F_p上p^n-周期序列的 1-错线性复杂度

朱凤翔　　戚文峰
(信息工程大学信息工程学院应用数学系 郑州　450002)

摘　要: 周期序列的线性复杂度和 k-错线性复杂度是衡量密钥流序列随机性的两个重要指标。该文给出了 $\boldsymbol{F}_p$ 上 p^n -周期的序列所有可能的 1-错线性复杂度的值以及具有给定 1-错线性复杂度的序列个数。更进一步, 该文给出了 $\boldsymbol{F}_p$ 上 p^n -周期的序列 1-错线性复杂度的期望。

关键词：线性复杂度；1-错线性复杂度； $\boldsymbol{F}_p$ 上周期序列；广义 Chan-Games 算法
中图分类号：TN918　　**文献标识码**：A　　**文章编号**：1009-5896(2007)09-2222-04

1-error Linear Complexity of p^n-Periodic Sequences over F_p

Zhu Feng-xiang　　Qi Wen-feng
(*Dept of Appl. Math., Info. Eng. Inst., Eng. Univ., Zhengzhou* 450002, *China*)

Abstract: The linear complexity and the k–error linear complexity of a periodic sequence are two important standards to scale the randomicity of keystreams. For a p^n -periodic sequence over $\boldsymbol{F}_p$, the possible values of the 1-error linear complexity and the number of sequences with certain 1-error linear complexity are established. Moreover, the expected value of the 1-error linear complexity for a random p^n-periodic sequence over $\boldsymbol{F}_p$ is also given.

Key words: Linear complexity; 1-error linear complexity; Periodic sequence over $\boldsymbol{F}_p$; Generalized Chan-Games algorithm

1　引言

设 p 为素数, $s=(s_0,s_1,\cdots,s_{N-1})^\infty$ 是有限域 $\boldsymbol{F}_p$ 上 N -周期(不必是最短周期)序列, 则存在非负整数 L 和 $\boldsymbol{F}_p$ 中系数 $d_1,d_2,\cdots,d_L$ 使得 $s_i+d_1s_{i-1}+\cdots+d_Ls_{i-L}=0$ 对于所有 $i\ge L$ 成立。定义 s 的线性复杂度 $\mathrm{LC}(s)$ 为满足上式的最小的 L , 即能生成该序列的最短线性反馈移位寄存器长度。特别地, 当 s 为0序列时, 令 $\mathrm{LC}(s)=0$ 。在密钥流的伪随机性研究中, 线性复杂度是一个非常重要的指标。为了抵抗Berlekamp-Massey算法的攻击, 适合做密钥流的序列不仅应具有很高的线性复杂度而且在改变几个比特的情况下, 其线性复杂度也不能大幅度下降。根据这一需求, Ding, Xiao和Shan[1]在Stamp和Martin[2]工作的基础上提出了一个衡量序列线性复杂度的指标。

定义1　设 $s=(s_0,s_1,\cdots,s_{N-1})^\infty$ 是 $\boldsymbol{F}_p$ 上 N - 周期序列, p 为素数, 定义 s 的 k -错线性复杂度为改变至多 k 个 s_i 所得到序列的最小线性复杂度, 记为 $\mathrm{LC}_k(s)$ 。

近来, 将二元周期序列如Legendre序列, Sidelnikov序列看成 $\boldsymbol{F}_p$ 上的周期序列, 对其 k -错线性复杂度的研究得到了广泛的关注[3, 4]。在文献[5]中, Meidl和Niederreiter给出了有限域 $\boldsymbol{F}_p$ 上线性复杂度为 c 的 p^n -周期序列个数,

$$N_0(c)=(p-1)p^{c-1},\quad c\ge 1\ \text{且}\ N_0(0)=1 \tag{1}$$

由此易得 $\mathbf{F}_p$ 上 p^n -周期线性复杂度的期望 $E_{p^n,0}=p^n-\dfrac{1-p^{-p^n}}{p-1}$ 。同时也给出了 $\boldsymbol{F}_p$ 上 p^n -周期序列 k -错线性复杂度期望 $E_{p^n,k}$ 的下界 $E_{p^n,k}\ge N-\log_p\left(\sum\limits_{t=0}^{k}\binom{N}{t}(p-1)^t\right)-\dfrac{p}{p-1}$ 。当 $p=2$ 时, Meidl 给出了具有最大线性复杂度 2^n 序列的 k-错线性复杂度的均值, $k=1,2$, 以及任意一条随机 2^n -周期序列的 1-错线性复杂度均值(见文献[5])。更多的相关工作见文献[6, 7–9]。

本文讨论了 $\boldsymbol{F}_p$ 上 p^n -周期序列的1-错线性复杂度。首先回顾了 $\boldsymbol{F}_p$ 上 p^n -周期线性复杂度的一些基本知识, 然后给出了 $\boldsymbol{F}_p$ 上 p^n -周期序列所有可能的1-错线性复杂度值以及具有给定1-错线性复杂度的序列个数。更进一步, 计算了 $\boldsymbol{F}_p$ 上 p^n -周期随机序列1-错线性复杂度的均值。

2　预备知识

定义 N -周期序列 s 的Hamming重量为 s 一个周期中非零项的个数, 记为 $W(s)$, 定义向量 $\boldsymbol{s}^N$ 的Hamming重量为 $\boldsymbol{s}^N$ 中非零项个数, 记为 $W(\boldsymbol{s}^N)$ 。显然, 如果向量 $\boldsymbol{s}^N$ 对应于 N -周期序列 s 的一个周期, 则 $W(s)=W(\boldsymbol{s}^N)$ 。记 $\boldsymbol{F}_p$ 上无限序列 s=$(s_0,s_1,\cdots)$ 的生成函数为 $s(x)$=$s_0+s_1x+s_2x^2+\cdots$, 向量 $\boldsymbol{s}^N=(s_0,s_1,\cdots,s_{N-1})\in\boldsymbol{F}_p^N$ 的生成函数为 $\boldsymbol{s}^N(x)=s_0+$

2006-10-17收到, 2007-04-02改回
国家自然科学基金(60673081)和国家“863”项目(2006AA01Z417)资助课题

$s_1x+\cdots+s_{N-1}x^{N-1}$，则 $s(x)=\boldsymbol{s}^N(x)(1+x^N+x^{2N}+\cdots)=\boldsymbol{s}^N(x)/(1-x^N)$。易知，序列 s 的线性复杂度为[1]

$$\mathrm{LC}(s)=N-\deg(\gcd(1-x^N,\boldsymbol{s}^N(x))) \tag{2}$$

为方便起见，定义向量 $\boldsymbol{s}^N=(s_0,s_1,\cdots,s_{N-1})$ 的线性复杂度为以 $\boldsymbol{s}^N$ 为一个周期的序列 $s=(s_0,s_1,\cdots,s_{N-1})^\infty$ 的线性复杂度，即 $\mathrm{LC}(s)=\mathrm{LC}(\boldsymbol{s}^N)$。此外，若 $N=p^n$，简记 $\boldsymbol{s}^{(n)}=\boldsymbol{s}^{p^n}$。

设非负整数 i 的 p 进制表示为 $(i_0,i_1,\cdots,i_{m-1})$，定义 $\mathrm{Prod}(i)=\prod_{j=0}^{m-1}(i_j+1)$。在文献[10]中，Kurosawa 等证明了 $\boldsymbol{F}_p$ 上 p^n -周期序列 k -错线性复杂度严格小于其线性复杂度的最小 k 值 $k_{\min}$ 满足

$$k_{\min}=\mathrm{Prod}(p^n-\mathrm{LC}(s)) \tag{3}$$

给定 $\boldsymbol{F}_p$ 上 p^n -周期序列 s，可以利用广义Chan-Games算法决定其线性复杂度 $\mathrm{LC}(s)$ [2, 1]。该算法是本文研究的重要工具，先回顾一下该算法。设 $\boldsymbol{s}^{(n)}=(s_0^{(n)},s_1^{(n)},\cdots,s_{p^n-1}^{(n)})$ 对应于序列 s 的一个周期，且将 $\boldsymbol{s}^{(n)}$ 写成

$\boldsymbol{s}^{(n)}=(\boldsymbol{s}(0)^{(n)},\boldsymbol{s}(1)^{(n)},\cdots,\boldsymbol{s}(p-1)^{(n)})$，其中 $\boldsymbol{s}(i)^{(n)}=(s_{ip^{n-1}}^{(n)},s_{ip^{n-1}+1}^{(n)},\cdots,s_{(i+1)p^{n-1}-1}^{(n)})$，$0\le i\le p-1$。

(1)初始化：$N=p^n,\mathrm{LC}(s)=0$，$\boldsymbol{s}^{(n)}=(\boldsymbol{s}(0)^{(n)},\boldsymbol{s}(1)^{(n)},\cdots,\boldsymbol{s}(p-1)^{(n)})$，$m=n$。

(2)重复下面的步骤直到 $m=0$。

(a)由 p^m 维向量 $\boldsymbol{s}^{(m)}$ 计算得到 p 个 p^{m-1} 维向量：$\boldsymbol{b}(0)^{(m-1)},\boldsymbol{b}(1)^{(m-1)},\cdots,\boldsymbol{b}(p-2)^{(m-1)}$，其中

$$\begin{aligned}\boldsymbol{b}(i)^{(m-1)}&=f_i(\boldsymbol{s}(0)^{(m)},\boldsymbol{s}(1)^{(m)},\cdots,\boldsymbol{s}(p-1)^{(m)})\\&=\sum_{j=0}^{p-i-1}c_{i,j}\boldsymbol{s}(j)^{(m)},\ i=0,1,\cdots,p-2,\end{aligned}$$

$$f_i(x_0,\cdots x_{p-1})=\sum_{j}^{p-i-1}c_{i,j}x_j,\ c_{i,j}=\binom{p-j-1}{i}$$

(b)选择下面 p 种情形之一。

情形 w：$0\le w\le p-2$

$\boldsymbol{b}(0)^{(m-1)}=\ldots=\boldsymbol{b}(w-1)^{(m-1)}=0$，$\boldsymbol{b}(w)^{(m-1)}\ne 0$。

情形 $p-1$：$\boldsymbol{b}(0)^{(m-1)}=\cdots=\boldsymbol{b}(p-2)^{(m-1)}=0$。

(c)如果是情形 w，$0\le w\le p-1$，则

$$\boldsymbol{s}^{(m-1)}\leftarrow f_w(\boldsymbol{s}(0)^{(m)},\boldsymbol{s}(1)^{(m)},\cdots,\boldsymbol{s}(p-1)^{(m)})$$

且 $\mathrm{LC}\leftarrow\mathrm{LC}+(p-w-1)p^{m-1}$，$m\leftarrow m-1$，返回 i)，其中 $f_{p-1}(x_0,\cdots,x_{p-1})=x_0$。

(3)设 $\boldsymbol{s}^{(0)}=(s_0^{(0)})$，如果 $s_0^{(0)}\ne 0$，则 $\mathrm{LC}\leftarrow\mathrm{LC}+1$。

最终的 LC 即为序列 s 的线性复杂度。

需要特别强调的是 $\mathrm{LC}(s)=p^n$ 时的情况。根据广义 Chan-Games 算法，如果 $\mathrm{LC}(s)=p^n=1+(p-1)+\cdots+(p-1)p^{n-1}$，则

$\boldsymbol{b}(0)^{(m-1)}=\boldsymbol{s}(0)^{(m)}+\boldsymbol{s}(1)^{(m)}+\cdots+\boldsymbol{s}(p-1)^{(m)}\ne 0,1\le m\le n$ 且 $s_0^{(0)}\ne 0$。从而该算法诱导出一个从 $\boldsymbol{F}_p^{p^m}$ 到 $\boldsymbol{F}_p^{p^{m-1}}$ 的映射 $\varphi_m, m\ge 1$：

$$\begin{aligned}\varphi_m(\boldsymbol{s}^{(m)})&=\varphi_m(\boldsymbol{s}(0)^{(m)},\boldsymbol{s}(1)^{(m)},\cdots,\boldsymbol{s}(p-1)^{(m)})\\&=\boldsymbol{s}(0)^{(m)}+\cdots+\boldsymbol{s}(p-1)^{(m)}\end{aligned}$$

显然映射 φ_m 具有以下性质：(1) $W(\varphi_m(\boldsymbol{s}^{(m)}))\le W(\boldsymbol{s}^{(m)})$，(2) $\boldsymbol{s}^{(m-1)}$ 的原像集合为 $\varphi_m^{-1}(\boldsymbol{s}^{(m-1)})=\{\boldsymbol{v}\in\boldsymbol{F}_p^{p^m}\mid\varphi_m(\boldsymbol{v})=\boldsymbol{s}^{(m-1)}\}$，该集合的势为 $p^{(p-1)p^{m-1}}$。

3　1-错线性复杂度及其均值

本节将给出 $\boldsymbol{F}_p$ 上具有给定1-错线性复杂度的 p^n -周期序列个数的具体表达式，并计算 $\boldsymbol{F}_p$ 上 p^n -周期序列1-错线性复杂度的均值。

为了讨论 $\boldsymbol{F}_p$ 上线性复杂度为 p^n 的 p^n -周期序列的1-错线性复杂度，先给出几个引理。

引理 1[8]　设 $s=(s_0,s_1,\cdots,s_{p^n-1})^\infty$ 是 $\boldsymbol{F}_p$ 上 p^n -周期序列，如果 s 具有ZSP性质，则 $\mathrm{LC}(s)\le p^n-1$，否则 $\mathrm{LC}(s)=p^n$，其中序列 s 具有ZSP性质是指 s 满足 $\sum_{i=0}^{p^n-1}s_i=0$。

引理 2　设 $u_0,u_1,\cdots,u_{p-1}$ 是 $\boldsymbol{F}_p$ 上满足下式的 p 个元素，

$$u_0+u_1+\cdots+u_{p-1}=a \tag{4}$$

$$(p-1)u_0+(p-2)u_1+\cdots+u_{p-2}=b \tag{5}$$

其中 $a,b\in\boldsymbol{F}_p,a\ne 0$。改变集合 $\{u_0,u_1,\cdots,u_{p-1}\}$ 中的某个元素可以使式(4)右边变成0，同时使式(5)右边变成 $b',b'\ne b,b'\in\boldsymbol{F}_p$，并且这样的改变方法是唯一的。

证明　由于 $a,b\in\boldsymbol{F}_p,a\ne 0$，存在唯一的整数 $d\in\boldsymbol{F}_p$ 使得 $b-b'=ad \mod p$。如果元素 u_{p-d-1} 被改变成 $u_{p-d-1}-a$，则 $u_0+u_1+\cdots+u_{p-1}-a=0$ 而且

$$\begin{aligned}&(p-1)u_0+\cdots+d(u_{p-d-1}-a)+\cdots+u_{p-2}\\&=(p-1)u_0+(p-2)u_1+\cdots+u_{p-2}-ad=b-ad=b'\end{aligned}$$

由 d 选择的唯一性易知这样的改变方法是唯一的。　证毕

定理 1　设整数 $L_{r,c}$ 形如 $L_{r,c}=p^n-p^{r+1}+c,0\le r\le n-1,1\le c\le p^r(p-1)-1$，则 $\boldsymbol{F}_p$ 上 $\mathrm{LC}(s)=p^n$ 且 $\mathrm{LC}_1(s)=L_{r,c}$ 的 p^n -周期序列 s 个数 $N_1(L_{r,c})$ 是 $N_1(L_{r,c})=(p-1)^2\cdot p^{p^n-p^{r+1}+c+r}$ 且 $N_1(0)=(p-1)p^n$。对于不是 $L_{r,c}$ 形式的正整数 L，不存在 $\boldsymbol{F}_p$ 上 $\mathrm{LC}(s)=p^n$ 且 $\mathrm{LC}_1(s)=L$ 的 p^n -周期序列。

证明　设 $\boldsymbol{s}^{(n)}=(s_0,s_1,\cdots,s_{p^n-1})$ 是线性复杂度为 p^n 的序列 s 一个周期所对应的向量. 由广义 Chan-Games 算法知对于每个 $\boldsymbol{s}^{(m)}=(\boldsymbol{s}(0)^{(m)},\boldsymbol{s}(1)^{(m)},\cdots,\boldsymbol{s}(p-1)^{(m)})$ 满足

$$\varphi_m(\boldsymbol{s}^{(m)})=\boldsymbol{s}(0)^{(m)}+\boldsymbol{s}(1)^{(m)}+\cdots+\boldsymbol{s}(p-1)^{(m)}\ne 0,\quad 1\le m\le n \tag{6}$$

显然，当 $W(s)=W(\boldsymbol{s}^{(n)})=1$ 时，线性复杂度达到最大 p^n 且 1-错线性复杂度 $\mathrm{LC}_1(s)=0$ 的序列个数为 $(p-1)p^n$，即 $N_1(0)=(p-1)p^n$。

下面讨论 $W(s)=W(\boldsymbol{s}^{(n)})>1$ 的情形。

(1) 证明 $\mathrm{LC}_1(s)=L_{r,c}$　由式(6)，若 $0\le m\le n-1$，$W(s)=W(\boldsymbol{s}^{(n)})>1$，则 $\boldsymbol{s}^{(m)}=\varphi_{m-1}\cdots\varphi_{n-1}\varphi_n(\boldsymbol{s}^{(n)})$ 不可能是 $\boldsymbol{F}_{p^m}$ 上的 0 向量。设 $r,0\le r\le n-1$，是使得 $W(\boldsymbol{s}^{(r)})=1$ 成立的最大整数，则对于整数 $j,r<j<n$，有 $W(\boldsymbol{s}^{(j)})>1$。也就是说，改变 $\boldsymbol{s}^{(n)}$ 中的任意一个比特都不可能将 $\boldsymbol{s}^{(j)}$ 变成 0,

从而 $\mathrm{LC}_1(s)>(p-1)p^{n-1}+\cdots+(p-1)p^{r+1}$。

由式(6)知，要改变 $\boldsymbol{s}^{(r+1)}=(\boldsymbol{s}(0)^{(r+1)},\boldsymbol{s}(1)^{(r+1)},\cdots,\boldsymbol{s}(p-1)^{(r+1)})$ 中的某个元素可以由改变 $\boldsymbol{s}^{(n)}$ 中的一个恰当的元素得到(为叙述方便，下文将直接说改变 $\boldsymbol{s}^{(r+1)}$ 中的一个元素)，从而使 $\boldsymbol{s}^{(r)}=\boldsymbol{s}(0)^{(r+1)}+\cdots+\boldsymbol{s}(p-1)^{(r+1)}=0$。根据广义 Chan-Games 算法递归过程可知，这样的改变可以避免线性复杂度增加 $(p-1)p^r$。由此可得 $\mathrm{LC}_1(s)$ 必形如

$$L_{r,c}=(p-1)p^{n-1}+\cdots+(p-1)p^{r+1}+c,\quad 1\le c\le(p-1)p^r,$$

其中 c 是 $\boldsymbol{s}^{(r+1)}$ 被改变后可能的最小线性复杂度。

下面证明 $c\ne(p-1)p^r$，注意到 $W(\boldsymbol{s}^{(r)})=1$，设 $\boldsymbol{s}^{(r)}=(0,\cdots,s_v^{(r)}\cdots,0),s_v^{(r)}\in\boldsymbol{F}_p^*\setminus\{0\}$ 且 $\boldsymbol{s}^{(r+1)}=(\boldsymbol{s}(0)^{(r+1)},\boldsymbol{s}(1)^{(r+1)},\cdots,\boldsymbol{s}(p-1)^{(r+1)})$，其中 $\boldsymbol{s}(i)^{(r+1)}=(s_{ip^r}^{(r+1)},s_{ip^r+1}^{(r+1)},\cdots,s_{(i+1)p^r-1}^{(r+1)})$，$0\le i\le p-1$。由式(6)，$\boldsymbol{s}^{(r)}=\varphi_{r+1}(\boldsymbol{s}^{(r+1)})=\boldsymbol{s}(0)^{(r+1)}+\cdots+\boldsymbol{s}(p-1)^{(r+1)}$，则

$$s_v^{(r+1)}+s_{p^r+v}^{(r+1)}+\cdots+s_{(p-1)p^r+v}^{(r+1)}=s_v^{(r)}\tag{7}$$

如果 $c=(p-1)p^r$，即 $\boldsymbol{s}^{(r+1)}$ 线性复杂度被改变成 $(p-1)p^r=(p-2)p^r+p^r$，根据广义 Chan-Games 算法，改变后的 $\boldsymbol{s}^{(r+1)}$ 满足

$$\boldsymbol{b}(1)^{(r)}=(p-1)\boldsymbol{s}(0)^{(r+1)}+(p-2)\boldsymbol{s}(1)^{(r+1)}+\cdots+\boldsymbol{s}(p-2)^{(r+1)}\ne0$$

这使得线性复杂度增加 $(p-2)p^r$ 且 $\mathrm{LC}(\boldsymbol{b}(1)^{(r)})=p^r$。由引理1，$\boldsymbol{b}(1)^{(r)}$ 不具有 ZSP 性质，即 $\boldsymbol{b}(1)^{(r)}$ 中所有元素和不等于0。但对于 $\boldsymbol{b}(1)^{(r)}$ 中的元素

$$(p-1)s_v^{(r+1)}+(p-2)s_{p^r+v}^{(r+1)}+\cdots+s_{(p-2)p^r+v}^{(r+1)}\in\boldsymbol{F}_p\tag{8}$$

由引理 2，改变 $\{s_v^{(r+1)},s_{p^r+v}^{(r+1)},\cdots,s_{(p-1)p^r+v}^{(r+1)}\}$ 中一个适当的比特可以使式(7)变成 0 同时式(8)被改变成任意其它的值。选择一个恰当的值使 $\boldsymbol{b}(1)^{(r)}$ 通过一个比特的改变后具有 ZSP 性质，再由引理1，$\mathrm{LC}(\boldsymbol{b}(1)^{(r)})\le p^r-1<p^r$。也就是说，改变 $\boldsymbol{s}^{(r+1)}$ 中的一个比特可以使 $\boldsymbol{s}^{(r)}$ 变成0同时使改变后的 $\boldsymbol{s}^{(r+1)}$ 线性复杂度小于 $p^r+(p-2)p^r=(p-1)p^r$，这与 $c=(p-1)p^r$ 矛盾。因此序列 s 的 1-错线性复杂度 $\mathrm{LC}_1(s)$ 为 $L_{r,c}=p^n-p^{r+1}+c,0\le r\le n-1,1\le c\le p^r(p-1)-1$，其中 c 是改变后 $\boldsymbol{s}^{(r+1)}$ 可能的最小线性复杂度。

(2)满足 $\mathrm{LC}_1(s)=L_{r,c}$ 且 $\mathrm{LC}(s)=p^n$ 的序列个数的计算

对于任意满足 $\varphi_{r+1}(\boldsymbol{s}^{(r+1)})=\boldsymbol{s}^{(r)}=(0,\cdots,s_v^{(r)},\cdots,0)$ 的 $\boldsymbol{s}^{(r+1)}$，根据上述讨论，改变集合 $\{s_v^{(r+1)},s_{p^r+v}^{(r+1)},\cdots,s_{(p-1)p^r+v}^{(r+1)}\}$ 中一个比特可以使得 $\boldsymbol{s}^{(r)}$ 变成0且 $\boldsymbol{s}^{(r+1)}$ 的线性复杂度变成最小值 c，$1\le c\le p^r(p-1)-1$。断言对于给定的向量 $\boldsymbol{s}^{(r)}$ 和整数 c，这样的改变是唯一的。否则，改变向量 $\boldsymbol{s}^{(r+1)}$ 中的一个比特得到线性复杂度为 c，$1\le c\le p^r(p-1)-1$ 的两个不同的向量，分别设为 $(\alpha_0,\alpha_1,\cdots,\alpha_{p^{r+1}-1})$ 和 $(\beta_0,\beta_1,\cdots,\beta_{p^{r+1}-1})$，即

$$\alpha_0+\alpha_1x+\cdots+\alpha_{p^{r+1}-1}x^{p^{r+1}-1}+\gamma x^{ip^r+v}=\beta_0+\beta_1x+\cdots+\beta_{p^{r+1}-1}x^{p^{r+1}-1}+\gamma' x^{jp^r+v}$$

其中 $\gamma,\gamma'\in\boldsymbol{F}_p$，$0\le i<j\le p-1$。由式(2)可知，$(1-x)^{p^{r+1}-c}$ 分别整除

$$\alpha_0+\alpha_1x+\cdots+\alpha_{p^{r+1}-1}x^{p^{r+1}-1}=\beta_0+\beta_1x+\cdots+\beta_{p^{r+1}-1}x^{p^{r+1}-1}+\gamma' x^{jp^r+v}-\gamma x^{ip^r+v}$$

和 $\beta_0+\beta_1x+\cdots+\beta_{p^{r+1}-1}x^{p^{r+1}-1}$，则 $(1-x)^{p^{r+1}-c}\mid\gamma' x^{jp^r+v}-\gamma x^{ip^r+v}$。由于 $1\le c\le p^r(p-1)-1$，即 $p^r+1\le p^{r+1}-c\le p^{r+1}-1$，从而 $\gamma'=\gamma$ 且 $(1-x)^{p^{r+1}-c}\mid\gamma' x^{jp^r+v}-\gamma x^{ip^r+v}=\gamma x^{jp^r+v}(x^{j-i}-1)^{p^r}$。另一方面，对于 $0\le i<j\le p-1$，即 $0<j-i\le p-1$，有 $(x-1)\mid x^{j-i}-1$，但 $(x-1)^2\nmid x^{j-i}-1$，因此 $(x-1)^{p^r}\mid(x^{j-i}-1)^{p^r}$，但 $(x-1)^{p^r+1}\nmid(x^{j-i}-1)^{p^r}$，即 $(1-x)^{p^{r+1}}\nmid\gamma' x^{jp^r+v}-\gamma x^{ip^r+v}$ 这与 $(1-x)^{p^{r+1}-c}\mid\gamma' x^{jp^r+v}-\gamma x^{ip^r+v}$ 矛盾，断言成立。

给定的向量 $\boldsymbol{s}^{(r)}$ 和整数 c，$1\le c\le p^r(p-1)-1$，满足 $\varphi_{r+1}(\boldsymbol{s}^{(r+1)})=\boldsymbol{s}^{(r)}$ 且 $\boldsymbol{s}^{(r+1)}$ 被改变称线性复杂度为 c 的相同向量有 p 种可能。由式(1)可知有 $(p-1)p^{c-1}$ 条线性复杂度为 c 的 p^{r+1}-周期序列，其中 $1\le c\le p^r(p-1)-1$。因此给定 $\boldsymbol{s}^{(r)}$ 和整数 c，有 $p\cdot(p-1)p^{c-1}=(p-1)p^c$ 种情况使得 $\varphi_{r+1}(\boldsymbol{s}^{(r+1)})=\boldsymbol{s}^{(r)}$ 且改变后 $\boldsymbol{s}^{(r+1)}$ 的线性复杂度为 c。另一方面，$\boldsymbol{s}^{(r)}$ 有 $p^r(p-1)$ 种选择，递归运用 φ_n 的性质 2 可得 $\boldsymbol{F}_p$ 上 $\mathrm{LC}(s)=p^n$ 且 $\mathrm{LC}_1(s)=L_{r,c}$ 的 p^n-周期序列 s 个数 $N_1(L_{r,c})$ 为

$$p^{(p-1)p^{n-1}}\cdot p^{(p-1)p^{n-2}}\cdots p^{(p-1)p^{r+1}}\cdot(p-1)p^r\cdot(p-1)p^c=(p-1)^2p^{p^n-p^{r+1}+c+r}$$

其中 $1\le c\le p^r(p-1)-1$，$0\le r\le n-1$。　　证毕

由定理 1 知，当 $p\ge3$ 时，$N_1(L_{0,p-2})=(p-1)^2p^{p^n-2}$，容易计算 $\boldsymbol{F}_p$ 上有 $(p-1)/p$ 条的 p^n-周期序列线性复杂度为 p^n、1-错线性复杂度为 p^n-2。这说明了在一般情况下 $\boldsymbol{F}_p$ 上线性复杂度为 p^n 的 p^n-周期序列在改变每个周期一个比特后线性复杂度不会大幅度下降。由定理 1 的结论可以计算 $\boldsymbol{F}_p$ 上线性复杂度为 p^n 的 p^n-周期序列 1-错线性复杂度均值。

定理 2　设 $E_{1|\mathrm{LC}(s)=p^n}$ 表示 $\boldsymbol{F}_p$ 上线性复杂度为 p^n 的 p^n-周期序列 1-错线性复杂度均值，若 $p,n\ge3$，则 $E_{1|\mathrm{LC}(s)=p^n}=p^n-1-\sum_{r=1}^{n-1}p^{-p^r+r+1}+(p^{-p^n+n+1}-1)/(p-1)$。

证明　由式(1)，有 $(p-1)p^{p^n-1}$ 条线性复杂度为 p^n 的 p^n-周期序列，则根据等式 $\sum_{c=0}^{m}cp^c=mp^{m+1}/(p-1)-(p^{m+1}-p)/(p-1)^2$，可得:

$$\begin{aligned}(p-1)p^{p^n-1}E_{1|\mathrm{LC}(s)=p^n}&=\sum_{r=0}^{n-1}\sum_{c=1}^{p^r(p-1)-1}N_1(L_{r,c})L_{r,c}\\&=\sum_{r=0}^{n-1}\sum_{c=1}^{p^r(p-1)-1}(p^n-p^{r+1}+c)\cdot(p-1)^2p^{p^n-p^{r+1}+c+r}\\&=p^{p^n}\sum_{r=0}^{n-1}(p-1)^2p^{-p^{r+1}+r}\left[\sum_{c=1}^{p^r(p-1)-1}(p^n-p^{r+1})\cdot p^c+\sum_{c=1}^{p^r(p-1)-1}c\cdot p^c\right]\end{aligned}$$

$$
\begin{aligned}
&= p^{p^n}\sum_{r=0}^{n-1} p^{-p^{r+1}+r}(p-1)[(p^n-p^{r+1})(p^{p^r(p-1)}-p)\\
&\quad + p^{p^r(p-1)}(p^{r+1}-p^r-1)] - p^{p^n}\sum_{r=0}^{n-1} p^{-p^{r+1}+r}(p^{p^r(p-1)}-p)\\
&= p^{p^n+n}(p-1)\sum_{r=0}^{n-1} p^{-p^{r+1}+r}(p^{p^r(p-1)}-p) - p^{p^n}(p-1)\\
&\quad \cdot\sum_{r=0}^{n-1} p^{-p^{r+1}+r}(p^{p^r(p-1)+r}-p^{r+2}) - (p-1)\\
&\quad \cdot\sum_{r=0}^{n-1} p^{p^n-p^r+r} - p^{p^n-1} + p^n\\
&= p^{p^n+n}(p-1)(p^{-1}-p^{-p^n+n}) - p^{p^n}(p-1)(p^{-1}-p^{-p^n+2n})\\
&\quad -(p-1)\sum_{r=0}^{n-1} p^{p^n-p^r+r} - p^{p^n-1} + p^n\\
&= p^{p^n}[(p-1)p^{n-1}-2+p^{-1}] + p^n - (p-1)\sum_{r=0}^{n-1} p^{p^n-p^r+r}
\end{aligned}
$$

两边同时整除 $(p-1)p^{p^n-1}$ 即得结论。　　证毕

注 $E_{1|\mathrm{LC}(s)=p^n}$ 表达式中的和式 $\sum_{r=1}^{n-1} p^{-p^r+r+1}$ 是很小的。例如当 $p=3$ 时，该和式接近 0.3347，相对于 3^n-1 要小得多。

定理 3 设 s 是 $\boldsymbol{F}_p$ 上 p^n -周期序列，如果 $\mathrm{LC}(s)<p^n$，则 $\mathrm{LC}_1(s)=\mathrm{LC}(s)$。

证明 由式(3)立即可得该结论。

由定理 1 和定理 3 可以计算 $\boldsymbol{F}_p$ 上 p^n -周期随机序列 1-错线性复杂度均值。

推论 1 设 E_1 表示 $\boldsymbol{F}_p$ 上 p^n -周期随机序列 1-错线性复杂度均值，若 $p, n\ge 3$ 则

$$
\begin{aligned}
E_1 &= p^n - 2 + p^{-p^n+n}\\
&\quad -(1-p^{-p^n})/(p^2-p) - (p-1)\sum_{r=1}^{n-1} p^{-p^r+r}
\end{aligned}
$$

证明　由式(3)，将 $p^{-p^n}\sum_{L=1}^{p^n-1}(p-1)p^{L-1}L$ 加上 $(p-1)p^{-1}E_{1|\mathrm{LC}(s)=p^n}$ 可得

$$
\begin{aligned}
E_1 &= (p-1)p^{-1}E_{1|\mathrm{LC}(s)=p^n} + p^{-p^n}\sum_{L=0}^{p^n-1}(p-1)p^{L-1}L\\
&= (p-1)p^{-1}[p^n-1-\sum_{r=1}^{n-1} p^{-p^r+r+1} + (p^{-p^n+n+1}-1)\\
&\quad /(p-1)] + p^{n-1} - p^{-1} - (p^{-1}-p^{-p^n})/(p-1)\\
&= p^n - 1 - p^{n-1} - (p-1)\sum_{r=1}^{n-1} p^{-p^r+r} + p^{-p^n+n}\\
&\quad + p^{n-1} - p^{-1} - (p^{-1}-p^{-p^n})/(p-1)\\
&= p^n - 1 - p^{-1} + p^{-p^n+n} - (p^{-1}-p^{-p^n})\\
&\quad /(p-1) - (p-1)\sum_{r=1}^{n-1} p^{-p^r+r}
\end{aligned}
$$

证毕

定理1的证明方法也可以用来计算 $\boldsymbol{F}_p$ 上 p^n -周期序列的任意 k -错线性复杂度，但结果相当复杂。

参 考 文 献

[1] Ding C, Xiao G, and Shan W, *et al.*. The Stability Theory of Stream Ciphers, Lecture Notes in Computer Science. Springer-Verlag, Berlin, 1991, Vol. 561, Chap 5.

[2] Stamp M and Martin C F, *et al.*. An algorithm for the k–error linear complexity of binary sequences with period 2^n. *IEEE Trans. on Inform. Theory*, 1993, IT–39(4): 1398–1401.

[3] Aly H and Winterhof A, *et al.*. On the k–error linear complexity over. $\boldsymbol{F}_p$ of legendre and sidelnikov sequences. Designs. *Codes and Cryptography*, 2006, 40(3): 369–374.

[4] Eun Y, Song H, and Kyureghyan G M, *et al.*. One–error linear complexity over $\boldsymbol{F}_p$ of sidelnikov sequences. Sequences and their Applications–SETA 2004, Lecture Notes in Computer Sciences, 2005, 3486: 154–165.

[5] Meidl W. On the stability of 2^n–periodic binary sequences. *IEEE Trans. Inform. Theory*, 2005, IT–51(3): 1151–1155.

[6] Meidl W and Niederreiter H, *et al.*. On the expected value of linear complexity and the k–error linear complexity of periodic sequences. *IEEE Trans. on Inform. Theory*, 2002, IT–48(11): 2817–2825.

[7] Meidl W and Niederreiter H. Linear complexity, k–error linear complexity and the descrete fourier transform. *Journal of Complexity*, 2002, 18(1): 87–103.

[8] Kaida T, Uehara S, and Imamura K, *et al.*. On the profile of the k–error linear complexity and the zero sum property for sequences over GF(p^m) with period p^n. Sequences and their Applications'01, Bergen, Norway, 2001: 13–17.

[9] Zhu fengxiang and Qi wenfeng. The 2–error linear complexity of 2^n –Periodic Binary Sequences with linear complexity 2^n-1. *Journal of Electronics* (*China*), 2007, 24(3): 390–395.

[10] Kurosaa K, Sato F, Sakata T, and Kishimoto W, *et al.*. A relationship between linear complexity and k–error linear complexity. *IEEE Trans. on Inform. Theory*, 2002, IT–46(2): 694–698.

[11] Kaida T, Uehara S and Imamura K, *et al.*. An algorithm for the k–error linear complexity of sequences over GF(p^m) with period p^n, p a prime. *Information and Computation*, 1999, 151(2): 134–147.

朱凤翔：　女，1977年生，博士生，研究方向为密码学.

戚文峰：　男，1963年生，教授，研究方向为信息安全、密码学.