a_{T-1}$ 的 Hamming 重量不超过

$((2n-5)/(2n))\times(n^2/2-1)+3<((2n-5)/(2n))\times n^2/2+3=n^2/2-1.25n+3$.

因此当串 $b_0b_1b_2\cdots b_{L-1}=00\cdots0$, 其长度满足 $L\leqslant n^2-2.5n+3$, n 为偶数时 $L\leqslant n^2/2-1.25n+3$.

假设 $b_0b_1b_2\cdots b_{L-1}=11\cdots1$, 即 $b(\boldsymbol{G})$ 的补序列有一个长度为 L 的 0 串, 注意到 $b(\boldsymbol{G})$ 的补序列仍然属于族 $B(a)$. 因此, 族 $B(a)$ 中序列的最长游程长度 L 满足 $L\leqslant n^2-2.5n+3$, n 为偶数时 $L\leqslant n^2/2-1.25n+3$. 证毕.

5 已知结果和猜想

到现在为止, 我们没有发现任何一个广义自缩序列的 0 游程(1 游程)长度超过 $2n$. 对于 $n\in\{3,4,5,6\}$, 程序实现的结果表明, 族 $B(a)$ 中所有序列的最长游程都小于 $n+4$. 我们有一个猜想: 除序列 000…和 111…外, 族 $B(a)$ 中所有序列的最长游程都小于 $2n$.

参考文献:

[1] D Coppersmith, H Krawczyk, Y Mansour. The shrinking generator[A]. Advances in Cryptology-CRYPTO'93[C]. Berlin: Springer-Verlag, 1993. 23-39.

[2] W Meier, O Stafflebach. The self-shrinking generator[A]. in Advances in Cryptology-EUROCRYPT'94 [C]. Berlin: Springer-Verlag, 1995. 205-214.

[3] S R Blackburn. The linear complexity of the self-shrinking generator[J]. IEEE Transactions on Information Theory, 1999, 45(6): 2073-2077.

[4] M J Mihaljevic. A faster cryptanalysis of the Self-Shrinking Generator[A]. in Proceedings of ACIPS'96[C]. Berlin: Springer-Verlag, 1996. 182-189.

[5] E Zenner, M Krause, S Lucks. Improved cryptanalysis of self-shrinking generator[A]. in Proceedings of ACIPS'2001[C]. Berlin: Springer-Verlag, 2002. 21-35.

[6] M Krause. BDD-based cryptanalysis of keysteam generators [A]. in Advances in Cryptology-EUROCRYPT'02[C]. Berlin: Springer-Verlag, 2002. 22-237.

[7] A Kanso. Clock-Controlled Generators[D]. in Thesis to the University of London for the degree of Doctor of Philosophy, Royal Holloway and Bedford New College, University of London, 1999.

[8] Yupu Hu, Guozhen Xiao. Generalized self-shrinking generator [J]. IEEE Transactions on Information Theory, 2004, 50(4): 714-719.

[9] Yupu Hu, Guozhen Xiao. Pseudo-randomness of the fourth class of GSS sequences[J]. Science in China, F Edition, 2004, 47(2): 170-183.

作者简介:

孙红波 男, 1965 年生于黑龙江省, 1989 年毕业于西安电子科技大学, 获理学硕士学位, 现为北京电子科技学院副教授. 研究方向为密码学、信息安全. E-mail: w.sun@besti.edu.cn

胡予濮 男, 1955 年生于河南濮阳, 西安电子科技大学教授, 博士生导师, 信息保密研究所所长, 中国电子学会会士. 主要研究方向为密码学和信息安全. E-mail: yphu@mail.xidian.edu.cn

高军涛 男, 1979 年生于河北临城, 西安电子科技大学讲师, 主要研究方向为序列密码, 信息安全. E-mail: gjt_albert@163.com