周期为 $N = n2^v$ 的序列线性复杂度的快速算法 [1]

蔡 勉 *** 王 宏 ** 肖国镇 **

*(西安电子科技大学综合业务网国家重点实验室 西安 710071)
**(中国科学院研究生院信息安全国家重点实验室 北京 100039)

摘 要 文中利用广义离散傅里叶变换对 GF(2) 上周期为 $N = n2^v$ ($\gcd(n,2)=1$) 序列进行了研究，给出了求周期为 $N = n2^v$ 的序列线性复杂度的快速算法，并得到了关于 GF(2) 上多项式的 Hasse 导数的一些新结果。

关键词 线性复杂度，广义离散傅里叶变换，Hasse 导数
中图号 TN918.1

1 引 言

序列线性复杂度是衡量密码序列强度的重要指标，迅速、准确地得到序列的线性复杂度尤为重要。目前对求 GF(p)(p 为素数) 上周期为 p^n 序列线性复杂度已经有了非常有效的算法如 Games-Chan 和 Imamura 快速算法 [1,2]，对于求更大周期序列的线性复杂度还没有其快速、有效的方法。文中利用了广义离散傅里叶变换 (GDFT) 求线性复杂度的方法 [3]，得到了 GF(2) 上周期为 $N = n2^v$ 序列线性复杂度的快速算法，使得求该周期线性复杂度的速度提高了一个指数级，即计算复杂度由指数级 $O(2^v)$ 减小到一次多项式级 $O(v)$，并给出了关于 $F[D]$(F=GF(2)) 上多项式的 Hasse 导数的一些新的结果。

2 $F(p)$ 上周期为 $N = np^v$ 序列线性复杂度

2.1 Hasse 导数、离散傅里叶变换和 Günther 重量的概念

设 $F[D]$ 表示未定元为 D 系数在域 F 上的多项式环，且

$$a(D) = \sum_i a_i D^i \in F[D] \tag{1}$$

$a(D)$ 的 j 次 Hasse 导数定义为

$$a^{[j]}(D) = \sum_i \begin{bmatrix} i \\ j \end{bmatrix} a_i d^{i-j} \tag{2}$$

定义 1 有限域 F 上的 Hasse 矩阵 $H_k(D)$ 为 $k \times k$ 矩阵，k 为正整数，矩阵的 i 行 j 列元素为 $\begin{bmatrix} j-1 \\ i-1 \end{bmatrix} D^{j-1}$，表示 D^{j-1} 的 $i-1$ 次 Hasse 导数。

设 $s^N = [s_0, s_1, \cdots, s_{N-1}]$ 是任意的 N 维矢量，表示序列 $\tilde{s} = s_0, s_1, \cdots, s_{N-1}, s_0, s_1 \cdots$ 的一个周期，序列中的每一位是有限域 GF(p^n) 上的元素，若假定 $\gcd(N,p) = 1$，并且

$$s^N(D) = s_0 + s_1 D + \cdots + s_{N-1} D^{N-1}, \qquad s^N(D) \in F[D] \tag{3}$$

[1] 2000-09-01 收到，2001-04-19 定稿
国家自然科学基金 (批准号：69673025)、信息安全国家重点实验室开放课题资助

对于多项式 $s^N(D)$ 存在 N 次单位本原根 α ，那么该周期序列的离散傅里叶变换 (DFT) 存在，表示为

$$S^N=[s^N(1),s^N(\alpha),\cdots,s^N(\alpha^{N-1})] \tag{4}$$

并且在假定 $\gcd(N,p)\neq 1$ 的情况下，对于 $N=np^v$ ， $\gcd(n,p)=1$ ，给出 GDFT ，即

$$S^{n\times p^v}\triangleq\begin{bmatrix} s^N(1) & s^N(\alpha) & \cdots & s^N(\alpha^{N-1}) \\ s^{N[1]}(1) & s^{N[1]}(\alpha) & \cdots & s^{N(1)}(\alpha^{N-1}) \\ \vdots & \vdots & \vdots & \vdots \\ s^{N[p^v-1]}(1) & s^{N[p^v-1]}(\alpha) & \cdots & s^{N[p^v-1]}(\alpha^{N-1}) \end{bmatrix} \tag{5}$$

$s^{N[i]}(D)$ 表示 $s^N(D)$ 的 i 次 Hasse 导数. 当 $v=0$ 时， GDFT 即 DFT .

定义 2　一个矩阵的 Günther 重量是指该矩阵非零阵元及在非零阵元下方阵元数的总和. 例如，矩阵

$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1+\alpha & \alpha \\ 0 & 0 & 0 \end{bmatrix}$ 的 Günther 重量为 4+2+2=8.

2.2 广义离散傅里叶变换的表示

GDFT 可以由 DFT 表示. 因为

$$s^N(D)=s^n_{(0)}(D^{p^v})+Ds^n_{(1)}(D^{p^v})+\cdots+D^{(p^v-1)}s^n_{(p^v-1)}(D^{p^v}) \tag{6}$$

和

$$s^n_{(k)}(D)=s_k+s_{k+p^v}D+\cdots+s_{k+(n-1)p^v}D^{n-1} \tag{7}$$

$s^n_{(k)}(1)=[s_k+s_{k+p^v}+\cdots+s_{k+(n-1)p^v}]$ ， $\gcd(n,p)=1$. 对 (6) 式求 Hasse 导数得到

$$\begin{bmatrix} s^N(D) \\ s^{N[1]}(D) \\ \vdots \\ s^{N[p^v-1]}(D) \end{bmatrix}=H_{p^v}(D)\begin{bmatrix} s^N_{(0)}(D^{p^v}) \\ s^N_{(1)}(D^{p^v}) \\ \vdots \\ s^N_{(p^v-1)}(D^{p^v}) \end{bmatrix} \tag{8}$$

α 和 β 是 GF(2^n) 上的单位原根，选择 $\beta=\alpha^{p^v}$ ，把 α^i ， $i=0,1,\cdots,n-1$ 代入 (8) 式得到

$$\begin{bmatrix} s^N(\alpha^i) \\ s^{N[1]}(\alpha^i) \\ \vdots \\ s^{N[p^v-1]}(\alpha^i) \end{bmatrix}=H_{p^v}(\alpha^i)\begin{bmatrix} s^n_{(0)}(\beta^i) \\ s^n_{(1)}(\beta^i) \\ \vdots \\ s^n_{(p^v-1)}(D^{\beta^i}) \end{bmatrix} \tag{9}$$

在 GF(2) 上 Hasse 矩阵 $H_{2^v}(D)$ 可以表示为

$$H_{2^v}(D)=\begin{bmatrix} 1 & D & \cdots & D^{2^v-1} \\ 0 & 1 & \cdots & D^{2^v-2} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}=\begin{bmatrix} H_{2^{v-1}} & D^{2^{v-1}}H_{2^{v-1}}(D) \\ 0 & H_{2^{v-1}}(D) \end{bmatrix} \tag{10}$$

2.3 GF(p)(p 为素数) 上的周期为 $N=np^v(\gcd(n,p)=1)$ 序列线性复杂度

在文献 [3] 中给出了如下的定理及其推论。

定理 1 如果 $a(D)$ 和 $h(D)$ 是 $F[D]$ 上的多项式，$h(D)$ 在 $F[D]$ 上是既约的，并且 $h^{(1)}(D)\neq 0$ ($h^{(1)}(D)$ 是 $h(D)$ 的一次形式导数)，m 是任意正整数，$[h(D)]^m$ 整除 $a(D)$，当且仅当 $h(D)$ 整除 $a(D)$ 和其 $m-1$ 次 Hasse 导数。

推论 1 设 $\tilde{s}=s_0,s_1,\cdots,s_{N-1},s_0,s_1\cdots$ 是 GF(p)(p 为素数) 上的周期为 $N=np^v(\gcd(n,p)=1)$ 序列，如果 α 是 GF(p) 或其扩域上的 n 次单位原根，那么 $\tilde{s}$ 的线性复杂度 $L(\tilde{s})=m_0+m_1+\cdots+m_{n-1}$。

$$m_i=\begin{cases}0, & \text{如果} s^N(\alpha^i)=s^{N[1]}(\alpha^i)=\cdots=s^{N[p^v-1]}(\alpha^i)=0\\ p^v-\min\{j:s^{N[j]}(\alpha^i)\neq 0\}, & \text{其它}\end{cases} \tag{11}$$

定理 2 GF(p) 上周期为 $N=np^v(\gcd(n,p)=1)$ 的序列 $\tilde{s}$ 的线性复杂度恰为 $s^N=[s_0,s_1,\cdots,s_{N-1}]$ 的 GDFT 矩阵 $S^{n\times p^v}$ 的 Günther 重量。

根据定理 2 和推论 1，由 (9) 式得到 m_i。

3 周期 $N=n2^v$ 序列线性复杂度快速算法

根据上面研究结果，对 F 为 GF(2) 的情况进行了深入研究，得到了以下定理，并给出求 GF(2) 上周期为 $N=n2^v(\gcd(n,2)=1)$ 序列线性复杂度的快速算法。

定理 3 设 $\tilde{s}$ 是 GF(2) 上的周期为 $N=n2^v(\gcd(n,2)=1)$ 序列，如果是 GF(2) 或其扩域上的 n 次单位原根，那么 $\tilde{s}$ 的线性复杂度 $L(\tilde{s})=m_0+(n-1)m_i$，$i=1,2,\cdots,n-1$，$m_1=m_2=\cdots=m_{n-1}$。

设 $s^N=(s_0,s_1,\cdots,s_N)$ 是 $\tilde{s}$ 的一个周期的序列，其线性复杂度为 L_c，α^i 是 $F[D]$ 上多项式 $s^N(D)$ 的 i 次单位原根，$i=0,1,\cdots,n-1$。

GF(2) 上周期为 $N=n2^v$ 序列线性复杂度快速算法如下：

(1) 初始条件：$s^N=(s_0,s_1,\cdots,s_{N-1})$，$N=n\times 2^v$，$M=2^r$，$L_c=0$，$m_i=0$，$i=0,1$，$M\equiv t(\mathrm{mod}n)$。

(2) $S^{(M_0)}=(S^{(0)}_{(0)},S^{(0)}_{(1)},\cdots,S^{(0)}_{(M-1)})$，

$S^{(0)}_{(K)}=(s_k+s_{k+M}+\cdots+s_{k+(n-1)M})=(s_{k,0}+s_{k,1}+\cdots+s_{k,(n-1)})$，

$S^{(M_1)}=(S^{(1)}_{(0)},S^{(1)}_{(1)},\cdots,S^{(1)}_{(M-1)})$，

$S^{(1)}_{(K)}=(s_k,s_{k+M},\cdots,s_{k+(n-1)M})=(s_{k,0},s_{k,1},\cdots,s_{k,(n-1)})$，$k=0,1,\cdots,M-1$。

(3) $M/2\equiv s(\mathrm{mod}n)\cdot c=(dn-s)t$，($d$ 是使 c 为最小正整数的任意正整数)，

$L^{(0)}=(S^{(0)}_{(0)},S^{(0)}_{(1)},\cdots,S^{(0)}_{(M/2-1)})$，$R^{(0)}=(S^{(0)}_{(M/2)},S^{(0)}_{(M/2+1)},\cdots,S^{(0)}_{(M-1)})$，

$B^{(0)}=L^{(0)}+R^{(0)}=(b^0_0,b^0_1,\cdots,b^0_{M/2-1})$，

$L^{(1)}=(S^{(1)}_{(0)},S^{(1)}_{(1)},\cdots,S^{(1)}_{(M/2-1)})$，$R^{(1)}=(S^{(1)}_{(M/2)},S^{(1)}_{(M/2+1)},\cdots,S^{(1)}_{(M-1)})$，

$(S^{(1)}_{(M/2+k)})''=(s_{k+M/2,q_0},s_{k+M/2,q_1},\cdots,s_{k+M/2,q_{n-1}})$，

$(i+c)\equiv q_i(\mathrm{mod}n)$，$i=0,1,\cdots,n-1$. $k=0,1,\cdots,M/2-1$。

$(R^{(1)})''=(S^{(1)}_{(M/2)})'',(S^{(1)}_{(M/2+1)})'',\cdots,(S^{(1)}_{(M-1)})'')$，

$B^{(1)}=L^{(1)}+(R^{(1)})''=(b^{(1)}_0,b^{(1)}_1,\cdots,b^{(1)}_{M/2-1})$

(4) 如果 $B^{(0)}\neq\mathbf{0}$，那么 $S^{(M_0)}=B^{(0)}$，$m_0=m_0+M/2$. 否则 $S^{(M_0)}=R^{(0)}$。

如果 $b_{(j)}^{(1)}=\mathbf{0}$ 或 $b_{(j)}^{(1)}=\mathbf{1}$, $j=0,1,\cdots,M/2-1$，那么 $S^{(M_1)}=R^{(1)}$，

否则 $S^{(M_1)}=B^{(1)}$, $m_1=:m_1+M/2$。

(5) $M=:M/2$. 如果 $M\neq 1$, 则转到 (3)，否则

如果 $S^{(M_0)}\neq 0$，那么 $m_0=:m_0+1$。

如果 $S^{(M_1)}\neq\mathbf{0}$ 或 $S^{(M_0)}\neq\mathbf{1}$，那么 $m_1=:m_1+1$。

(6) $L_c=m_0+(n-1)m_1$。

例子

(1) 初始条件：$s^N=(0100110110111)$, $n=3$, $v=2$，$N=3\times 2^2$, $M=2^2=4$, $L_c=0$, $m_i=0$, $i=0,1$, $t=1$。

(2) (a) $S^{(M_0)}=((0+1+0)(1+0+1)(0+1+1)(0+1+1))=(1000)$,

$S^{(M_1)}=((010)(101)(011)(011))$。

(b) $s=2$, $c=1$. $L^{(0)}=(10)$, $R^{(0)}=(00)$, $B^{(0)}=(10)$。

$L^{(1)}=((010)(101))$, $R^{(1)}=((011)(011))$, $(R^{(1)})''=((101)(101))$, $B^{(1)}=((111)(000))$,

(c) $S^{(M_0)}=(10)$, $m_0=2$. $S^{(M_1)}=((011)(011))$, $m_1=0$。

(d) $M=2$。

(3) (a) $s=1$, $c=2$. $L^{(0)}=(1)$, $R^{(0)}=(0)$, $B^{(0)}=(1)$。

$L^{(1)}=(011)$, $R^{(1)}=(011)$, $(R^{(1)})''=(110)$, $B^{(1)}=(101)$。

(b) $S^{(M_0)}=(1)$, $m_0=3$. $S^{(M_1)}=(101)$, $m_1=1$。

(c) $M=1$。

(4) $m_0=4$, $m_1=2$。

(5) $L_c=4+2\times 2=8$。

4 GF(2) 上周期为 $N=n2^v$ 序列线性复杂度快速算法及定理 3 的证明

令 $S^M(\beta^i)=[s_{(0)}^n(\beta^i),s_{(1)}^n(\beta^i),\cdots,s_{(M-1)}^n(\beta^i)]$，$M=2^v$ 并且

$$L(\beta^i)=[s_{(0)}^n(\beta^i),s_{(1)}^n(\beta^i),\cdots,s_{(M/2-1)}^n(\beta^i)]$$
$$R(\beta^i)=[s_{(M/2)}^n(\beta^i),s_{(M/2+1)}^n(\beta^i),\cdots,s_{(M-1)}^n(\beta^i)]$$

由 (9)，(10) 式得到

$$\begin{bmatrix} s^N(\alpha^i)\\ s^{N[1]}(\alpha^i)\\ \vdots\\ s^{N[2^v-1]}(\alpha^i)\end{bmatrix}=\begin{bmatrix} H_{M/2}(\alpha^i) & \alpha^{(M/2)i}H_{M/2}(\alpha^i)\\ 0 & H_{M/2}(\alpha^i)\end{bmatrix}\begin{bmatrix} L(\beta^i)^T\\ R(\beta^i)^T\end{bmatrix}\tag{12}$$

从 (12) 式得到

$$\begin{bmatrix} s^N(\alpha^i)\\ s^{N[1]}(\alpha^i)\\ \vdots\\ s^{N[2^v-1]}(\alpha^i)\end{bmatrix}=\begin{bmatrix} H_{M/2}(\alpha^i)[L(\beta^i)^T+\alpha^{(M/2)i}R(\beta^i)^T]\\ H_{M/2}(\alpha^i)R(\beta^i)^T\end{bmatrix}\tag{13}$$

$L(\beta^i)+\alpha^{(M/2)i}R(\beta^i)=b(\beta^i)$, $b(\beta^i)=[b_{(0)}(\beta^i),b_{(1)}(\beta^i),\cdots,b_{(M/2-1)}(\beta^i)]$, $b_{(k)}(\beta^i)=s_{(k)}^n(\beta_i)+\alpha^{(M/2)i}s_{(k+M/2)}^n(\beta^i)$。若 $b(\beta^i)=0$，则 $s^{N[j]}(\alpha^i)=0, j=0,1,\cdots,M/2-1$。即 $m_{i,1}=0$,

$m_i=\sum_{i=1}^{v}m_{i,t}$，由推论 1 可知 $m_i\le M/2$。令 $S^M(\beta^i)=R(\beta^i)$，$M=M/2$。重复以上方法，从矩阵 $H_{2^{v-1}}(\alpha^i)R(\beta^i)$ 中得到 $s^{N[j]}(\alpha^i)$，$j=M/2,M/2-1,\cdots,M-1$。若 $b(\beta^i)\neq 0$，$m_{i,1}=M/2$，$m_i\ge M/2$，令 $S^M(\beta^i)=L(\beta^i)+\alpha^{i(2^{v-1})}R(\beta^i)$，$M=M/2$，从下式 $H_{M/2}[L(\beta^i)+\alpha^{(M/2)i}R(\beta^i)$ 中得到 $s^{N[j]}(\alpha^i)$，$j=0,1,\cdots,M/2-1$。重复上面的过程，直到 $M=1$，得到 $m_i=\sum_{t=1}^{v}m_{i,t}$，求 m_i 的过程由上述的 v 步骤完成。GF(2) 上周期为 $N=n2^v$ 序列线性复杂度为 $L_c=\sum_{i=0}^{n-1}m_i$。

由于 α 是 n 次单位原根，是 GF(2^m) 上的本原元素，GF(2^m) 上的本原多项式可以表示为 $x^m+a_{m-1}x^{m-1}+a_{m-2}x^{m-1}+\cdots+a_1x+1=0$，并且 $\alpha^m=\sum_{i=0}^{m-1}a_{i,j}\alpha^i$，$a_{i,j}=0,1$。$\alpha$ 的 n 次单位原根，可由集合 $\{\alpha^0,\alpha,\alpha^2,\cdots,\alpha^{m-1}\}$ 的 m 个元素线性组合表示，即

$$\alpha^i=a_{i,0}+\alpha_{i,1}\alpha+\cdots+a_{i,m-1}\alpha^{m-1}=A_i\overline{\alpha}^T \tag{14}$$

其中 $A_i=(a_{i,0},a_{i,1},\cdots,a_{i,m-1})$，$a_{i,j}=0,1$。$\overline{\alpha}=(1,\alpha,\cdots,\alpha^{m-1})$。把另一 i 次单位原根 β^i 代入 (7) 式得

$$s^n_{(k)}(\beta^i)=s_k+s_{k+M}\beta^i+\cdots+s_{k+(n-1)M}\beta^{i(n-1)} \tag{15}$$

$$\alpha^{(M/2)i}s^n_{(k+M/2)}(\beta^i)=s_{k+M/2}\alpha^{(M/2)i}+s_{k+M/2+M}\beta^i\alpha^{(M/2)i}+\cdots+s_{k+M/2+(n-1)M}\beta^{i(n-1)}\alpha^{(M/2)i} \tag{16}$$

(1) 当 $i=0$ 时，由 (15), (16) 式得

$$s^n_{(k)}(\beta^i)=s_k+s_{k+M}+\cdots+s_{k+(n-1)M} \tag{17}$$

$$\alpha^{(M/2)i}s^n_{(k+M/2)}(\beta^i)=s_{k+M/2}+s_{k+M/2+M}+\cdots+s_{k+M/2+(n-1)M} \tag{18}$$

$S^M(1)$ 是一 2 元序列，$\alpha^{(M/2)i}R(1)=R(1)$，令 $S^{(M_0)}=S^M(1)$。

(2) 当 $i\neq 0$ 时，由 $\beta=\alpha^{2^v}=\alpha^M$，设 $s_{k,j}=s_{k+j\cdot m}$，$s_{k+M/2,j}=s_{k+M/2+j\cdot M}$ 由 (15), (16) 式得到

$$s^n_{(k)}(\beta^i)=s_{k,0}+s_{k,l}\alpha^{Mi}+\cdots+s_{k,n-1}\alpha^{(n-1)Mi} \tag{19}$$

$$\alpha^{(M/2)i}s^n_{(k+M/2)}(\beta^i)=s_{k+M/2,0}\alpha^{(M/2)i}+s_{k+M/2,1}\alpha^{Mi+(M/2)i}+\cdots+s_{k+M/2,n-1}\alpha^{(n-1)Mi+(M/2)i} \tag{20}$$

若 $M\equiv t(\mathrm{mod}n)$，$(M/2)\equiv s(\mathrm{mod}n)$，则由 (19)，(20) 式得到

$$s^n_{(k)}(\beta^i)=s_{k,0}+s_{k,1}\alpha^{t\cdot i}+\cdots+s_{k,j}\alpha^{t\cdot ji}+\cdots+s_{k,n-1}\alpha^{t\cdot(n-1)i} \tag{21}$$

$$\alpha^{si}s^n_{(k+M/2)}(\beta^i)=s_{k+M/2,0}\alpha^{s\cdot i}+s_{k+M/2,1}\alpha^{t\cdot i+si}+\cdots+s_{k+M/2,j+c}\alpha^{[t\cdot(j+c)+s]i}+\cdots+s_{k+M/2,n-1}\alpha^{t\cdot(n-1)i+si} \tag{22}$$

若 $t(j+c)\cdot i+s\cdot i\equiv tji(\mathrm{mod}n)$，则 $t(j+c)+s=dn+tj$，$c=(dn-s)/t$，d 是使 c 为最小正整数的任意正整数，因此 $s_{k+M/2,j+c}\alpha^{[t(j+c)+s]i}=s_{k+M/2,j+c}\alpha^{t\cdot ji}$，$A_{[t(j+c)+s]i}=A_{t\cdot ji}$ 且

$$a_{[t(j+c)+s]i,h}=a_{t\cdot ji,h},\quad h=0,1,\cdots,n-1 \tag{23}$$

由 (14)， (21) 式有

$$\begin{aligned}s^n_{(k)}(\beta^i)&=s_{k,0}A_0\overline{\alpha}^T+s_{k,1}A_{t\cdot i}\overline{\alpha}^T+s_{k,2}A_{t\cdot 2i}\overline{\alpha}^T+\cdots+s_{k,n-1}A_{t\cdot(n-1)i}\overline{\alpha}^T\\&=f_{k\cdot 0}+f_{k,1}\alpha+\cdots+f_{k,m-1}\alpha^{m-1}\end{aligned} \tag{24}$$

$$f_{k,j}=s_{k,0}a_{0,j}+s_{k,1}a_{t\cdot i,j}+\cdots+s_{k,n-1}a_{t\cdot(n-1)\cdot i,j} \tag{25}$$

由 (14), (22) 式有

$$\begin{aligned}\alpha^{si}s^n_{(k+M/2)}(\beta^i)&=s_{k+M/2,0}A_{si}\overline{\alpha}^T+s_{k+M/2,1}A_{t\cdot(1+c)i}\overline{\alpha}^T+\cdots+s_{k+M/2,n-1}A_{t\cdot(n-1+c)i}\overline{\alpha}^T\\&=f_{k+M/2,0}+f_{k+M/2,1}\alpha+\cdots+f_{k+M/2,m-1}\alpha^{m-1}\end{aligned} \tag{26}$$

$$f_{k+M/2,j}=s_{k+M/2,0}a_{s,j}+s_{k+M/2,1}a_{[t\cdot(1+c)i],j}+\cdots+s_{k+M/2,n-1}a_{[t\cdot(n-1+c)i],J} \tag{27}$$

由于

$$\begin{aligned}b_{(k)}(\beta^i)&=s^n_{(k)}(\beta^i)+\alpha^{(M/2)i}s^n_{(k+M/2)}(\beta^i)\\&=(f_{k,0}+f_{k+M/2,0})+(f_{k,1}+f_{k+M/2,1})\alpha+\cdots+(f_{k,m-1}+f_{k+M/2,m-1})\alpha^{m-1}\end{aligned} \tag{28}$$

若使 (28) 式为 0，则其系数 $f_{k,j}+f_{k+M/2,j}=0$，即由 (23)， (25) 和 (27) 式得

$$(s_{k,0}+s_{k+M/2,c})a_{0,j}+(s_{k,1}+s_{k+M/2,1+c})a_{1,j}+\cdots+(s_{k,n-1}+s_{k+M/2,n-1+c})a_{(n-1),j}=0 \tag{29}$$

由 α 的 j 次根的表达式可知， $a_{0,j}+a_{1,j}+\cdots+a_{(n-1),j}=0$，若使 (29) 式为 0，则 $s_{k,h}+s_{k+M,h+c}=1$， $h,h+c\in\{0,1,\cdots,n-1\}$, 或 $s_{k,h}+s_{k+M,h+c}=0$。因此使 $b_{(k)}(\beta^i)$=0 的条件是对于 $h=0,1,\cdots,n-1$， $s_{k+h\cdot M}+s_{k+(h+c)M}$ 同时为 0 或同时为 1。

由 (21)， (22) 和 (23) 式， $b_{(k)}(\beta^i)$ 可以表示为

$b_{(k)}(\beta^i)=b_{k,0}+b_{k,1}\alpha^{t\cdot i}+\cdots+b_{k,M/2-1}\alpha^{t\cdot(n-1)i}$, $b_{k,j}=s_{k+j\cdot M}+s_{k+(j+c)M}$, $j=0,1,\cdots,M/2$

令 $S^{(M_1)}=(S^{(1)}_{(0)},S^{(1)}_{(1)},\cdots,S^{(1)}_{(M-1)})$, $S^{(1)}_{(k)}=(s_{k,1},s_{k,2},\cdots,s_{k,(n-1)})=(s_k,s_{k+M},\cdots,s_{k+(n-1)2M})$

$L^{(1)}=(S^{(1)}_{(0)},S^{(1)}_{(1)},\cdots,S^{(1)}_{(M/2-1)})$， $R^{(1)}=(S^{(1)}_{(M/2)},S^{(1)}_{(M/2+1)},\cdots,S^{(1)}_{(M-1)})$， $(R^{(1)})'=((S^{(1)}_{(M/2)})'$ $+(S^{(1)}_{(M/2+1)})'+\cdots,(S^{(1)}_{(M-1)})')=(s_{k+M/2,c},s_{K+M/2,1+c},\cdots,s_{k+M/2,h+c},\cdots,s_{k+M/2,n-1+c})$, $h+c\in\{0,1,\cdots,n-1\}$, $h=0,1,\cdots,n-1$, $B^{(1)}=L^{(1)}+(R^{(1)})'$, 如果 $B^{(1)}_j=(00\cdots0)$ 或 $B^{(1)}_j=(11\cdots1)$, $j=0,1,\cdots,M/2-1$，即 $b(\beta^i)=0$， $s^{N[j]}(\alpha^i)=0$， $j=0,1,\cdots$, $M/2-1$， $m_{it}=0$， $m_i\le M/2$。令 $S^{(m_1)}=R^{(1)}$， $S^{(1)}_{(k)}=:S^{(1)}_{(k+M/2)}$， $s_{k,j}=:s_{k+M/2,j}$, $k=0,1,\cdots,M/2-1$， $M=:M/2$。否则 $b(\beta^i)\neq0$， $m_i\ge M/2$，令 $S^{(M_1)}=B^{(1)}$, $S^{(1)}_{(k)}=:(S^{(1)}_{(k)}+(S^{(1)}_{(k+M/2)})')$， $s_{k,j}=b_{k,j}$， $k=0,1,\cdots,M/2-1$。$m_{it}=M/2$, $M=:M/2$。重复上面的过程，直到 $M=1$，得到 $m_i=\sum_{t=1}^{v}m_{it}$。

由 (21)， (22) 和 (23) 式可知，当 $1\le i\le n-1$ 时，使 $b(\beta^i)=0$ 即 $b_{(k)}(\beta^i)=0$ 的条件是 $s_{k+h\cdot M}+s_{k+(h+c)M}$ 同时为 0 或同时为 1， $h=0,1,\cdots,n-1$。因此当 $1\le i\le n-1$ 时, $S^{N[j]}(\alpha^i)$ 相同，即 $m_1=m_2=\cdots=m_{n-1}$。　　证毕

求 GF(2) 上的周期为 $N = n2^v(\gcd(n,2) = 1)$ 序列线性复杂度快速算法，其计算速度比用 GDFT 的方法求序列线性复杂度快指数级，利用 GDFT 求其线性复杂度要对多项式求 2^v 次 Hasse 导数，文中给出的快速算法只需 v 次的加运算，计算复杂度由指数级 $O(2^v)$ 减少到一次多项式级 $O(v)$。另外由于定理 3 的给出，使得求周期为 $N = n2^v$ 序列线性复杂度减少了 $n-2$ 次求 m_i 的重复运算，计算速度有了显著的提高。

4 结 束 语

在对 GF(p) 上周期为 $N = np^v(\gcd(n,p) = 1)$ 序列线性复杂度研究的基础上，给出了求 GF(2) 上周期为 $N = n2^v(\gcd(n,2) = 1)$ 序列线性复杂度的快速算法，并得到了用 Hasse 导数求 GF(2) 上的周期为 $N = n2^v(\gcd(n,2) = 1)$ 序列线性复杂度的新结果，使得求其序列线性复杂度快速有效，对于研究 GF(p) 上周期为 $N = np^v(\gcd(n,p) = 1)$ 序列线性复杂度提供了一种途径，可在此基础上研究其 k-错线性复杂度的快速算法。

参 考 文 献

[1] R. A. Games, A. H. Chan, A fast algorithm for determining the complexity of a binary sequence with period 2^n, IEEE Tans. on Inform. Theory, 1983, 29(3), 144–146.

[2] K.Imamura, T. Moriuchi, A fast algorithm for determining the linear complexity of p-ary sequence with period p^n, p a prime, IEICE Tech. Rep, 1993, in Japanese, 75(1), 73–78.

[3] J. L. Massey, S. Serconek, Linear complexity of periodic sequencs, A general theory, Advances in Cryptology-CRYPTO'96, USA, 1996, 358–371.

[4] C. Ding, G. Xiao, W. Shan, The Stability of Stream Ciphers, Lecture Notes in Computer Science, Spinger-Verlag, 1991, Ch.5, 81–129.

[5] S. R. Blackburn, A generalisation of the discrete Fourier transfrom: determining the minimal polynomial of a periodic, IEEE Trans. on Info. Theory, 1994, 40(5), 1702–1705.

A FAST ALGORITHM FOR DETERMING THE LINEAR COMPLEXITY OF A PSEUDO-RANDOM SEQUENCE WITH PERIODIC $n2^v$

Cai Mian* ** Wang Hong** Xiao Guozhen**

*(*National Key Laboratory of Integrated Services Networks and Research Inst. of Information Security, Xidian Univ., Xi'an* 710071, *China*)

**(*National Key Laboratory of Information Security, The Graduate School of the Chinese Academy of Sciences, Beijing* 100039, *China*)

Abstract A generalizd discrete Fourier transfom is used to give a fast algorithm for determing the linear complexity of a pseudo-random sequence with periodic $n2^v$, and a new conclusion of Hasse derivatives of polynoimial on GF(2) are proposed.

Key words Linear complexity, Discrete Fourier transform, Hasse derivatives

蔡 勉：女，1960 年生，副教授，研究方向为密码学.

王 宏：男，1972 年生，工程师，研究方向为密码学.

肖国镇：男，1934 年生，教授，研究方向为密码学.