随机周期序列 k 错线性复杂度的方差估计

苏 明, 符方伟
(南开大学 数学学院, 天津 300071)

摘 要: 周期序列的 k 错线性复杂度是衡量流密码系统的安全性能的一个重要指标. 本文首次给出了随机周期序列 k 错线性复杂度方差的一个表达公式, 同时给出了一些情形下的随机周期序列 k 错线性复杂度方差的上下界的估计和特定情形下的精确结果.

关键词: 流密码系统; 周期序列; 错线性复杂度; 期望; 方差
中图分类号: TN918. 1 文献标识码: A 文章编号: 0372-2112 (2005) 02-0279-05

The Estimated Bounds for the Variance of k-Error Linear Complexity of Random Periodic Sequences

SU Ming, FU Fang-wei
(Department of Mathematics, Nankai University, Tianjin 300071, China)

Abstract: The k-error linear complexity of periodic sequences is one of the important security indices of stream cipher systems. A general computation formula for the variance of the k-error linear complexity of random periodic sequences is given. Some upper bounds, lower bounds for the variance of the k- error linear complexity of random periodic sequences with certain periods are obtained. Furthermore, the exact value of the variance of the k-error linear complexity of a specific random periodic sequence is determined.

Key words: stream cipher systems; periodic sequences; k-error linear complexity; expectation; variance

1 引言

一个好的密码序列不仅应该有大的线性复杂度, 而且应该有很好的稳定性, 即使序列中出现几个错误, 也不会很大的降低线性复杂度, 根据这一点, 丁存生和肖国镇在/流密码学及其应用0一书中提出了 k 错线性复杂度这一概念, 国外学者 Stamp 和 Martin 在文献[1]中也提出了这一概念. 设 $S=(s_0, s_1, \cdots, s_{N-1})^{\infty}$ 是有限域 F_q 上周期为 N 的序列, 当改变 S 的周期中至多 k 位后, 这样得到的序列的线性复杂度中最小的线性复杂度, 称为序列 S 的 k 错复杂度, 记为 $L_{N,k}(S)$, 也就是

$$L_{N,k}(s)=\min_{X_H(T)\leqslant k}\{c(S+T)\}$$

这里 T 是周期为 N 的序列, $X_H(T)$ 表示 T 的一个周期中不为 0 的元素的个数, $c(S)$ 表示序列 S 的线性复杂度. 为了研究随机周期序列的 k 错线性复杂度, 文献[2]引入如下的定义, $N_{N,k}(c)$, 也就是周期为 N 的序列, 元素在 F_q 中, k 错线性复杂度为 c 的序列的个数. $M_{N,k}(c)=\sum_{r=0}^{c}N_{N,k}(r)$, 也就是 k 错线性复杂度小于或等于 c 的周期序列的个数. 利用这些定义, Meidl 和 Niederreiter[3] 得出了随机周期序列 k 错线性复杂度期望的表达公式和一些精确的估计结果. 为了更深入了解随机周期序列 k 错线性复杂度的整体分布情况, 还需要知道随机周期序列 k 错线性复杂度的方差. 本文采用类似的方法, 给出了随机周期序列 k 错线性复杂度的方差的一个表达公式. 并且给出了随机周期序列 k 错线性复杂度的方差的界的估计. 此外, 还得到了特定情形下随机周期序列 k 错线性复杂度的方差的精确结果.

这里给出的不同周期下的随机周期序列 k 错线性复杂度方差的上下界, 这些界的结果只依赖于周期序列最本质的一些与周期 N, 错误 k 相关的参数. 如果用普通的算法去实现来寻找周期序列分布的规律, 当周期大一些的时候计算复杂度, 需要的存储空间是非常大的, 甚至是不可以实现的; 但是通过本文计算给出的结果, 再结合已经有的关于随机周期序列 k 错线性复杂度期望的一些界的结果, 就可以很快预测出随机周期序列 k 错线性复杂度的大致分布情况, 是认识其分布的有力工具. 这是容易通过编程实现的, 因为本文给出的公式中都近似是关于周期 N 的二次多项式, 可以用这些界的结果来拟合分布.

这篇文章里, 潜在的统计假设是 N 周期的序列分布是均匀的.

2 k 错线性复杂度方差的估计

本节将给出随机周期序列 k 错线性复杂度的方差的一些估计.

这里 $E_{N,k}(c)$ 定义的是周期为 N 的随机周期序列 k 错线性复杂度的期望; $E_{N,k}(c^2)$ 定义的是周期为 N 的随机周期序列 k 错线性复杂度平方的期望; $V_{N,k}$ 定义的是周期为 N 的随机周期序列 k 错线性复杂度的方差.

收稿日期: 2003-09-26; 修回日期: 2004-10-03
基金项目: 国家自然科学基金(No. 60172060); 教育部跨世纪优秀人才培养计划基金和资助高等学校骨干教师计划基金

首先将给出随机周期序列 k 错线性复杂度的方差 $V_{N,k}$ 的一个表达公式, 然后通过文献[3]中 $N_{N,k}(c)$, $M_{N,k}(c)$ 的一些结果, 给出了一些特定周期下随机周期序列 k 错线性复杂度的方差的界. 还得到了特殊情形下, $V_{N,k}$ 的精确结果. 下面先介绍文献[3]中的一些结果.

引理 1 对于整数 $N\geq 1, 0\leq k\leq N$, 就有

$$M_{N,k}(c)\leq \min\left(q^N, M_{N,0}(c)\sum_{t=0}^{k}\binom{N}{t}(q-1)^t\right)$$

引理 2 设 $N=p^v n$, n 是素数, 而且 q 是有限域 F_n 中的本原元, 如果 $p^v<n-1$, 那么

$$M_{N,0}(c)=q^c, \quad \text{对于所有的 } c\leq p^v,$$

$M_{N,0}(r(n-1)+s)=q^{(n-1)(r-1)}(q^{p^v}+q^s(q^{n-1}-1))$, 对所有的 $1\leq r\leq p^v$, $0\leq s\leq p^v$,

对于 $c=r(n-1)+s$, $0\leq r\leq p^v$, $p^v\leq s\leq n-1$, $N_{N,k}(c)=0$, 因此, $M_{N,k}(c)=M_{N,k}(r(n-1)+p^v)$.

下面将给出随机周期序列 k 错线性复杂度方差的一个表达公式.

定理 1 对于整数 $N\geq 1, 0\leq k\leq N$, 那么周期为 N 的随机周期序列 k 错线性复杂度方差有以下表示:

$$V_{N,k}=\frac{(2N-1)^2}{4}-\left(\frac{1}{q^N}\sum_{c=0}^{N-1}M_{N,k}(c)-\frac{2N-1}{2}\right)^2-\frac{2}{q^N}\sum_{c=0}^{N-1}cM_{N,k}(c)$$

证明:

$$\begin{aligned}q^N E_{N,k}(c^2)&=\sum_{c=0}^{N}c^2N_{N,k}(c)\\&=\sum_{c=0}^{N}c^2(M_{N,k}(c)-M_{N,k}(c-1))\\&=\sum_{c=0}^{N}c^2M_{N,k}(c)-\sum_{c=0}^{N-1}(c+1)^2M_{N,k}(c)\\&=N^2q^N-\sum_{c=0}^{N-1}(1+2c)M_{N,k}(c)\\&=N^2q^N-\sum_{c=0}^{N-1}M_{N,k}(c)-2\sum_{c=0}^{N-1}cM_{N,k}(c)\end{aligned}$$

又从文献[3]中可知

$$E_{N,k}(c)=N-\frac{1}{q^N}\sum_{c=0}^{N-1}M_{N,k}(c)$$

$$\begin{aligned}V_{N,k}&=E_{N,k}(c^2)-(E_{N,k}(c))^2\\&=\frac{2N-1}{q^N}\sum_{c=0}^{N-1}M_{N,k}(c)-\frac{1}{q^{2N}}\left(\sum_{c=0}^{N-1}M_{N,k}(c)\right)^2\\&\quad-\frac{2}{q^N}\sum_{c=0}^{N-1}cM_{N,k}(c)\end{aligned}$$

配方以后可得上面结果.

从上可以知道

$$V_{N,k}=\frac{(2N-1)^2}{4}-(E_{N,k}(c)-\frac{1}{2})^2-\frac{2}{q^N}\sum_{c=0}^{N-1}cM_{N,k}(c)$$

为了对 $V_{N,k}$ 有更好的估计, 将引用文献[4], 命题 1, 从而得到关于 $E_{N,k}(c)$ 上界的一些结果.

引理 3 设 F_q 的特征为 p, $N=p^v n$, 设正整数 m, k 满足 $1\leq m\leq p^r$, $m\mid C_i$ $\leq k\leq N$, 其中 C_i 是 F_q 上模 n 的一个分圆陪集, $1\leq i\leq h$. 整数 $0\leq r\leq v$. 那么定义在 F_q 上的 N 周期序列的 k 错线性复杂度满足

$$L_{N,k}(S)\geq N-m\mid C_i\mid .$$

从引理 3 可以得到如下的结果.

引理 4 设 $N=p^v$, $0\leq k\leq N-1$, 那么 $E_{N,k}(c)\leq N-k$.

证明 此时 $h=1$, $C_1=\{0\}$, 从引理 3 可以知道, $L_{N,k}\geq N-k$, 又存在序列 S 使得 $L_{N,k}(S)=0$. 因此 $E_{N,k}(c)\leq N-k$, 可得结论. □

引理 5 设 $N=p^v n$, n 是素数, 而且 q 是有限域 F_n 中的本原元, 其中 $p^v<n-1$, 那么 $E_{N,k}(c)\leq N-S_{N,k}$, 其中

$$S_{N,k}=k, \quad \text{如果 } k\leq p^v$$

$$S_{N,k}=p^v, \quad \text{如果 } p^v\leq k\leq n-1$$

$$S_{N,k}=(n-1)\lfloor\frac{k}{n-1}\rfloor, \text{ 如果 } n-1\leq k\leq p^v(n-1)$$

$$S_{N,k}=p^v(n-1), \text{ 如果 } k\geq p^v(n-1)$$

证明 此时, 只有 $C_1=\{0\}$, $C_2=\{1, \cdots, n-1\}$ 两个分圆陪集, 从引理 3 就有对 k 的分段讨论, 可得结论. □

定理 2 设有限域 F_q 的特征为 p, $N=p^v$, $1\leq k\leq N-1$, 则 F_q 上 N 周期随机周期序列的 k 错线性复杂度的方差满足

$$V_{N,k}\geq -N^2+(2k+1)N+K(K+1)-k(k+1)-\frac{8}{q^N}$$
$$\geq\frac{2Kq^{K+2}-(2K+2)q^{K+1}+2q}{(q-1)^2}.$$

同时, k 错线性复杂度的方差还满足

(1) 如果 $N-\log_q\left(\sum_{t=0}^{k}\binom{N}{t}(q-1)^t\right)-\frac{q}{q-1}\leq\frac{1}{2}$

$$V_{N,k}\leq N^2-\frac{q+1}{q-1}N+\frac{1}{4}-\frac{2}{q^N}\frac{q}{(q-1)^2}+\frac{2q}{(q-1)^2}.$$

(2) 如果 $N-\log_q\left(\sum_{t=0}^{k}\binom{N}{t}(q-1)^t\right)-\frac{q}{q-1}\geq\frac{1}{2}$, ($8\geq q^{N-2}$, $q\neq 2$ 满足条件)

$$V_{N,k}\leq(2\log_q 8+2)N-\log_q^2 8-\frac{3q-1}{q-1}\log_q 8-\frac{2}{q^N}$$
$$\geq\frac{q}{(q-1)^2}.+\frac{-2q^2+3q}{(q-1)^2}$$

其中

$$8:=\sum_{t=0}^{k}\binom{N}{t}(q-1)^t$$

$$K=\lfloor N-\log_q\left(\sum_{t=0}^{k}\binom{N}{t}(q-1)^t\right)\rfloor 8.$$

证明 设 $q^c\sum_{t=0}^{k}\binom{N}{t}(q-1)^t<q^N$ 当仅当 $c\leq K:=\lfloor N-\log_q\left(\sum_{t=0}^{k}\binom{N}{t}(q-1)^t\right)\rfloor 8$. 文献[3](P. 2823)中给出了 $M_{N,0}(c)=q^c$, $c\leq p^v$, 根据引理 1, 就有

$$\begin{aligned}\sum_{c=0}^{N-1}cM_{N,k}(c)&\geq\left[\sum_{c=K+1}^{N-1}cq^N+\sum_{c=0}^{K}cq^c\right]\sum_{t=0}^{k}\binom{N}{t}(q-1)^t\\&=q^N\frac{(N-K-1)(N+K)}{2}\\&\quad+\sum_{t=0}^{k}\binom{N}{t}(q-1)^t\sum_{c=0}^{K}cq^c\end{aligned}$$

又

$$\sum_{c=0}^{K}cq^c=\frac{q-(K+1)q^{K+1}+Kq^{K+2}}{(q-1)^2}$$

于是

$$\sum_{c=0}^{N-1} cM_{N,k}(c)[\ q^N\#\frac{(N-K-1)(N+K)}{2}+\sum_{t=0}^{k}\binom{N}{t}(q-1)^t \#\frac{q-(K+1)q^{K+1}+Kq^{K+2}}{(q-1)^2}$$

根据引理4, 可以得到 $E_{N,k}< N-k, 0[\ k[\ N-1$. 又 $N-k\backslash 1$, 可得

$$V_{N,k}>\frac{(2N-1)^2}{4}-(N-k-\frac{1}{2})^2-\frac{2}{q^N}\sum_{c=0}^{N-1}cM_{N,k}(c)$$

$$\backslash k(2N-k-1)-(N-K-1)(N+K)-\frac{2}{q^N}$$

$$\#8\#\frac{q-(K+1)q^{K+1}+Kq^{K+2}}{(q-1)^2}$$

$$=-N^2+(2k+1)N+K(K+1)-k(k+1)-\frac{8}{q^N}$$

$$\#\frac{2Kq^{K+2}-(2K+2)q^{K+1}+2q}{(q-1)^2}$$

其中

$$8:=\sum_{t=0}^{k}\binom{N}{t}(q-1)^t$$

$$N-\log_q 8-1<K:=\tilde{o}N-\log_q\left(\sum_{t=0}^{k}\binom{N}{t}(q-1)^t\right)8[\ N-\log_q 8.$$

此外, 从文献[3]定理 6 中, 给出了 $E_{N,k}(c)$ 的一个下界

$$E_{N,k}\backslash N-\log_q\left(\sum_{t=0}^{k}\binom{N}{t}(q-1)^t\right)-\frac{q}{q-1}.$$

此外, 容易知道 $M_{N,k}(c)>M_{N,0}(c)$, 于是有下面的结论:

(1) 如果 $N-\log_q\left(\sum_{t=0}^{k}\binom{N}{t}(q-1)^t\right)-\frac{q}{q-1}<\frac{1}{2}$, 就有

$$V_{N,k}<\frac{(2N-1)^2}{4}-\frac{2}{q^N}\sum_{c=0}^{N-1}cM_{N,0}(c)$$

$$=\frac{(2N-1)^2}{4}-\frac{2}{q^N}\sum_{c=0}^{N-1}cq^c$$

$$=\frac{(2N-1)^2}{4}-\frac{2}{q^N}\#\frac{q-Nq^N+(N-1)q^{N+1}}{(q-1)^2}$$

$$=N^2-\frac{q+1}{q-1}N+\frac{1}{4}-\frac{2}{q^N}\frac{q}{(q-1)^2}+\frac{2q}{(q-1)^2}$$

(2) 如果 $N-\log_q\left(\sum_{t=0}^{k}\binom{N}{t}(q-1)^t\right)-\frac{q}{q-1}\backslash\frac{1}{2}$, ($8[\ q^{N-2}$, $q\mathrm{X}2$ 满足条件), 就有

$$V_{N,k}<\frac{(2N-1)^2}{4}-(N-\log_q 8-\frac{q}{q-1}-\frac{1}{2})^2-\frac{2}{q^N}\sum_{c=0}^{N-1}cM_{N,0}(c)$$

$$=(\log_q 8+\frac{q}{q-1})(2N-\log_q 8-\frac{q}{q-1}-1)-\frac{2}{q^N}$$

$$\#\frac{q-Nq^N+(N-1)q^{N+1}}{(q-1)^2}$$

$$=(2\log_q 8+2)N-\log_q^2 8-\frac{3q-1}{q-1}\log_q 8-\frac{2}{q^N}\#\frac{q}{(q-1)^2}$$

$$+\frac{-2q^2+3q}{(q-1)^2}$$

下面将根据引理 2, 得出在此情形下随机周期序列 k 错线性复杂度方差更精细的表达式.

定理 3　设 $N=p^v n$, n 是素数, 而且 q 是有限域 F_n 中的本原元, 其中 $p^v< n-1$, 那么 F_q 上 N 周期随机周期序列 k 错线性复杂度的方差

$$V_{N,k}=\frac{(2N-1)^2}{4}-\left[\frac{1}{q^N}\left((n-1-p^v)\sum_{r=0}^{p^v-1}M_{N,k}(r(n-1)+p^v)\right.\right.$$

$$\left.\left.+\sum_{s=0}^{p^v-1}\sum_{r=0}^{p^v}M_{N,k}(r(n-1)+s)\right)-\frac{2N-1}{2}\right]^2-\frac{2}{q^N}$$

$$\left\{\sum_{r=0}^{p^v-1}M_{N,k}(r(n-1)+p^v)\right.$$

$$\#\left((n-1-p^v)r(n-1)+\frac{(n-1-p^v)(n-2+p^v)}{2}\right)$$

$$\left.-\sum_{s=0}^{p^v-1}\sum_{r=0}^{p^v}M_{N,k}(r(n-1)+s)\#(r(n-1)+s)\right\}$$

证明　根据引理 2 和定理 1, 代入既得到结果.

定理 4　设 $N=p^v n$, n 是素数, 而且 q 是有限域 F_n 中的本原元, 其中 $p^v< n-1$.

设 K, J 是非负整数满足

$$M_{N,0}(r(n-1)+s)\sum_{t=0}^{k}\binom{N}{t}(q-1)^t<q^N$$

当仅当 $r(n-1)+s[\ K(n-1)+J$ 成立. 那么 F_q 上 N 周期随机周期序列 k 错线性复杂度的方差满足

情形 1: $K\backslash 1$, $J=p^v$

$$V_{N,k}>(2S_{N,k}+1)N-N^2-S_{N,k}(S_{N,k}+1)-(n-1)(1+K)$$

$$+(n-1)^2(1+K)^2-\frac{8}{q^N}\#g(K,p^v,n)$$

情形 2: $K\backslash 1$, $J<p^v$

$$V_{N,k}>(2S_{N,k}+1)N-N^2-S_{N,k}(S_{N,k}+1)-K(n-1)+K^2(n-1)^2+(J+1)(2Kn-2K+J)-\frac{8}{q^N}\#g_c(K,k,p^v,n)$$

情形 3: $K=0$, $J=p^v$

$$V_{N,k}>(2S_{N,k}+1)N-N^2-S_{N,k}(S_{N,k}+1)+(n-1)(n-2)-\frac{8}{q^N}$$

$$\left\{q^{p^v}(n-1-p^v)(n-2+p^v)+\frac{(2p^v-2)q^{p^v+1}-2p^vq^{p^v}+2q}{(q-1)^2}\right\}$$

情形 4: $K=0$, $k<p^v$

$$V_{N,k}>(2S_{N,k}+1)N-N^2-S_{N,k}(S_{N,k}+1)+J^2$$

$$+J-\frac{8}{q^N}\#\frac{2Jq^{J+2}-(2J+2)q^{J+1}+2q}{(q-1)^2}$$

其中 $S_{N,k}$ 满足

$$S_{N,k}=k,\quad \text{如果 } k[\ p^v$$

$$S_{N,k}=p^v,\quad \text{如果 } p^v<k<n-1$$

$$S_{N,k}=(n-1)\#\tilde{o}\frac{k}{n-1}8,\quad \text{如果 } n-1[\ k<p^v(n-1)$$

$$S_{N,k}=p^v(n-1),\quad \text{如果 } k\backslash p^v(n-1)$$

此外, k 错线性复杂度的方差还满足

$$V_{N,k}<V_{N,0}+(E_{N,0}(c)-\frac{1}{2})^2-(E_{N,k}(c)-\frac{1}{2})^2$$

$$[\ V_{N,0}+(E_{N,0}(c)-\frac{1}{2})^2$$

其中

$$V_{N,0}=\frac{(2p^v+1)(q^{-p^v}-q^{-p^{v+1}})-q^{-2p^v}+q}{(q-1)^2}+(n-1)^2$$
$$\#\frac{(2p^v+1)(q^{-p^v(n-1)}-q^{(-p^{v+1})(n-1)})-q^{-2p^v(n-1)}+q^{n-1}}{(q^{n-1}-1)^2}$$
$$E_{N,0}(c)=N-\frac{1}{q-1}\left(1-\frac{1}{q^{p^v}}\right)-\frac{n-1}{q^{n-1}-1}\left(1-\frac{1}{q^{(n-1)p^v}}\right).$$

证明

$$V_{N,k}=\left(N-\frac{1}{2}\right)^2-\left(E_{N,k}(c)-\frac{1}{2}\right)^2-\frac{2}{q^N}\sum_{c=0}^{N-1}cM_{N,k}(c)$$
$$=\left(N-\frac{1}{2}\right)^2-\left(E_{N,k}(c)-\frac{1}{2}\right)^2-\frac{2}{q^N}\left[\sum_{r=0}^{p^v-1}M_{N,k}(r(n-1)+p^v)\#f(r)+\sum_{s=0}^{p^v-1}\sum_{r=0}^{p^v}M_{N,k}(r(n-1)+s)\#(r(n-1)+s)\right]$$

其中

$$f(r)=(n-1-p^v)r(n-1)+\frac{(n-1-p^v)(n-2+p^v)}{2}$$

根据引理 5, 可以知道 $E_{N,k}(c)<N-S_{N,k}.N-S_{N,k}>1$. 假设

$$M_{N,0}(r(n-1)+s)\sum_{t=0}^{k}\binom{N}{t}(q-1)^t<q^N$$

当仅当 $r(n-1)+s[K(n-1)+J$ 成立. 于是就有关于 $V_{N,k}$ 下界的结果.

情形 1: $K\geqslant 1, J=p^v$

$$V_{N,k}>S_{N,k}(2N-S_{N,k}-1)-\frac{2}{q^N}\left\{q^{p^v}\#\frac{(n-1-p^v)(n-2+p^v)}{2}\right.$$
$$+\sum_{r=1}^{K}q^{r(n-1)+p^v}f(r)\#\,8+\sum_{r=K-1}^{p^v-1}f(r)q^N+\sum_{s=0}^{p^v-1}q^s\,8$$
$$+\sum_{s=0}^{p^v-1}\sum_{r=1}^{K}q^{(n-1)(r-1)}\#(q^{p^v}+q^s(q^{n-1}-1))$$
$$\left.\#(r(n-1)+s)\,8+\sum_{s=0}^{p^v-1}\sum_{r=K-1}^{p^v}(r(n-1)+s)q^N\right\}$$
$$=2S_{N,k}N-S_{N,k}(S_{N,k}+1)-\frac{2}{q^N}\left\{\sum_{r=K-1}^{p^v-1}f(r)\,q^N\right.$$
$$\left.+\sum_{s=0}^{p^v-1}\sum_{r=K-1}^{p^v}(r(n-1)+s)q^N\right\}-\frac{2}{q^N}8$$
$$\#\left\{q^{p^v}\#\frac{(n-1-p^v)(n-2+p^v)}{2}+\sum_{r=1}^{K}q^{r(n-1)+p^v}f(r)\right.$$
$$\left.+\sum_{s=0}^{p^v-1}q^s+\sum_{s=0}^{p^v-1}\sum_{r=1}^{K}q^{(n-1)(r-1)}\#(q^{p^v}+q^s(q^{n-1}-1))\#(r(n-1)+s)\right\}$$
$$=2S_{N,k}N-S_{N,k}(S_{N,k}+1)-\{n^2p^{2v}-np^v+(n-1)(1+K)$$
$$-(n-1)^2(1+K)^2\}-\frac{8}{q^N}\#g(K,p^v,n)$$
$$=(2S_{N,k}+1)N-N^2-S_{N,k}(S_{N,k}+1)-(n-1)(1+K)$$
$$+(n-1)^2(1+K)^2-\frac{8}{q^N}\#g(K,p^v,n)$$

情形 2: $K\geqslant 1, J<p^v$

$$V_{N,k}>S_{N,k}(2N-S_{N,k}-1)-\frac{2}{q^N}\left\{q^{p^v}\#\frac{(n-1-p^v)(n-2+p^v)}{2}8\right.$$
$$+\sum_{r=1}^{K-1}q^{r(n-1)+p^v}f(r)\#\,8+\sum_{r=K}^{p^v-1}q^Nf(r)+\sum_{s=0}^{p^v-1}q^s\,8$$
$$+\sum_{s=0}^{p^v-1}\sum_{r=1}^{K-1}q^{(n-1)(r-1)}\#(q^{p^v}+q^s(q^{n-1}-1))$$
$$\#(r(n-1)+s)\#\,8+\sum_{s=0}^{p^v-1}\sum_{r=K-1}^{p^v}q^N(r(n-1)+s)$$
$$+\sum_{s=0}^{J}q^{(n-1)(K-1)}(q^{p^v}+q^s(q^{n-1}-1))\,8\#(K(n-1)+s)$$
$$\left.+\sum_{s=K-1}^{p^v-1}q^N\#(K(n-1)+s)\right\}$$
$$=2S_{N,k}N-S_{N,k}(S_{N,k}+1)-\{n^2p^{2v}-np^v+K(n-1)$$
$$-K^2(n-1)^2-(J+1)(2Kn-2K+J)$$
$$\left.-\frac{8}{q^N}\#g(K,J,p^v,n)\right\}$$
$$=(2S_{N,k}+1)N-N^2-S_{N,k}(S_{N,k}+1)-K(n-1)$$
$$+K^2(n-1)^2+(J+1)(2Kn-2K+J)$$
$$-\frac{8}{q^N}\#g(K,J,p^v,n)$$

情形 3: $K=0, J=p^v$

$$V_{N,k}>S_{N,k}(2N-S_{N,k}-1)-\frac{2}{q^N}\left\{q^{p^v}\#\frac{(n-1-p^v)(n-2-p^v)}{2}\#\,8\right.$$
$$+\sum_{r=1}^{p^v-1}q^Nf(r)+\sum_{s=0}^{p^v-1}\sum_{r=1}^{p^v}q^N\#(r(n-1)+s)+\sum_{s=0}^{p^v-1}q^s\#\,8\Big\}$$
$$=2S_{N,k}N-S_{N,k}(S_{N,k}+1)-\frac{2}{q^N}$$
$$\left\{q^{p^v}\#\frac{(n-1-p^v)(n-2-p^v)}{2}\#\,8+q^N\#\sum_{r=1}^{p^v-1}\left[(n-1-p^v)r(n-1)+\frac{(n-1-p^v)(n-2-p^v)}{2}\right]\right.$$
$$+q^N\left[(n-1)\frac{p^v(p^v-1)}{2}\#p^v+\frac{p^{2v}(p^v-1)}{2}\right]$$
$$\left.+\,8\#\frac{q-p^vq^{p^v}+(p^v-1)q^{p^v+1}}{(q-1)^2}\right\}$$
$$=2S_{N,k}N-S_{N,k}(S_{N,k}+1)-\{n^2p^{2v}-np^v$$
$$-(n-1)(n-2)\}-\frac{8}{q^N}\{q^{p^v}(n-1-p^v)(n-2+p^v)$$
$$\left.+2\#\frac{q-p^vq^{p^v}+(p^v-1)q^{p^v+1}}{(q-1)^2}\right\}$$
$$=(2S_{N,k}+1)N-N^2-S_{N,k}(S_{N,k}+1)+(n-1)(n-2)$$
$$-\frac{8}{q^N}\{q^{p^v}(n-1-p^v)(n-2+p^v)$$
$$\left.+\frac{(2p^v-2)q^{p^v+1}-2p^vq^{p^v}+2q}{(q-1)^2}\right\}$$

情形 4: $K=0, k<p^v$

$$V_{N,k}>S_{N,k}(2N-S_{N,k}-1)-\frac{2}{q^N}\left\{\sum_{r=0}^{p^v-1}q^Nf(r)\right.$$
$$\left.+\sum_{s=0}^{p^v-1}\sum_{r=1}^{p^v}q^N\#(r(n-1)+s)+\sum_{s=0}^{J}q^s\#\,8+\sum_{s=J+1}^{p^v-1}q^Ns\right\}$$

$$= 2S_{N,k}N - S_{N,k}(S_{N,k}+1) - \frac{2}{q^N}\left\{ q^N \# \sum_{r=0}^{p^v-1} [(n - 1 - p^v)r(n-1) + \frac{(n-1-p^v)(n-2+p^v)}{2}] + q^N \sum_{s=0}^{p^v-1}\sum_{r=1}^{p^v}(r(n-1)+s) + 8 \# \sum_{s=0}^{J} q^s + q^N \# \frac{(p^v-1-J)(p^v+J)}{2}\right\}$$

$$= 2S_{N,k}N - S_{N,k}(S_{N,k}+1) - \{n^2p^{2v} - np^v - J^2 + J\} - \frac{28}{q^N} \# \frac{q-(J+1)q^{J+1}+J\#q^{J+2}}{(q-1)^2}$$

$$= (2S_{N,k}+1)N - N^2 - S_{N,k}(S_{N,k}+1) + J^2 + k - \frac{8}{q^N} \# \frac{2Jq^{J+2} - (2J+2)q^{J+1} + 2q}{(q-1)^2}.$$

下面将对随机周期序列 k 错线性复杂度方差的上界进行估计. 易见 $M_{N,k}(c) > M_{N,0}(c)$, 就有

$$V_{N,k} < \frac{(2N-1)^2}{4} - \frac{2}{q^N}\sum_{c=0}^{N-1} cM_{N,0}(c) - (E_{N,k}(c) - \frac{1}{2})^2$$

$$= \frac{(2N-1)^2}{4} + V_{N,0} - \frac{(2N-1)^2}{4} + (E_{N,0}(c) - \frac{1}{2})^2 - (E_{N,k}(c) - \frac{1}{2})^2$$

$$= V_{N,0} + (E_{N,0}(c) - \frac{1}{2})^2 - (E_{N,k}(c) - \frac{1}{2})^2$$

文献[3]中给出了 $E_{N,k}$ 下界的一些结果(P. 2824), 利用这个结果可以得到 $V_{N,k}$ 的界的估计.

如果 $E_{N,k}$ 下界小于 $\frac{1}{2}$, 就有

$$V_{N,k} < V_{N,0} + (E_{N,0}(c) - \frac{1}{2})^2$$

如果 $E_{N,k}$ 下界大于等于 $\frac{1}{2}$, 就有

$$V_{N,k} < V_{N,0} + (E_{N,0}(c) - \frac{1}{2})^2 - (E_{N,k}(c) - \frac{1}{2})^2$$

其中, 从文献[5]定理 6 中, 可以得到

$$V_{V,0} = \frac{(2p^v+1)(q - p^v - q^{-p^v+1}) - q^{-2p^v} + q}{(q-1)^2} + (n-1)^2 \# \frac{(2q^v+1)(q^{-p^v(n-1)} - q^{(-p^v+1)(n-1)}) - q^{-2p^v(n-1)} + q^{n-1}}{(q^{n-1}-1)^2}$$

从文献[3]中定理 5(P. 2821), 可以得到

$$E_{N,0}(c) = N - \frac{1}{q-1}(1 - \frac{1}{q^{p^v}}) - \frac{n-1}{q^{n-1}-1}(1 - \frac{1}{q^{(n-1)p^v}})$$

代入可得随机周期序列 k 错线性复杂度的方差的上界的估计结果.

下面将给出特殊情况下随机周期序列 k 错线性复杂度的方差.

定理 5　设 N 周期序列定义在 F_q 上, 满足 $N \setminus 3$ 是一个素数, N 不被 $q-1$ 整除, q 是 F_N 上的本原元, 对于 $1 \leqslant k \leqslant \frac{N-1}{2}$, 那么随机周期序列 k 错线性复杂度的方差为:

$$V_{N,k} = (qN^2 - (4q-2)N + 4q - 3) \# \frac{8}{q^N} - (qN - 2q + 1)^2 \# \frac{8^2}{q^{2N}}$$

其中

$$8 := \sum_{t=0}^{k} \binom{N}{t} (q-1)^t$$

证明　因为 q 是有限域 F_N 中的本原元, 那么线性复杂度只能是 0, 1, N-1, N, 容易知道 k 错线性复杂度不为 N.

由文献[2]知道错线性复杂度为 0 的序列一共有 $\sum_{t=0}^{k} \binom{N}{t} (q-1)^t$, k 错线性复杂度为 1 的序列一共有 $(q-1)\sum_{t=0}^{k} \binom{N}{t} (q-1)^t$, 余下的就是 k 错线性复杂度为 N-1 的序列, 一共有 $q^N - q\sum_{t=0}^{k} \binom{N}{t} (q-1)^t$. 设 $8 := \sum_{t=0}^{k} \binom{N}{t} (q-1)^t$, 那么

$$E_{N,k}(c) = (q-1) \# \frac{8}{q^N} + (N-1) \# \frac{q^N - q8}{q^N} = N - 1 - (qN - 2q + 1) \# \frac{8}{q^N}$$

可以知道

$$E_{N,k}(c^2) = \frac{1}{q^N}(q-1)8 + \frac{1}{q^N}(N-1)^2(q^N - q8)$$

又 $V_{N,k} = E_{N,k}(c^2) - (E_{N,k}(c))^2$, 代入化简即得结论.

参考文献:

[1] M Stamp, C F Martin. An algorithm for the k2error linear complexity of binary sequences with period 2^n[J]. IEEE Trans Information Theory, 1993, 39: 1398- 1401.

[2] W Meidl. Linear complexity, k2error linear complexity, and the discrete fourier transform[J]. J Complexity, 2002, 118: 87- 103.

[3] W Meidl, H Niederreiter. On the expected value of the linear complex2ity and the k2error linear complexity of periodic sequences[J]. IEEE Trans Information Theory, 2002, 48(11): 2817- 2825.

[4] H Niederreiter. Periodic sequences with large k2error linear complexity [J]. IEEE Trans Information Theory, 2003, 49: 501- 505.

作者简介:

苏　明　男, 1978 年 5 月生于湖北沙市, 1999 年获南开大学数学学院基础数学学士学位, 南开大学数学学院信息科学专业博士生, 主要研究兴趣为信息论, 编码理论, 密码学(序列复杂度, 数字水印). E2mail: suming@mail. nankai. edu. cn.

符方伟　男, 1963 年 10 月 28 日生, 博士, 现为南开大学数学科学学院教授, 博士生导师, 主要从事信息论, 编码理论和密码学的研究与教学工作, 在国际和国内重要学术期刊上发表一系列论文, 其中在5 IEEE Transactions on Information The2ory6 上发表论文 17 篇, 多次应邀访问香港和国外的大学与研究机构进行合作研究.