第14卷 第5期 电子科学学刊 Vol. 14, No. 5
1992 年 9 月 JOURNAL OF ELECTRONICS Sept., 1992

几种流密码研究的母函数方法

武 传 坤
(西安电子科技大学,西安 710071)

摘要 本文利用母函数的方法对几种经常用到的特殊的流密码——周期序列的补序列，周期序列的部分和序列,逆向序列和有限生成序列进行了研究,给出了它们的极小多项式，周期和母函数. 对有限生成序列讨论了线性复杂度变化情况和联结多项式次数不变的情况下两个生成序列之间的关系.

关键词 流密码;母函数;补序列;部分和序列;逆向序列;有限生成序列; B-M 算法

一、引 言

序列的母函数（无穷幂级数）在许多研究领域都作为有力的数学方法起到了重要作用. 在流密码的研究中，它同样是一种方便灵活而且非常有效的数学工具. 利用母函数方法不仅可以把已有的结果表达得更简单明了，而且可得出许多新的结论. 例如在流密码中，一个序列的补序列是经常被用到的，但它的性质并不能由原来序列明显地反映出来. 又如一个序列的部分和序列,对实数的情况我们已经很熟悉它们之间的关系,但对于伪随机序列,它们之间除了还有同样的转换关系外,又增添了许多新的内容. 作为流密码的安全性度量指标,这也是一个重要的方面. 本文对以上这些问题都给出了解答,而且由于使用了母函数方法,这些问题很容易得到解决. 另外,我们还用这种母函数方法研究了逆向序列和有限生成序列.

应该指出的是,母函数方法尽管有如此重要的作用,但在众多有关流密码和伪随机序列的论著中,对这种方法使用不多. 文献 [1—3] 对该方法作了简单介绍，文献 [4] 又对它的应用作了扩展. 有些论著 [5—7] 尚未提到这种方法.

二、几个有关的命题

对于一个二元序列 $A=(a_0, a_1, \cdots)$，无论它是有穷还是无穷序列,都可以定义一个母函数

1991.05.08 收到, 1991.11.25 定稿.

$$A(x)=\sum_{n=0}^{\infty}a_nx^n \tag{1}$$

当序列 A 为有限序列 $(a_0, a_1, \cdots, a_N)$ 时，只要在 (1) 式中令 $a_i=0$，$i=N+1, N+2, \cdots$ 即可。本文只研究二元域(记为 GF(2)) 上周期序列的母函数。

命题 1　若序列 $A=(a_t)$ 的周期为 p，则其母函数为

$$A(x)=(a_0+a_1x+\cdots+a_{p-1}x^{p-1})(1+x^p+x^{2p}+\cdots) \tag{2}$$

记 $A_p(x)=a_0+a_1x+\cdots+a_{p-1}x^{p-1}$ 为序列 A 的第一个周期段的母函数。类似于实数幂级数，可将和式 $1+x^p+x^{2p}+\cdots$ 写为 $1/(1-x^p)$。由于二元域上加法与减法是一样的，故 (2) 式可写为

$$A(x)=A_p(x)/(1+x^p) \tag{3}$$

记 $Q(f)$ 为以 $f(x)$ 为联结多项式的线性移位寄存器产生的所有周期序列的集合，则有

命题 2　设 $f(x)=1+c_1x+\cdots+c_nx^n$ 是 GF(2) 上 n 次多项式，序列 $A=(a_t)$ 的母函数为 $A(x)=\sum_{i=0}^{\infty}a_ix^i$，则 $(a_t)\in Q(f)$ 的充分必要条件是 $A(x)$ 可表示为

$$A(x)=\varphi(x)/f(x) \tag{4}$$

其中

$$\varphi(x)=A_p(x)f(x)/(1+x^p) \tag{5}$$

是次数小于 n 的多项式。

命题 3　$f(x)$ 是序列 $A=(a_t)$ 的极小多项式，当且仅当在 (4) 式中 $\varphi(x)$ 与 $f(x)$ 互素。

命题 4　$Q(f)=\{A: A(x)=k(x)/f(x),\ \deg k(x)<\deg f(x)\}$。

三、周期序列的补序列

设 A 是周期为 p 的序列，其补序列 $\bar{A}=A+\mathbf{1}$ 也是周期为 p 的序列，其中 $\mathbf{1}$ 表示全 1 序列，$A+\mathbf{1}$ 表示序列对应比特相加。

记 $A(x)=A^*(x)/f(x)=A_p(x)/(1+x^p)$，则

$$A_p(x)=A^*(x)d(x) \tag{6}$$

其中 $d(x)=(1+x^p)/f(x)$。$A_p(x)$ 的系数序列就是序列 A 的第 1 个周期。由 $A=\bar{A}+\mathbf{1}$ 又得到

$$A_p(x)+\bar{A}_p(x)=1+x+x^2+\cdots+x^{p-1}=(1+x^p)/(1+x) \tag{7}$$

于是序列 $\bar{A}$ 的母函数为

$$\bar{A}(x)=\frac{\bar{A}_p(x)}{1+x^p}=\frac{(1+x^p)/(1+x)+A_p(x)}{1+x^p}=\frac{(1+x^p)+(1+x)A_p(x)}{(1+x)(1+x^p)}$$

$$=\frac{f(x)+A^*(x)(1+x)}{(1+x)f(x)} \tag{8}$$

再根据命题 2 就得到

定理 1 设序列 A 的特征多项式为 $f(x)$，则 A 的补序列 $\bar{A}$ 的特征多项式为 $(1+x)f(x)$.

一个序列的特征多项式是不唯一的. 要想较精确地研究序列的性质，应讨论它的极小多项式. 记 $f'(x)$ 为多项式 $f(x)$ 的形式导数，则有下述定理

定理 2 设序列 A 的极小多项式为 $f(x)$，则 (1) 当且仅当 $f(1)=1$ 时，$\bar{A}$ 的极小多项式为 $(1+x)f(x)$; (2) 当且仅当 $f(1)=0$, $f'(1)=0$ 时，$\bar{A}$ 的极小多项式为 $f(x)$; (3) 当且仅当 $f(1)=0$, $f'(1)=1$ 时，$\bar{A}$ 的极小多项式为 $f(x)/(1+x)$.

证明 记 $e(x)=\gcd(f(x)+A^*(x)(1+x), (1+x)f(x))$. 由命题 3 知

$$\bar{A} \text{ 的极小多项式} = (1+x)f(x)/e(x) \tag{9}$$

(1) 若 $f(1)=1$，因 $\gcd(A^*(x), f(x))=1$，故 $e(x)=1$. 反之，若 $e(x)=1$，则必有 $f(1)=1$. 因此由 (9) 式知，当且仅当 $f(1)=1$ 时，$\bar{A}$ 的极小多项式为 $(1+x)f(x)$.

(2) 若 $f(1)=0$, $f'(1)=0$，则 $f(x)$ 与 $f(x)/(1+x)$ 都含因式 $1+x$. 而由 $\gcd(A^*(x), f(x))=1$ 知 $A^*(x)$ 不含因式 $1+x$，故 $e(x)/(1+x)$ 不再含因式 $1+x$，易知它也不含其它非常数因式，因此 $e(x)=1+x$. 再由 (9) 式就知道 $\bar{A}$ 的极小多项式为 $f(x)$.

(3) 若 $f(1)=0$, $f'(1)\neq 0$，则 $f(x)/(1+x)$ 不再含因式 $1+x$. 但由于 $f(1)=0$，故 $f(x)$ 含因式 $1+x$，从而 $A^*(x)$ 不含因式 $1+x$，因此 $f(x)/(1+x)+A^*(x)$ 含有因式 $1+x$. 于是可写为 $e(x)=(1+x)^2\gcd\left(\dfrac{f(x)/(1+x)+A^*(x)}{1+x}, \dfrac{f(x)}{1+x}\right)$ 容易证明 $e(x)/(1+x)^2$ 不再含有非常数因式，即有 $e(x)=(1+x)^2$. 由 (9) 式知 $\bar{A}$ 的极小多项式为 $f(x)/(1+x)$.

由于上述条件 (1), (2), (3) 互不相容，故都是充分必要条件. *Q.E.D.*

定理 2 精确地刻划出一个序列的极小多项式与其补序列的极小多项式之间的关系. 由定理 2 还可得到几个推论.

推论 1 n 级 m 序列的补序列的线性复杂度为 $n+1$.

推论 2 周期为 2^n 的非平凡序列与其补序列有相同的极小多项式.

四、周期序列的部分和序列

设 $A=(a_0, a_1, \cdots, a_{p-1}, \cdots)$ 是周期为 p 的序列. 记

$$A_k=\sum_{i=0}^{k} a_i \tag{10}$$

则称序列 $\tilde{A}=(A_0, A_1, \cdots)$ 为序列 A 的部分和序列. 由 (10) 式可得

$$a_i=A_{i-1}+A_i, \quad i=0, 1, \cdots \tag{11}$$

其中 $A_{-1}=0$. 于是得到

$$A(x)=\sum_{i=0}^{\infty} a_i x^i=\sum_{i=0}^{\infty}(A_{i-1}+A_i)x^i=(1+x)\sum_{i=0}^{\infty} A_i x^i$$

注意到 $\sum_{i=0}^{\infty} A_i x^i = \tilde{A}(x)$ 是序列 $\tilde{A}$ 的母函数，故得到

$$A(x) = (1+x)\tilde{A}(x) \tag{12}$$

因序列 A 的周期为 p，故其母函数可写为 $A(x) = A_p(x)/(1+x^p)$，于是又得到

$$\tilde{A}(x) = A_p(x)/[(1+x)(1+x^p)] \tag{13}$$

若 $(1+x)|A_p(x)$，即序列 A 的一个周期中有偶数个 1，则由 (11) 式和 (13) 式可知序列 $\tilde{A}$ 的周期为 p。若 $(1+x)\nmid A_p(x)$，因 $(1+x)(1+x^p)|(1+x^{2p})$，这说明序列 $\tilde{A}$ 的周期为 $2p$ 或 $2p$ 的因子。但由 $(1+x)\nmid A_p(x)$ 和 (13) 式知，序列 $\tilde{A}$ 的周期不可能为 p，也不可能小于 p，故 $\tilde{A}$ 的周期为 $2p$。综上即得

定理 3　设 $A=(a_0, a_1, \cdots, a_{p-1}, \cdots)$ 是周期为 p 的序列。若序列 A 的一个周期中含有偶数个 1，则其部分和序列 $\tilde{A}=(A_0, A_1, \cdots)$ 是周期为 p 的序列；若序列 A 的一个周期中含有奇数个 1，则 $\tilde{A}$ 的周期为 $2p$。

推论 3　m 序列和 M 序列与其部分和序列有相同的周期。

设 $f(x)$ 是序列 A 的极小多项式，(13) 式可写为

$$\tilde{A}(x) = \varphi(x)/[(1+x)f(x)] \tag{14}$$

其中 $\varphi(x)$ 如 (5) 式所示。因此 $\tilde{A}$ 的极小多项式为

$$F(x) = (1+x)f(x)/\gcd(1+x, \varphi(x)) \tag{15}$$

下面对 $f(x)$ 为既约多项式的情况进行讨论。

设 $f(x)$ 既约，对所有次数小于 $n=\deg f(x)$ 的多项式 $k(x)$，以 $k(x)/f(x)$ 为母函数的序列都以 $f(x)$ 为极小多项式。我们把多项式 $k(x)$ 分为含有因式 $1+x$ 与不含因式 $1+x$ 两类。容易证明含有因式 $1+x$ 的非零多项式有 $2^{n-1}-1$ 个，而不含因式 $1+x$ 的非零多项式有 2^{n-1} 个。根据命题 3，命题 4 和 (15) 式可知，当 $\varphi(x)$ 含有因式 $1+x$ 时有 $F(x)=f(x)$，$\varphi(x)$ 不含因式 $1+x$ 时有 $F(x)=(1+x)f(x)$。于是得到

定理 4　设序列 $A=(a_0, a_1, \cdots)$ 的极小多项式 $f(x)$ 是 n 次既约的，则在 $\Omega(f)$ 中有 $2^{n-1}-1$ 个非零序列的部分和序列以 $f(x)$ 为极小多项式，其余 2^{n-1} 个非零序列的部分和序列以 $(1+x)f(x)$ 为极小多项式。

由定理 4 和推论 3 可以看到，m 序列尽管与其部分和序列有相同的周期，却不一定有相同的极小多项式。我们把 m 序列分为两类：一类是与其部分和序列移位等价的，记为 M_1；其余的算作另一类，记为 M_2。可以证明，任取 M_2 中两个不同的序列，它们的和序列属于 M_1；任取 M_1 中两个不同的序列，它们的和序列仍属于 M_1；而 M_1 中任一序列与 M_2 中任一序列的和序列属于 M_2。按照这种关系，在线性空间 $\Omega(f)$ 中构造一个线性子空间 $M_0=M_1\cup\{0\}$。这样，M_2 中的序列可由其中一个序列与 M_0 中序列之和得到。我们选这一序列为以 $1/f(x)$ 为母函数的序列，它是第一个周期末尾有连续 $n-1$ 个 0 的 m 序列。

对于 M_0 中序列，同样可再作它们的部分和序列。以同样方法可以证明这些序列中又有一半序列与其部分和序列移位等价。这个过程可以继续下去。为了精确刻划一个序列与其部分和序列这种移位等价关系，我们给出 k 阶部分和移位等价序列的概念：若一

个序列与其部分和序列移位等价，部分和序列又与自己的部分和序列移位等价，这种关系持续 k 次，而到第 $k+1$ 次不再具有这种等价关系，则把这种序列称为 k 阶部分和移位等价序列。与部分和序列不移位等价的称作 0 阶部分和移位等价序列。在这些序列中每阶选一代表元，这样共有 n 个代表元。它们通过线性组合能产生 $\Omega(f)$ 中的所有序列，即 $\Omega(f)$ 的一组基。由这组基的线性组合表示的序列中可以看出该序列的部分和移位等价的阶数。

如何产生这组基呢？首先取以 $1/f(x)$ 为母函数的 0 阶部分和移位等价序列 a_0，将此序列右移一位与自己相加得 a_1，再将 a_1 右移一位并与 a_1 相加得 a_2，如此下去便得到所要求的基，其中 a_i 是 i 阶部分和移位等价序列。

例 1 取 $n=4$，$f(x)=1+x+x^4$，$p(f)=2^4-1=15$，

$$(1+x^{15})/(1+x+x^4)=1+x+x^2+x^3+x^5+x^7+x^8+x^{11}$$

令 $a_0=111101011001000$，作下列移位加法

0 阶
$$\begin{array}{l} 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0 \longleftarrow a_0 \\ +0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0 \longleftarrow a_0 \text{ 右移一位} \end{array}$$

1 阶
$$\begin{array}{l} 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0 \longleftarrow a_1 \\ +0\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0 \longleftarrow a_1 \text{ 右移一位} \end{array}$$

2 阶
$$\begin{array}{l} 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0 \longleftarrow a_2 \\ +0\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1 \longleftarrow a_2 \text{ 右移一位} \end{array}$$

3 阶 $\quad 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1 \longleftarrow a_3$

取 a_0，a_1，a_2，a_3 为 $\Omega(f)$ 的一组基，若有某序列 $A\in\Omega(f)$，使 $A=c_0a_0+c_1a_1+c_2a_2+c_3a_3$，如果 $c_0=1$，则由上面的分析知，A 是 0 阶部分和移位等价序列；否则，考虑 c_1。若 $c_1=1$，则 A 是 1 阶部分和移位等价序列。依此类推，可以判断出 A 的部分和移位等价阶数为 $k=\min\{i:c_i=1\}$。

五、逆向序列

有许多流密码体制的破译问题[8]在恢复一个线性移位寄存器初态时知道从第 $k(k>1)$ 位之后的若干位，根据反馈多项式可产生一个周期，将周期段上后面几位补过来当然就得到初态。但当周期较大时这种做法是不可行的。如果把序列倒过来，初始的几位则是已知若干位后面紧接着的几位。因此，逆向序列的研究可将这类问题大大简化，这在实际中亦经常用到。

设序列 $A=(a_0, a_1, \cdots)$ 周期为 p，极小多项式为 $f(x)$，它的逆向序列 $\overleftarrow{A}=(a_{p-1}, a_{p-2}, \cdots, a_0, \cdots)$，于是

$$A(x)=A^*(x)/f(x)=(a_0+a_1x+\cdots+a_{p-1}x^{p-1})/(1+x^p)$$

$$\overleftarrow{A}(x)=(a_{p-1}+a_{p-2}x+\cdots+a_0x^{p-1})/(1+x^p)=x^{n-1-\deg A^*(x)}\overleftarrow{A}^*(x)/\overleftarrow{f}(x)$$

其中 $\overleftarrow{A}^*(x)$ 与 $\overleftarrow{f}(x)$ 分别表示多项式 $A^*(x)$ 与 $f(x)$ 的互反多项式。因 $\gcd(A^*(x), f(x))=1$，故 $\gcd(\overleftarrow{A}^*(x), \overleftarrow{f}(x))=1$，又 $\gcd(\overleftarrow{f}(x), x)=1$，故得到

注意到 $\sum_{i=0}^{\infty} A_i x^i = \tilde{A}(x)$ 是序列 $\tilde{A}$ 的母函数，故得到

$$A(x) = (1+x)\tilde{A}(x) \tag{12}$$

因序列 A 的周期为 p，故其母函数可写为 $A(x) = A_p(x)/(1+x^p)$，于是又得到

$$\tilde{A}(x) = A_p(x)/[(1+x)(1+x^p)] \tag{13}$$

若 $(1+x)|A_p(x)$，即序列 A 的一个周期中有偶数个 1，则由 (11) 式和 (13) 式可知序列 $\tilde{A}$ 的周期为 p。若 $(1+x)\nmid A_p(x)$，因 $(1+x)(1+x^p)|(1+x^{2p})$，这说明序列 $\tilde{A}$ 的周期为 $2p$ 或 $2p$ 的因子。但由 $(1+x)\nmid A_p(x)$ 和 (13) 式知，序列 $\tilde{A}$ 的周期不可能为 p，也不可能小于 p，故 $\tilde{A}$ 的周期为 $2p$。综上即得

定理 3　设 $A=(a_0, a_1, \cdots, a_{p-1}, \cdots)$ 是周期为 p 的序列。若序列 A 的一个周期中含有偶数个 1，则其部分和序列 $\tilde{A}=(A_0, A_1, \cdots)$ 是周期为 p 的序列；若序列 A 的一个周期中含有奇数个 1，则 $\tilde{A}$ 的周期为 $2p$。

推论 3　m 序列和 M 序列与其部分和序列有相同的周期。

设 $f(x)$ 是序列 A 的极小多项式，(13) 式可写为

$$\tilde{A}(x) = \varphi(x)/[(1+x)f(x)] \tag{14}$$

其中 $\varphi(x)$ 如 (5) 式所示。因此 $\tilde{A}$ 的极小多项式为

$$F(x) = (1+x)f(x)/\gcd(1+x, \varphi(x)) \tag{15}$$

下面对 $f(x)$ 为既约多项式的情况进行讨论。

设 $f(x)$ 既约，对所有次数小于 $n=\deg f(x)$ 的多项式 $k(x)$，以 $k(x)/f(x)$ 为母函数的序列都以 $f(x)$ 为极小多项式。我们把多项式 $k(x)$ 分为含有因式 $1+x$ 与不含因式 $1+x$ 两类。容易证明含有因式 $1+x$ 的非零多项式有 $2^{n-1}-1$ 个，而不含因式 $1+x$ 的非零多项式有 2^{n-1} 个。根据命题 3，命题 4 和 (15) 式可知，当 $\varphi(x)$ 含有因式 $1+x$ 时有 $F(x)=f(x)$，$\varphi(x)$ 不含因式 $1+x$ 时有 $F(x)=(1+x)f(x)$。于是得到

定理 4　设序列 $A=(a_0, a_1, \cdots)$ 的极小多项式 $f(x)$ 是 n 次既约的，则在 $\Omega(f)$ 中有 $2^{n-1}-1$ 个非零序列的部分和序列以 $f(x)$ 为极小多项式，其余 2^{n-1} 个非零序列的部分和序列以 $(1+x)f(x)$ 为极小多项式。

由定理 4 和推论 3 可以看到，m 序列尽管与其部分和序列有相同的周期，却不一定有相同的极小多项式。我们把 m 序列分为两类：一类是与其部分和序列移位等价的，记为 M_1；其余的算作另一类，记为 M_2。可以证明，任取 M_2 中两个不同的序列，它们的和序列属于 M_1；任取 M_1 中两个不同的序列，它们的和序列仍属于 M_1；而 M_1 中任一序列与 M_2 中任一序列的和序列属于 M_2。按照这种关系，在线性空间 $\Omega(f)$ 中构造一个线性子空间 $M_0=M_1\cup\{0\}$。这样，M_2 中的序列可由其中一个序列与 M_0 中序列之和得到。我们选这一序列为以 $1/f(x)$ 为母函数的序列，它是第一个周期末尾有连续 $n-1$ 个 0 的 m 序列。

对于 M_0 中序列，同样可再作它们的部分和序列。以同样方法可以证明这些序列中又有一半序列与其部分和序列移位等价。这个过程可以继续下去。为了精确刻划一个序列与其部分和序列这种移位等价关系，我们给出 k 阶部分和移位等价序列的概念：若一

个序列与其部分和序列移位等价，部分和序列又与自己的部分和序列移位等价，这种关系持续 k 次，而到第 $k+1$ 次不再具有这种等价关系，则把这种序列称为 k 阶部分和移位等价序列．与部分和序列不移位等价的称作 0 阶部分和移位等价序列．在这些序列中每阶选一代表元，这样共有 n 个代表元．它们通过线性组合能产生 $\Omega(f)$ 中的所有序列，即 $\Omega(f)$ 的一组基．由这组基的线性组合表示的序列中可以看出该序列的部分和移位等价的阶数．

如何产生这组基呢？首先取以 $1/f(x)$ 为母函数的 0 阶部分和移位等价序列 a_0，将此序列右移一位与自己相加得 a_1，再将 a_1 右移一位并与 a_1 相加得 a_2，如此下去便得到所要求的基，其中 a_i 是 i 阶部分和移位等价序列．

例 1 取 $n=4$，$f(x)=1+x+x^4$，$p(f)=2^4-1=15$，

$$(1+x^{15})/(1+x+x^4)=1+x+x^2+x^3+x^5+x^7+x^8+x^{11}$$

令 $a_0=111101011001000$，作下列移位加法

0 阶
$$\begin{array}{r} 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0 \longleftarrow a_0 \\ +\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0 \longleftarrow a_0 \text{ 右移一位} \end{array}$$

1 阶
$$\begin{array}{r} 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0 \longleftarrow a_1 \\ +\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0 \longleftarrow a_1 \text{ 右移一位} \end{array}$$

2 阶
$$\begin{array}{r} 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0 \longleftarrow a_2 \\ +\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1 \longleftarrow a_2 \text{ 右移一位} \end{array}$$

3 阶 $\quad 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1 \longleftarrow a_3$

取 a_0，a_1，a_2，a_3 为 $\Omega(f)$ 的一组基，若有某序列 $A\in\Omega(f)$，使 $A=c_0a_0+c_1a_1+c_2a_2+c_3a_3$，如果 $c_0=1$，则由上面的分析知，A 是 0 阶部分和移位等价序列；否则，考虑 c_1．若 $c_1=1$，则 A 是 1 阶部分和移位等价序列．依此类推，可以判断出 A 的部分和移位等价阶数为 $k=\min\{i:c_i=1\}$．

五、逆向序列

有许多流密码体制的破译问题[8]在恢复一个线性移位寄存器初态时知道从第 $k(k>1)$ 位之后的若干位，根据反馈多项式可产生一个周期，将周期段上后面几位补过来当然就得到初态．但当周期较大时这种做法是不可行的．如果把序列倒过来，初始的几位则是已知若干位后面紧接着的几位．因此，逆向序列的研究可将这类问题大大简化，这在实际中亦经常用到．

设序列 $A=(a_0, a_1, \cdots)$ 周期为 p，极小多项式为 $f(x)$，它的逆向序列 $\overleftarrow{A}=(a_{p-1}, a_{p-2}, \cdots, a_0, \cdots)$，于是

$$A(x)=A^*(x)/f(x)=(a_0+a_1x+\cdots+a_{p-1}x^{p-1})/(1+x^p)$$

$$\overleftarrow{A}(x)=(a_{p-1}+a_{p-2}x+\cdots+a_0x^{p-1})/(1+x^p)=x^{n-1-\deg A^*(x)}\overleftarrow{A}^*(x)/\overleftarrow{f}(x)$$

其中 $\overleftarrow{A}^*(x)$ 与 $\overleftarrow{f}(x)$ 分别表示多项式 $A^*(x)$ 与 $f(x)$ 的互反多项式．因 $\gcd(A^*(x), f(x))=1$，故 $\gcd(\overleftarrow{A}^*(x), \overleftarrow{f}(x))=1$，又 $\gcd(\overleftarrow{f}(x), x)=1$，故得到

定理 5　设序列 $A=(a_0, a_1, \cdots, a_{p-1}, \cdots)$的极小多项式为 $f(x)$，则其逆向序列 $\tilde{A}=(a_{p-1}, a_{p-2}, \cdots, a_0, \cdots)$ 的极小多项式为 $\tilde{f}(x)$.

六、有限序列的生成序列

采用文献 [7] 中符号，记 $\langle f_i, l_i\rangle$ 为能产生序列 $a_0, a_1, \cdots, a_{i-1}$ 的最短线性移位寄存器，其中 f_i 表示线性移位寄存器的联结多项式，l_i 是该线性移位寄存器的级数或序列的线性复杂度. 这样的线性移位寄存器可由 Berlekamp-Massey(B-M) 算法得到[9,10]. 它的唯一性可由下述引理描述.

引理 1[7]　产生序列 $a_0, a_1, \cdots, a_{k-1}$ 的最短线性移位寄存器 $\langle f_k, l_k\rangle$ 唯一的充要条件是 $l_k \leqslant k/2$.

定义序列 $a_0, a_1, \cdots, a_{k-1}$ 的生成序列为能产生序列 $a_0, a_1, \cdots, a_{k-1}$ 的最短线性移位寄存器产生的带枝或不带枝的周期序列.由引理 1 知当且仅当序列 $a_0, a_1, \cdots, a_{k-1}$ 的线性复杂度 $< k/2$ 时，它的生成序列是唯一的.

用符号 $L(b_1, b_2, \cdots, b_t)$ 记序列 $b_1, b_2, \cdots b_t$ 的线性复杂度. 下面先给出几个引理.

引理 2[7]　设 l_i 是序列 $a_0, a_1, \cdots, a_{i-1}$ 的线性复杂度，则

$$l_{i+1}=\max\{l_i, i+1-l_i\} \tag{16}$$

引理 3[7]　设周期序列 $a_0, a_1, \cdots$ 的线性复杂度为 n，则 $\langle f_{2n}, l_{2n}\rangle$ 就是产生该序列的最短线性移位寄存器.

引理 4　线性复杂度为 n 的周期序列的任意连续 $2n-1$ 位的线性复杂度为 n.

引理 5[3]　由 n 级线性移位寄存器产生的线性复杂度为 n 的周期序列的任意 n 个连续状态是线性无关的.

根据上述这些引理，我们得到下面两个定理. 它们反映了改变第 $2n$ 位后生成序列的变化.

定理 6　设序列 $a_0, a_1, \cdots, a_{2n-1}$ 是线性复杂度为 n 的周期序列中连续的 $2n$ 位. 将第 $2n$ 位的 a_{2n-1} 的值改变，则当

$$\Delta=\begin{vmatrix} a_1 & a_2 & \cdots & a_{n-1} \\ a_2 & a_3 & \cdots & a_n \\ \cdots & \cdots & \cdots & \\ a_{n-1} & a_n & \cdots & a_{2n-2} \end{vmatrix}=0$$

时，新序列 $a_0, a_1, \cdots, a_{2n-2}, \bar{a}_{2n-1}$ 的生成序列仍是线性复杂度为 n 的周期序列，而当 $\Delta \neq 0$时，序列 $a_0, a_1, \cdots, a_{2n-2}, \bar{a}_{2n-1}$ 的生成序列，除 a_0 外是线性复杂度为 $n-1$ 的周期序列.

定理 7　设序列 $A=(a_0, a_1, \cdots)$的线性复杂度为 n，极小多项式为 $f(x)$. 改变 a_{2n-1} 的值，使 $a_0, a_1, \cdots, a_{2n-2}, \bar{a}_{2n-1}$ 生成一个新序列 B. 当 $\Delta=0$ 时，序列 B 是线性复杂度为 n 的周期序列. 设其极小多项式为 $g(x)$，则 A 与 B 的和序列的母函数为 $(A+B)(x)=x^{2n-1}/[f(x)g(x)]$，从而 $(A+B)\in Q(fg)$.

七、结 束 语

利用母函数方法可使许多看似无从下手的问题很简单地得到解决，而且由于序列与母函数之间的一一对应关系，使得母函数刻划出的序列具有许多代数性质，如线性复杂度，周期和极小多项式等. 母函数方法还可用来研究其他问题. 但作为序列的统计特性，还需结合使用别的方法去研究.

作者感谢肖国镇教授、王新梅教授和王育民教授对本文的宝贵意见.

参 考 文 献

[1] H. J. Beker, F. C. Piper, Cipher System——The Protection of Communications, Northwood Books, London, (1982). 中译本：《密码体制——通信保护》，通信保密编辑部，1982年，第154—161页.
[2] R. Lidl, H. Niedereiter, Finite Fields, Addison-Wesley, (1983), Ch. 8.
[3] 王育民，何大可，保密学——基础与应用，西安电子科技大学出版社，西安，1990年，第86页.
[4] 武传坤，现代密码学基础，西安电子科技大学教材科，西安，1990年，第19—23页.
[5] R. A. Rueppel, Analysis and Design of Stream Ciphers, Springer-Verlag, (1986).
[6] T. Siegenthaler 著，陈立东译，流密码体制的设计方案，西北电讯工程学院情报资料室，西安，1988年.
[7] 肖国镇，梁传甲，王育民，伪随机序列及其应用，国防工业出版社，北京，1985年，第100—119页.
[8] 武传坤，通信学报，11(1990)6，46—49.
[9] E.R.Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York, (1968).
[10] J. L. Massey, *IEEE Trans. on IT*, IT-15(1969)1, 122—127.

STUDY ON SOME STREAM CIPHERS USING GENERATING FUNCTIONS

Wu Chuankun

(*Xidian University, Xi'an* 710071)

Abstract Several kinds of stream ciphers——complement sequences of period sequences, partial sum of period sequences, inverse order sequences and finitely generated sequences, are studied by using techniques of generating functions. Their minimal polynomials, periods, as well as generating functions are given. As to finitely generated sequences, the change of their linear complexity profiles as well as the relationship between the two generated sequences under the case in which the degree of connected polynomials are fixed, are discussed.

Key words Stream cipher; Generating function; Complement sequence; Partial sum sequence; Inverse order sequence; Finitely generated sequence; B-M algorithm