二元周期序列的 k 错误线性复杂度

赵耀东,戚文峰
(郑州信息工程大学信息工程学院应用数学系,郑州 450002)

摘 要: 随着 k 的增大,序列 k 错误线性复杂度的值会从线性复杂度递减到 0. 对于周期为 2 的方幂的二元序列,Kurosawa 讨论了线性复杂度和 k 错误线性复杂度的关系,给出了使得序列的 k 错误线性复杂度严格小于序列的线性复杂度最小的 k 值. 本文利用多项式的权重关系给出了使得序列 k 错误线性复杂度再次减小的最小 k 值.

关键词: 序列密码; 线性复杂度; k 错误线性复杂度
中图分类号: TN918. 1 **文献标识码**: A **文章编号**: 0372 - 2112 (2005) 01 - 0012 - 05

On the k-Error Linear Complexity of Binary Period Sequences

ZHAO Yao-dong, QI Wen-feng
(Department of Applied Mathematics, Zhengzhou Information Engineering University, Zhengzhou 450002, China)

Abstract: With the increase of k, the k-error linear complexity will decrease to 0 from the value of the linear complexity of the sequences. For the binary sequences whose period is a power of 2, a relationship between the linear complexity and k-error linear complexity is discussed by Kurosawa, which indicates the least value of the positive integer k such that the k-error linear complexity less than linear complexity. In this paper, using the Hamming weight of polynomials, the least k is given such that the k-error linear complexity decreased again.

Key words: stream cipher; linear complexity; k-error linear complexity

1 引言

在序列密码理论中,线性复杂度是一个重要的复杂度标准. 序列 $\underline{s}$ 的线性复杂度定义为产生序列 $\underline{s}$ 的最短线性移位寄存器(LFSR)的级数,记为 $LC(\underline{s})$. 若已知序列 $\underline{s}$ 的连续 $2LC(\underline{s})$ 比特,利用 Berlekamp - Massey 算法就可以恢复出整条序列 $\underline{s}$. 因此一条抗攻击强度大的密钥序列一定具有较高的线性复杂度. 但是具有高的线性复杂度并不能保证序列具有强的抗攻击强度. 例如:二元序列 $\underline{s} = (0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,1,\cdots)$ 具有等于周期的线性复杂度,即线性复杂度达到了最大. 但是当把它每周期第八个比特改为 0 时其线性复杂度立即就变为 0. 由这个例子可以看出若改变一条序列每个周期中的少量比特后该序列的线性复杂度下降得很剧烈,则可以用一条线性复杂度较低的序列来逼近线性复杂度较高的原序列. 很显然这样的序列是不能用来做密钥序列的. 为此,上世纪 90 年代人们提出了 k 错误线性复杂度[3]的概念(类似的有球体复杂度[4]).

设 $\underline{s} = (s_0, s_1, s_2, \cdots, s_{N-1}, s_0, \cdots)$ 是周期为 N 的二元序列,k 是一个非负整数. 定义序 $\underline{s}$ 的 k 错误线性复杂度为改变任意不多于 k 个 s_i 后所得到的最小的线性复杂度,记为 $LC_k(\underline{s})$. 对于周期整除 N 的二元周期序列 $\underline{e} = (e_0, e_1, \cdots, e_{N-1}, e_0, \cdots)$,记向量 $(e_0, e_1, \cdots, e_{N-1})$ 中"1"的个数为 $W_N(\underline{e})$,则有 $LC_k(\underline{s}) = \min_{W_N(\underline{e}) \le k} LC(\underline{s} + \underline{e})$,其中序列 $\underline{e}$ 跑遍所有周期整除 N 的二元序列.

注 设 $T = W_N(\underline{s})$,$\underline{s}$ 是周期为 N 的二元周期序列,则显然有 $LC(\underline{s}) = LC_0(\underline{s}) \ge LC_1(\underline{s}) \ge \cdots \ge LC_T(\underline{s})$

可以看出序列的 k 错误线性复杂度反映了序列线性复杂度的稳定性. 它描述了序列在改变几个比特后线性复杂度下降的情况. 对于抗攻击强度大的序列 $\underline{s}$,希望对于较小的 k,其 k 错误线性复杂度与线性复杂度相近,而只有对于较大的 k,其 k 错误线性复杂度才会与线性复杂度相差较大. 故研究随着 k 的增大,序列的线性复杂度何时下降是十分重要的.

设 $\underline{s}$ 是二元周期序列,记 $err_1(s)$ 为最小的 k 使得 $LC_k(\underline{s}) < LC(\underline{s})$. 同样,记 $err_2(s)$ 为最小的 t 使得 $LC_t(\underline{s}) < LC_{k_1}(\underline{s})$,其中 $k_1 = err_1(\underline{s})$. 对于周期为 2^n 的二元序列 $\underline{s}$,[1]刻划了 $err_1(\underline{s})$ 的值,即 $err_1(\underline{s}) = 2^{W_h(2^n - LC(s))}$,其中 $W_h(m)$ 表示非负整数 m 的二进制表示中"1"的个数. 对于某些序列 $\underline{s}$,$LC_k(s)$ $(k = err_1(\underline{s}))$ 与其线性复杂度十分接近,但是如果改变更多一点比特后其 k 错误线性复杂度下降得十分显著. 例如令

$\underline{s} = (0,0,1,0,0,1,0,1,0,1,0,1,0,1,0,1,0,0,1,0,0,1,0,0,1,0,1,0,1,0,1,0,1,\cdots)$.

收稿日期:2004 - 02 - 06;修回日期:2004 - 11 - 28
基金项目:全国优秀博士学位论文专项基金(No. 200060);国家自然科学基金(No. 60373092)

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

这条序列的线性复杂度为 16 且 $LC_k(\underline{s}) = 13$ 其中 $k = err_1(\underline{s}) = 1$. 但是若每周期多改变两个比特(第二个,三个,四个比特),其 k 错误线性复杂度立即降为 2. 显然这三个比特要更重要. 由此计算 $LC(\underline{s}) - LC_k(s)\ (k = err_1(\underline{s}))$ 以及最小的 t 使得 $LC_t(\underline{s}) < LC_k(\underline{s})$ 是十分有意义的. [1]给出了 $LC(\underline{s}) - LC_k(\underline{s})\ (k = err_1(\underline{s}))$ 的下界并将求 $err_2(\underline{s})$ 作为一个公开问题提了出来.

本文研究了周期序列的 $err_2(\underline{s})$ 和 $LC_{k_2}(\underline{s})$,其中 $k_2 = err_2(\underline{s})$,利用多项式的权重关系,对于一类周期为 2^n 的二元序列,给出了 $err_2(\underline{s})$ 及 $LC(\underline{s}) - LC_k(\underline{s})\ (k = \mathrm{err}_1(\underline{s}))$ 的精确值,并且给出了 $LC_{k_2}(\underline{s})$ 的紧的上界.

2　多项式的权重关系

设多项式 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F_2[x]$. $f(x)$ 的权重 $W(f(x))$ 为向量 $(a_0, a_1, \cdots, a_n)$ 中"1"的个数. 因为 $\{(1+x)^0, (1+x)^1, \cdots, (1+x)^{2^n-1}\}$ 也是向量空间 $\{f(x) \mid \deg(f(x)) < 2^n\}$ 的一组基,故对任意的 $f(x) \in_F 2[x]$,存在非负整数 $t_1, t_2, \cdots, t_n$ 使得 $f(x) = (1+x)^{t_1} + (1+x)^{t_2} + \cdots + (1+x)^{t_n}$ 其中 $t_1 < t_2 < \cdots < t_n$. [2]中研究了形如 $(1+x)^{t_1} + \cdots + (1+x)^{t_n}$ 的多项式其权重问题.

引理 1[2]　设 s 是非负整数,则 $W((1+x)^s) = 2^{W_h(s)}$.

引理 2[2]　设整数 $t_1, \cdots, t_n$ 满足 $0 \le t_1 \le \cdots \le t_n$,则 $W((1+x)^{t_1} + \cdots + (1+x)^{t_n}) \ge W((1+x)^{t_1})$.

引理 2 表明当 $0 \le t_1 < t_2 < \cdots < t_n$ 时,多项式 $(1+x)^{t_1} + (1+x)^{t_2} + \cdots + (1+x)^{t_n}$ 的权重总不小于多项式 $(1+x)^{t_1}$ 的权重. 为了研究周期为 2^n 的二元序列的 k 错误线性复杂度,需要讨论 $W((1+x)^{t_1} + (1+x)^{t_2} + \cdots + (1+x)^{t_n})$ 和 $W((1+x)^{t_1} + (1+x)^{t_2})$ 之间的关系.

引理 3(Lucas)[8]　对 $a_0, a_1, \cdots, a_n, b_0, \cdots, b_n \in \{0,1\}$ 有 $\binom{\sum_{i=0}^{n} a_i 2^i}{\sum_{i=0}^{n} b_i 2^i} \pmod 2 = 1$ 当且仅当 $b_i \le a_i$ 对所有的 i.

令 $a = a_m 2^m + a_{m-1}2^{m-1} + \cdots + a_0$ 并且 $b = b_m 2^m + b_{m-1}2^{m-1} + \cdots + b_0$ 为两个正整数,其中 $a_0, a_1, \cdots, a_m, b_0, \cdots, b_m \in \{0,1\}$. 定义 $a \wedge b = a_m b_m 2^m + a_{m-1} b_{m-1} 2^{m-1} + \cdots + a_0 b_0$. 为了得到本节的主要结论,许多引理需要给出. 这些引理的证明限于篇幅将不给出证明.

引理 4　令 t_1 和 t_2 均为非负整数. 若 $t_1 < t_2$,则有

$$W((1+x)^{t_1} + (1+x)^{t_2}) = 2^{W_h(t_1)} + 2^{W_h(t_2)} - 2^{W_h((t_1 \wedge t_2)+1)}.$$

引理 5　设 $f(x), g(x) \in F_2[x]$,则 $W(f(x)+g(x)) \le W(f(x)) + W(g(x))$. 进一步,若 $f(x)$ 的项在 $g(x)$ 中不出现,即若 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$, $a_i b_i = 0$ 则 $W(f(x)+g(x)) = W(f(x)) + W(g(x))$.

引理 6　若正整数 $t_1, t_2, \cdots, t_n$ 及 m 满足 $2^m \le t_1 < t_2 < \cdots < t_n < 2^{m+1}$,则

$$W((1+x)^{t_1} + (1+x)^{t_2} + \cdots + (1+x)^{t_n}) = 2W((1+x)^{t_1-2^m} + (1+x)^{t_2-2^m} + \cdots + (1+x)^{t_n-2^m}.$$

引理 7　若正整数 t 满足 $2^m + 2^{m-1} > t \ge 2^m$ 并设 $(1+x)^t = a_t x^t + a_{t-1}x^{t-1} + \cdots + a_0$,则

$$a_{2^{m-1}} = a_{2^{m-1}+1} = \cdots = a_{2^m-1} = 0.$$

引理 8　若对正整数 $t_1, t_2, \cdots, t_n$ 及 $m \ge 2$ 有 $2^{m-2} \le t_1 \le 2^{m-1} \le t_2 < \cdots < t_n$ 且 $t_i - 2^{m-1} \ge 2^{m-2}$, $i = 2, \cdots, n$,则有 $W((1+x)^{t_1} + (1+x)^{t_2} + \cdots + (1+x)^{t_n}) = 2W((1+x)^{t_1-2^{m-2}} + (1+x)^{t_2-2^{m-1}} + \cdots + (1+x)^{t_n-2^{m-1}})$.

引理 9　设正整数 $t_1, t_2, \cdots, t_n$ 及 $m \ge 2$ 满足 $2^{m-2} \le t_1 < 2^{m-1} \le t_2 < \cdots < t_n < 2^m$. 若存在正整数 $s, n \ge s > 2$ 使得 $t_{s-1} < 2^{m-1} + 2^{m-2} \le t_s$,则有 $W((1+x)^{t_1} + (1+x)^{t_2} + \cdots + (1+x)^{t_n}) \ge W((1+x)^{t_1} + (1+x)^{t_2} + \cdots + (1+x)^{t_{s-1}})$.

引理 10　若对正整数 $t_1, t_2, \cdots, t_n$ 及 $m \ge 2$ 有 $t_1 < 2^{m-1} \le t_2 < \cdots < t_n$, $t_1 < 2^{m-2}$ 且 $t_i - 2^{m-1} < 2^{m-2}$, $i = 2, \cdots, n$ 则有 $W((1+x)^{t_1} + (1+x)^{t_2} + \cdots + (1+x)^{t_n}) = W((1+x)^{t_1} + (1+x)^{t_2-2^{m-1}+2^{m-2}} + \cdots + (1+x)^{t_n-2^{m-1}+2^{m-2}})$.

引理 11　设正整数 $t_1, t_2, \cdots, t_n$ 及 m 满足 $t_1 < 2^{m-2}$,且 $2^{m-1} \le t_2 < t_3 < \cdots < t_{s-1} < 2^{m-2} + 2^{m-1} \le t_s < t_{s+1} < \cdots < t_n$,其中 $2 < s < n$, $m \ge 2$,则有 $W((1+x)^{t_1} + (1+x)^{t_2} + \cdots + (1+x)^{t_n}) = W((1+x)^{t_1} + (1+x)^{t_2-2^{m-1}+2^{m-2}} + \cdots + (1+x)^{t_{s-1}-2^{m-1}+2^{m-2}} + (1+x)^{t_s} + \cdots + (1+x)^{t_n})$.

引理 12　设 $n \ge 2, 0 \le t_1 < t_2 < \cdots < t_n < 4$,则 $W((1+x)^{t_1} + (1+x)^{t_2} + \cdots + (1+x)^{t_n}) \ge W((1+x)^{t_1} + (1+x)^{t_2})$.

下面给出本节的主要定理.

定理 1　设 $n \ge 2, 0 \le t_1 < t_2 < \cdots < t_n$,则在 F_2 上有 $W((1+x)^{t_1} + (1+x)^{t_2} + \cdots + (1+x)^{t_n}) \ge W((1+x)^{t_1} + (1+x)^{t_2})$.

证明　对 t_n 进行归纳. 引理 12 表明当 $t_n < 4 = 2^2$ 时结论成立. 现在假设当 $t_n < 2^{m-1}$ 时结论成立,则要证明当 $2^{m-1} \le t_n < 2^m$ 时结论成立. 证明将分三种情况讨论:

(Ⅰ) $t_1 < t_2 < 2^{m-1}$; (Ⅱ) $2^{m-1} \le t_1 < t_2$; (Ⅲ) $t_1 < 2^{m-1} \le t_2$.

情况(Ⅰ)　$t_1 < t_2 < 2^{m-1}$.

因为 $t_1 < t_2 < \cdots < t_n$ 并且 $2^{m-1} \le t_n < 2^m$,故存在 $s, 2 < s \le n$,使得 $t_{s-1} < 2^{m-1} \le t_s$. 于是

$$\begin{aligned}
&W((1+x)^{t_1} + (1+x)^{t_2} + \cdots + (1+x)^{t_n}) \\
&= W((1+x)^{t_1} + \cdots + (1+x)^{t_{s-1}} + (1+x)^{2^{m-1}}((1+x)^{t_s-2^{m-1}} + \cdots + (1+x)^{t_n-2^{m-1}})) \\
&= W((1+x)^{t_1} + \cdots + (1+x)^{t_{s-1}} + ((1+x)^{t_s-2^{m-1}} + \cdots + (1+x)^{t_n-2^{m-1}}) + x^{2^{m-1}}((1+x)^{t_s-2^{m-1}} + \cdots + (1+x)^{t_n-2^{m-1}})) \\
&= W((1+x)^{t_1} + \cdots + (1+x)^{t_{s-1}} + ((1+x)^{t_s-2^{m-1}} + \cdots + (1+x)^{t_n-2^{m-1}})) + W((1+x)^{t_s-2^{m-1}} + \cdots + (1+x)^{t_n-2^{m-1}}) \quad \text{(由引理 5)} \\
&\ge W((1+x)^{t_1} + (1+x)^{t_2} + \cdots + (1+x)^{t_{s-1}}) \quad \text{(由引理 5)}
\end{aligned}$$

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

因为 $s-1\geq 2$, $t_{s-1}<2^{m-1}$,由条件假设得

$$W((1+x)^{t_1}+(1+x)^{t_2}+\cdots+(1+x)^{t_{s-1}})\geq W((1+x)^{t_1}+(1+x)^{t_2}).$$

故结论在这种情况下成立.

情况(Ⅱ) $2^{m-1}\leq t_1<t_2$.由引理 6 得

$$W((1+x)^{t_1}+(1+x)^{t_2}+\cdots+(1+x)^{t_n})=2W((1+x)^{t_1-2^{m-1}}+(1+x)^{t_2-2^{m-1}}+\cdots+(1+x)^{t_n-2^{m-1}}).$$

由 $2^{m-1}\leq t_1<t_2<\cdots<t_n<2^m$ 和条件假设得

$$2W((1+x)^{t_1-2^{m-1}}+(1+x)^{t_2-2^{m-1}}+\cdots+(1+x)^{t_n-2^{m-1}})\geq 2W((1+x)^{t_1-2^{m-1}}+(1+x)^{t_2-2^{m-1}})\quad(\text{由条件假设})$$
$$=W((1+x)^{t_1}+(1+x)^{t_2})\quad(\text{由引理 6})$$

故结论在这种情况下成立.

情况(Ⅲ) $t_1<2^{m-1}\leq t_2$,即 $t_1<2^{m-1}\leq t_2<\cdots<t_n<2^m$.

为证明结论在情况(Ⅲ)下成立,需要再分三种子情况讨论:

(Ⅲ1) $t_i-2^{m-1}<2^{m-2}$, $i=2,\cdots,n$; (Ⅲ2) $t_i-2^{m-1}\geq 2^{m-2}$, $i=2,\cdots,n$; (Ⅲ3) 其他情况.

情况(Ⅲ1) $t_i-2^{m-1}<2^{m-2}$, $i=2,\cdots,n$.

先假设 $t_1<2^{m-2}$.由引理 10 得

$$W((1+x)^{t_1}+(1+x)^{t_2}+\cdots+(1+x)^{t_n})=W((1+x)^{t_1}+(1+x)^{t_2-2^{m-1}+2^{m-2}}+\cdots+(1+x)^{t_n-2^{m-1}+2^{m-2}}).$$

由 $0\leq t_1<2^{m-2}\leq t_2-2^{m-1}+2^{m-2}<\cdots<t_n-2^{m-1}+2^{m-2}<2^{m-1}$和条件假设得 $W((1+x)^{t_1}+(1+x)^{t_2-2^{m-1}+2^{m-2}}+\cdots+(1+x)^{t_n-2^{m-1}+2^{m-2}})\geq W((1+x)^{t_1}+(1+x)^{t_2-2^{m-1}+2^{m-2}})$(由条件假设)

$$=W((1+x)^{t_1}+(1+x)^{t_2})\quad(\text{由引理 10}).$$

再假设 $2^{m-2}\leq t_1<2^{m-1}$.

$$W((1+x)^{t_1}+(1+x)^{t_2}+\cdots+(1+x)^{t_n})=W((1+x)^{2^{m-2}}(1+x)^{t_1-2^{m-2}}+(1+x)^{t_2}+\cdots+(1+x)^{t_n})$$
$$=W((1+x)^{t_1-2^{m-2}}+x^{2^{m-2}}(1+x)^{t_1-2^{m-2}}+(1+x)^{t_2}+\cdots+(1+x)^{t_n})$$
$$=W((1+x)^{t_1-2^{m-2}}+(1+x)^{t_2}+\cdots+(1+x)^{t_n})+W(x^{2^{m-2}}(1+x)^{t_1-2^{m-2}})\quad(\text{由引理 5 和引理 7})$$

由 $t_1-2^{m-2}<2^{m-1}$和上面当 $t_1<2^{m-2}$时的讨论得

$$W((1+x)^{t_1-2^{m-2}}+(1+x)^{t_2}+\cdots+(1+x)^{t_n})\geq W((1+x)^{t_1-2^{m-2}}+(1+x)^{t_2}).$$

于是 $W(x^{2^{m-2}}(1+x)^{t_1-2^{m-2}})+W((1+x)^{t_1-2^{m-2}}+(1+x)^{t_2}+\cdots+(1+x)^{t_n})\geq W(x^{2^{m-2}}(1+x)^{t_1-2^{m-2}})+W((1+x)^{t_1-2^{m-2}}+(1+x)^{t_2})=W((1+x)^{t_1}+(1+x)^{t_2})$

(由引理 5 和引理 7)

故定理在情况(Ⅲ.1)下成立.

情况(Ⅲ.2) $t_i-2^{m-1}\geq 2^{m-2}$, $i=2,\cdots,n$.

先假设 $t_1<2^{m-2}$,则

$$W((1+x)^{t_1}+(1+x)^{t_2}+\cdots+(1+x)^{t_n})$$
$$=W((1+x)^{t_1}+(1+x)^{2^{m-1}}+(1+x)^{t_2-2^{m-1}}+\cdots+(1+x)^{t_n-2^{m-1}}))$$
$$=W((1+x)^{t_1}+((1+x)^{t_2-2^{m-1}}+\cdots+(1+x)^{t_n-2^{m-1}})+x^{2^{m-1}}((1+x)^{t_2-2^{m-1}}+\cdots+(1+x)^{t_n-2^{m-1}}))$$
$$=W((1+x)^{t_1}+((1+x)^{t_2-2^{m-1}}+\cdots+(1+x)^{t_n-2^{m-1}}))+W((1+x)^{t_2-2^{m-1}}+\cdots+(1+x)^{t_n-2^{m-1}}).$$

由 $0\leq t_1<t_2-2^{m-1}<\cdots<t_n-2^{m-1}<2^{m-1}$,条件假设和引理 2 得

$$W((1+x)^{t_1}+(1+x)^{t_2}+\cdots+(1+x)^{t_n})$$
$$=W((1+x)^{t_1}+((1+x)^{t_2-2^{m-1}}+\cdots+(1+x)^{t_n-2^{m-1}}))+W((1+x)^{t_2-2^{m-1}}+\cdots+(1+x)^{t_n-2^{m-1}})$$
$$\geq W((1+x)^{t_1}+(1+x)^{t_2-2^{m-1}})+W((1+x)^{t_2-2^{m-1}})$$
$$=W((1+x)^{t_1}+(1+x)^{t_2-2^{m-1}})+W(x^{2^{m-1}}(1+x)^{t_2-2^{m-1}})$$
$$=W((1+x)^{t_1}+(1+x)^{2^{m-1}}(1+x)^{t_2-2^{m-1}})\quad(\text{由引理 5})$$
$$=W((1+x)^{t_1}+(1+x)^{t_2}).$$

再假设 $2^{m-2}\leq t_1<2^{m-1}$.由引理 8 得

$$W((1+x)^{t_1}+(1+x)^{t_2}+\cdots+(1+x)^{t_n})=2W((1+x)^{t_1-2^{m-2}}+(1+x)^{t_2-2^{m-1}}+\cdots+(1+x)^{t_n-2^{m-1}})$$

由 $0\leq t_1-2^{m-2}<2^{m-2}\leq t_2-2^{m-1}<t_3-2^{m-1}<\cdots<t_n-2^{m-1}<2^{m-1}$和条件假设得

$$2W((1+x)^{t_1-2^{m-2}}+(1(x)^{t_2-2^{m-1}}+\cdots+(1+x)^{t_n-2^{m-1}})\geq 2W((1+x)^{t_1-2^{m-2}}+(1+x)^{t_2-2^{m-1}})$$
$$=W((1+x)^{t_1}+(1+x)^{t_2}).\quad(\text{由引理 8})$$

于是定理在情况(Ⅲ.2)下成立.

情况(Ⅲ.3)其他情况,即存在正整数 s, $2<s\leq n$,使得 $t_2<t_3<\cdots<t_{s-1}<2^{m-1}+2^{m-2}\leq t_s<\cdots<t_n$.

先假设 $2^{m-2}\leq t_1<2^{m-1}$.由引理 9 得

$$W((1+x)^{t_1}+(1+x)^{t_2}+\cdots+(1+x)^{t_n})\geq W((1+x)^{t_1}+(1+x)^{t_2}+\cdots+(1+x)^{t_{s-1}}).$$

由情况(Ⅲ.1)的证明和 $t_2<t_3<\cdots<t_{s-1}<2^{m-1}+2^{m-2}$得 $W((1+x)^{t_1}+(1+x)^{t_2}+\cdots+(1+x)^{t_{s-1}})\geq W((1+x)^{t_1}+(1+x)^{t_2})$.

于是有 $W((1+x)^{t_1}+(1+x)^{t_2}+\cdots+(1+x)^{t_n})\geq W((1+x)^{t_1}+(1+x)^{t_2})$.

再假设 $t_1<2^{m-2}$.由引理 11 得 $W((1+x)^{t_1}+(1+x)^{t_2}+\cdots+(1+x)^{t_n})=W((1+x)^{t_1}+(1+x)^{t_2-2^{m-1}+2^{m-2}}+\cdots+(1+x)^{t_{s-1}-2^{m-1}+2^{m-2}}+(1+x)^{t_s}+\cdots+(1+x)^{t_n})$.

由于 $2^{m-2}\leq\deg((1+x)^{t_2-2^{m-1}+2^{m-2}}+\cdots+(1+x)^{t_{s-1}-2^{m-1}+2^{m-2}})<2^{m-1}$由情况(Ⅰ)的证明和条件假设得

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

$$W((1+x)^{t_1}+(1+x)^{t_2-2^{m-1}+2^{m-2}}+\cdots+(1+x)^{t_{s-1}-2^{m-1}+2^{m-2}}+(1+x)^{t_s}+\cdots+(1+x)^{t_n})$$
$$\geq W((1+x)^{t_1}+(1+x)^{t_2-2^{m-1}+2^{m-2}})=W((1+x)^{t_1}+(1+x)^{t_2}).$$ (由引理 10)

故结论在情况(Ⅲ.3)下成立,于是当 $2^{m-1}\leq t_n<2^m$ 时结论成立.

由归纳法得结论成立. #

定理 1 表明当 $t_1<t_2<\cdots<t_n$ 时,多项式 $(1+x)^{t_1}+(1+x)^{t_2}+\cdots+(1+x)^{t_n}$ 的权重不小于多项式 $(1+x)^{t_1}+(1+x)^{t_2}$ 的权重,但是当 $n\geq 4$ 时多项式 $(1+x)^{t_1}+(1+x)^{t_2}+(1+x)^{t_3}$ 的权重可能大于多项式 $(1+x)^{t_1}+(1+x)^{t_2}+\cdots+(1+x)^{t_n}$ 的权重. 例如当 $t_1=0, t_2=1, t_3=2, t_4=3$ 时, $W((1+x)^{t_1}+(1+x)^{t_2}+(1+x)^{t_3}+(1+x)^{t_4})=1$ 但 $W((1+x)^{t_1}+(1+x)^{t_2}+(1+x)^{t_3})=3$.

在下一节中,将利用定理 1 给出 $err_2(\underline{s})$ 的值.

3　周期为 2^n 的二元序列其 $\mathrm{err}_2(\underline{s})$ 的值

对周期为 N 的二元序列 $\underline{s}=(s_0,s_1,\cdots,s_{N-1},s_0,\cdots)$ 记

$$s(x)=s_0+s_1x+\cdots+s_{N-1}x^{N-1}+s_0x^N+\cdots;$$
$$s^N(x)=s_0+s_1x+\cdots+s_{N-1}x^{N-1}.$$

于是有

$$\begin{aligned}s(x)&=s_0+s_1x+s_2x^2+\cdots+s_{N-1}x^{N-1}+s_0x^N+\cdots\\&=s^N(x)+x^Ns^N(x)+x^{2N}s^N(x)+\cdots\\&=s^N(x)/(1+x^{2^n})=s^N(x)/(1+x)^{2^n}.\end{aligned}$$

由于 $\{(1+x)^0,(1+x)^1,\cdots,(1+x)^{2^n-1}\}$ 也是线性空间 $\{f(x)\mid \deg(f(x))<2^n\}$ 的一组基,故存在 $t_1,t_2,\cdots,t_m$ 满足 $0\leq t_1<t_2<\cdots<t_m, m\geq 1$ 使得 $s^N(x)=(1+x)^{t_1}+(1+x)^{t_2}+\cdots+(1+x)^{t_m}$,于是 $s(x)=((1+x)^{t_1}+(1+x)^{t_2}+\cdots+(1+x)^{t_m})/(1+x)^{2^n}$.

若序列 $\underline{s}$ 的线性复杂度为 $LC(\underline{s})$,则有 $t_1=2^n-LC(\underline{s})$,即 $s^N(x)=(1+x)^{2^n-LC(\underline{s})}+(1+x)^{t_2}+\cdots+(1+x)^{t_m}$ 其中 $2^n-LC(\underline{s})<t_2<\cdots<t_m, m\geq 1$.

定理 2[1]　对周期为 2^n 的二元序列 $\underline{s}$ 有 $err_1(\underline{s})=2^{W_h(2^n-LC(\underline{s}))}$. 若 $\underline{e}$ 是周期为 2^n 的二元序列并且 $e^N(x)=e_0+e_1x+\cdots+e_{N-1}x^{N-1}$,则 $LC(\underline{s}+\underline{e})<LC(\underline{s})$ 当且仅当 $e^N(x)=(1+x)^{2^n-LC(\underline{s})}e_1(x)$,其中 $e_1(x)$ 是二元域上的多项式并且 $e_1(1)=1$.

注　若把 $e^N(x)$ 写成形如 $e^N(x)=(1+x)^{c_1}+(1+x)^{c_2}+\cdots+(1+x)^{c_k}$,其中 $0\leq c_1<c_2<\cdots<c_k$ 并且 $k\geq 1$,则定理 2 表明 $LC(\underline{s}+\underline{e})<LC(\underline{e})$ 当且仅当 $c_1=2^n-LC(\underline{s})$.

定理 3　设 $\underline{s}$ 是周期为 $N=2^n$ 的二元序列,$LC(\underline{s})$ 为其线性复杂度. 若

$$s^N(x)=(1+x)^{2^n-LC(\underline{s})}+(1+x)^{t_2}+\cdots+(1+x)^{t_m}$$

并且 $W((1+x)^{2^n-LC(\underline{s})}+(1+x)^{t_2})>W((1+x)^{2^n-LC(\underline{s})})$,其中 $2^n-LC(\underline{s})<t_2<\cdots<t_m, m>1$ 则

$$LC_{k_1}(\underline{s})=2^n-t_2,$$

其中 $k_1=err_1(\underline{s})$.

证明　首先令 $e^N(x)=(1+x)^{2^n-LC(\underline{s})}$,则 $W(e^N(x))=k_1$ 并且 $LC(\underline{s}+\underline{e})=2^n-t_2$. 故由 $err_1(\underline{s})$ 的定义得只要证明对任意的周期为 2^n 的二元序列 $\underline{e}$ 满足 $LC(\underline{s}+\underline{e})<LC(\underline{s})$, $W_N(\underline{e})=k_1$ 都有 $LC(\underline{s}+\underline{e})\geq 2^n-t_2$.

由定理 2 的注得要使 $LC(\underline{s}+\underline{e})<LC(\underline{s})$ 就必有 $e^N(x)=(1+x)^{c_1}+(1+x)^{c_2}+\cdots+(1+x)^{c_k}$,其中 $0\leq c_1=2^n-LC(\underline{s})<c_2<\cdots<c_k$.

若 $k=1$ 则 $e^N(x)=(1+x)^{2^n-LC(\underline{s})}$. 于是 $LC(\underline{s}+\underline{e})=2^n-t_2$.

现在假设 $k>1$,则断言 $c_2\neq t_2$ 事实上,若 $c_2=t_2$,则由定理 1 $W(e^N(x))\geq W((1+x)^{2^n-LC(\underline{s})}+(1+x)^{t_2})>W((1+x)^{2^n-LC(\underline{s})})=2^{W_h(2^n-LC(\underline{s}))}$. 这与 $W_N(\underline{e})=k_1$ 矛盾. 故 $c_2\neq t_2$ 若 $c_2>t_2$,显然 $LC(\underline{s}+\underline{e})=2^n-t_2$. 反之若 $c_2<t_2$,则有 $LC(\underline{s}+\underline{e})=2^n-c_2>2^n-t_2$. 于是对所有的周期为 2^n 的二元序列 $\underline{e}$ 满足 $LC(\underline{s}+\underline{e})<LC(\underline{s})$, $W_N(\underline{e})=k_1$ 都有 $LC(\underline{s}+\underline{e})=2^n-t_2$.

故结论成立. #

定理 4　若 $\underline{s}$ 是周期为 $N=2^n$ 的二元序列,$LC(\underline{s})$ 是其线性复杂度. 若

$$s^N(x)=(1+x)^{2^n-LC(\underline{s})}+(1+x)^{t_2}+\cdots+(1+x)^{t_m}$$

并且 $W((1+x)^{2^n-LC(\underline{s})}+(1+x)^{t_2})>W((1+x)^{2^n-LC(\underline{s})})$,其中 $2^n-LC(\underline{s})<t_2<\cdots<t_m, m>1$,则

$$err_2(\underline{s})=2^{W_h(2^n-LC(\underline{s}))}+2^{W_h(t_2)}-2^{W_h((2^n-LC(\underline{s}))\wedge t_2)+1}$$

并且 $LC_{k_2}(\underline{s})\leq 2^n-t_3$,其中 $k_2=err_2(\underline{s})$.

证明　首先由定理 3 得 $LC_{k_1}(\underline{s})=2^n-t_2$ 其中 $k_1=err_1(\underline{s})$. 设二元序列 $\underline{e}$ 满足 $e^N(x)=(1+x)^{c_1}+(1+x)^{c_2}+\cdots+(1+x)^{c_k}$,其中 $c_1<c_2<\cdots<c_k$. 下面证明只有当 $c_1=2^n-LC(\underline{s})$ 且 $c_2=t_2$ 时才有 $LC(\underline{s}+\underline{e})<LC_{k_1}(\underline{s})<LC(\underline{s})$. 事实上,若 $k=1$,则由定理 2 得存在唯一的二元序列满足 $LC(\underline{s}+\underline{e})<LC(\underline{s})$ 即 $e^N(x)=(1+x)^{2^n-LC(\underline{s})}$. 但 $LC(\underline{s}+\underline{e})=2^n-t_2=LC_{k_1}(\underline{s})$,故 $k>1$. 由定理 2 要证明定理成立,只要证明对二元序列 $\underline{e}$ 都有 $LC(\underline{s}+\underline{e})\geq LC_{k_1}(\underline{s})=2^n-t_2$,其中 $\underline{e}$ 满足 $e^N(x)=(1+x)^{c_1}+(1+x)^{c_2}+\cdots+(1+x)^{c_k}$ 并且 $0\leq c_1=2^n-LC(\underline{s})<c_2<\cdots<c_k, c_2\neq t_2$. 事实上,若 $c_2>t_2$,显然有 $LC(\underline{s}+\underline{e})=2^n-t_2$. 反之若 $c_2<t_2$ 则有 $LC(\underline{s}+\underline{e})=2^n-c_2>2^n-t_2$. 故只有当 $c_1=2^n-LC(\underline{s})$ 并且 $c_2=t_2$ 时才有 $LC(\underline{s}+\underline{e})<LC_{k_1}(\underline{s})<LC(\underline{s})$. 又由定理 1 得

$$W((1+x)^{2^n-LC(\underline{s})}+(1+x)^{t_2}+(1(x)^{c_3}+\cdots+(1+x)^{c_k})$$
$$\geq W((1+x)^{2^n-LC(\underline{s})}+(1+x)^{t_2}).$$

故由 $err_2(\underline{s})$ 的定义得 $err_2(\underline{s})\geq W((1+x)^{2^n-LC(\underline{s})}+(1+x)^{t_2})$.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

对满足 $e^N(x) = (1+x)^{2^n - LC(\underline{s})} + (1+x)^{t_2}$ 的二元序列 $\underline{e}$，显然有 $LC(\underline{s}+\underline{e}) = 2^n - t_3 < LC_{k_1}(\underline{s})$，$W(e^N(x)) = W((1+x)^{2^n - LC(\underline{s})} + (1+x)^{t_2})$.

由 $err_2(\underline{s})$ 的定义和引理 4 得

$$err_2(\underline{s}) = W((1+x)^{2^n - LC(\underline{s})} + (1+x)^{t_2}) = 2^{W_h(2^n - LC(\underline{s}))} + 2^{W_h(t_2)} - 2^{W_h((2^n - LC(\underline{s})) \wedge t_2) + 1}$$

并且 $LC_{k_2}(\underline{s}) \leq 2^n - t_3$. #

由定理 4 立得推论 1.

推论 1 设二元序列 $\underline{s}$ 的周期为 2^n，若序列的线性复杂度为 2^n，则存在正整数 $t_1, t_2, \cdots, t_m, 0 < t_1 < \cdots < t_m$ 使得 $s^N(x) = 1 + (1+x)^{t_1} + (1+x)^{t_2} + \cdots + (1+x)^{t_m}$. 若 t_1 不为 2 的方幂，则 $err_2(\underline{s}) = 2^{W_h(t_1)} - 1$，并且 $LC_{k_2}(\underline{s}) \leq 2^n - t_2$ 其中 $k_2 = err_2(\underline{s})$.

证明 因为 $LC(\underline{s}) = 2^n$ 易得 $s^N(x) = 1 + (1+x)^{t_1} + (1+x)^{t_2} + \cdots + (1+x)^{t_m}$ 其中 $t_1, t_2, \cdots, t_m$ 是正整数且 $0 < t_1 < t_2 < \cdots < t_m$. 断言 $W(1 + (1+x)^{t_1}) = 1$ 当且仅当 t_1 为 2 的方幂. 事实上，若 t_1 为 2 的方幂，则 $1 + (1+x)^{t_1} = 1 + 1 + x^{t_1} = x^{t_1}$. 反之若 $W(1 + (1+x)^{t_1}) = 1$，则 $1 + (1+x)^{t_1} = x^{t_1}$，即 t_1 为 2 的方幂. 由定理 4 得 $err_2(\underline{s}) = 2^{W_h(t_1)} - 1$ 并且 $LC_{k_2}(\underline{s}) \leq 2^n - t_2$，其中 $k_2 = err_2(\underline{s})$. #

参考文献:

[1] K Kurosawa, F Sato, T Sakata, W Kishimoto. A relationship between linear complexity and k-error linear complexity[J]. IEEE Trans IT, 2000, IT-46:694-698.

[2] James L. Massey D J. Costello, J Justesen. Polynomial Weights and Code Constructions[J]. IEEE Trans IT. 1973, IT-19:101-110.

[3] Mark Stamp, Clyde F Martin. An Algorithm for the k-error Linear Complexity of Binary Sequences with Period 2n[J]. IEEE Trans IT. July, 1993. IT-39:1398-1401.

[4] C Ding, G Xiao, W Shan. The stability theory of stream ciphers[M]. In Springer Verlag, Lecture Notes in Computer Science, 1991. 561.

[5] W Meidl, H Niederreiter. Counting Functions and Expected Values for the k-error Linear Complexity[J]. Finite Fields and Their Applications 8. 2002. 142-154.

[6] W Meidl, H Niederreiter. Linear Complexity, k-error Linear Complexity, and the Discrete Fourier Transform[J]. Journal of Complexity. 2002, 18. 87-103.

[7] R A Rueppel. Linear Complexity and Random Sequences[A]. Advances in Cryptology-EUROCRYPT '85[C]. Lecture Notes in Computer Science, Vol. 219, Berlin, Springer Verlag, 1986. 167-188.

[8] E R Berlekamp. Algebraic Coding Theory[M]. New York: McGraw-Mill, 1986.

作者简介:

赵耀东 男，1979 生于山东莱芜，郑州信息工程大学信息工程学院博士研究生，主要研究方向为密码学，信息安全. E-mail: zhaoyaodong@163.com.

威文峰 男，1963 生于浙江宁波，郑州信息工程大学信息工程学院教授，博士生导师，主要研究方向为密码学，信息安全. E-mail: wenfen.qi@263.net.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net