第 36 卷 第 1 期 计 算 机 工 程 2010 年 1 月
Vol.36 No.1 Computer Engineering January 2010
·安全技术· 文章编号：1000—3428(2010)01—0164—02 文献标识码：A 中图分类号：TP309.2

$GF(2)$上周期为 $2p^n$ 序列的 $m(s)$

赵 峰[1,2]，冯金磊[2]
(1.安徽工业大学管理科学与工程学院，马鞍山 243002；2. 安徽工业大学计算机学院，马鞍山 243002)

摘 要：给出多项式的若干引理，并对引理进行证明。在此基础上，给出 $GF(2)$上周期序列线性复杂度的表达形式，应用该表达式得出周期 $N=2p^n$ 的二元序列线性复杂度和 $m(s)$之间的关系，其中 p 是个奇素数，并且 2 是一个模 p^2 的本源根。结合魏算法，给出 2 个实例进行证明，结果表明该结果的正确性。

关键词：密码；流密码；线性复杂度；最小多项式

$m(s)$ of Sequences with Period $2p^n$ over $GF(2)$

ZHAO Feng[1,2], FENG Jin-lei[2]
(1. College of Management Science and Engineering, Anhui University of Technology, Ma'anshan 243002;
2. College of Computer, Anhui University of Technology, Ma'anshan 243002)

【Abstract】This paper gives some polynomial lemmas and proof of lemma. On basis of these lemmas, the expression of Linear Complexity(LC) of periodic sequences is gave. Application of the expression show the most important result of this article, a relationship between $m(s)$ and the LC of a given sequence s with period $N=2p^n$ over $GF(2)$. Where p is an odd prime, 2 is a primitive root module p. Combined with Wei algorithm, it gives two examples to prove the results. Result shows that the relationship is correct.

【Key words】cipher; stream cipher; Linear Complexity(LC); minimum polynomial

1 概述

密钥序列的线性复杂度(LC)是流密码强度的一个重要度量指标。文献[1]给出了周期为 2^n 二元序列线性复杂度的快速算法(Games-Chan 算法)。文献[2]推广了该算法。文献[3]给出了 $GF(q)$上周期为 p^n 序列线性复杂度的快速算法，这里 p 是个奇素数，q 是素数且是模 p^2 的本源根。文献[4]给出了 $GF(q)$上周期为 $2p^n$ 序列线性复杂度的快速算法，这里 p 是个奇素数，q 是素数且是模 p^2 的本源根。文献[5]给出了 $GF(p^m)$上周期为 $2n$ 序列线性复杂度的快速算法，这里 n 是个正整数，且存在元素 $b\in GF(p^m)$，使得 $b^n=-1$。该算法的思路是转化为求 2 个周期为 n 的序列的线性复杂度。把此结果和已知的算法如 Berlekamp-Massey 算法，Games-Chan 算法等相结合，可以得到 $GF(p^m)$上周期为 2^tn 序列线性复杂度的快速算法，这里 p 是个素数，$\gcd(n,p^m-1)=1, p^m-1=2^tu$，其中，$n$ 和 u 为整数。

某些序列的线性复杂度极不稳定，即当改变这些序列周期的一位或几位时，其线性复杂度发生很大的变化。序列的 k-错线性复杂度(k-LC)被文献[6]定义为改变序列中至多 $k(0\leqslant k\leqslant N)$位后，得到的所有序列的线性复杂度中最小的线性复杂度。k-LC 能够很好地减少由于元素改变引起的线性复杂度的不稳定性。特别需要指出的是文献[7]提出的球体复杂度要早于 k-LC，其本质和 k-error 一样。目前只有 $GF(2)$上周期为 2^n 的二元序列的 k-错线性复杂度的有效算法[6] (Stamp-Martin 算法)。文献[8]将这个算法推广为计算 $GF(p^m)$上周期为 p^n 序列的 k 错线性复杂度，这里 p 是个素数。

有时人们只关心当改变序列多少位时，序列的线性复杂度会否降低。本文中 $m(s)$代表使序列 S 的 k-错线性复杂度严格小于线性复杂度的 k。给出了 $GF(2)$上周期 $N=2p^n$ 的序列的 $m(s)$和 LC 之间的关系。

令 $s=\{s_0,s_1,s_2,s_3,\cdots\}$ 为 $GF(2)$上的数列。如果存在正整数 N，使 $s_i=s_{i+N}$ 成立，$i=0,1,\cdots$，则称 s 为周期序列；N 为序列的周期；$s(x)=s_0+s_1x+s_2x^2+\cdots=\sum_{i=0}^{\infty}s_ix^i$ 为 $s=\{s_0,s_1,s_2,s_3,\cdots\}$ 的生成函数。

令 s 为周期序列，第一个周期为 $s^N=\{s_0,s_1,s_2,\cdots s_{N-1}\}$。$s^N$ 的生成函数为 $s(x)=s_0+s_1x+s_2x^2+\cdots+s_{N-1}x^{N-1}$。

如果 s 是周期序列，第一个周期为 s^N，那么

$$s(x)=s^N(x)(1+x^N+x^{2N}+\cdots)=\frac{s^N(x)}{1-x^N}=\frac{s^N(x)/\gcd(s^N(x),1-x^N)}{(1-x^N)/\gcd(s^N(x),1-x^N)}=\frac{g(x)}{f_s(x)}$$

其中，

$$f_s(x)=(1-x^N)/\gcd(s^N(x),1-x^N),$$
$$g(x)=s^N(x)/\gcd(s^N(x),1-x^N)$$

显然，$\gcd(g(x),f_s(x))=1$，$\deg(g(x))<\deg(f_s(x)))=1$。$f_s(x)$ 称为 s 的最小多项式，$f_s(x)$ 的度数称为 s 的线性复杂度。即

基金项目：安徽省教育厅基金资助重大项目“Web 主动服务关键技术研究与应用”(ZD200904)
作者简介：赵 峰(1977－)，男，讲师、硕士，主研方向：信息安全，数据挖掘；冯金磊，硕士研究生
收稿日期：2009-06-04 **E-mail：**zhaofeng169@sina.com

$$c(s)=\deg(f_s(x))=N-\deg(\gcd(s^N(x),1-x^N)) \quad (1)$$

2 使k-$LC(s)$<$LC(s)$成立的最小k

$GF(2)$ 上周期 $N=2p^n$ 的序列 $s=(a_0,a_0,\cdots)$ 的 k-$LC(s)$定义为 $k-LC(s)=\min\{LC(s+e)\,|\,W_H(e)\leqslant k\}$，这里 $e=(e_0,e_1,\cdots)$ 为 $GF(2)$ 上周期为 $N=2p^n$ 的误差序列，$W_H(e)$ 为 N 元组 $(e_0,e_1,\cdots,e_N)$ 的汉明重量。

定义 设 n 是正整数，称 $\Phi_n(x)$ 是 n 次分圆多项式，若 $\Phi_n(x)=\prod_{\substack{i=1\\ \gcd(i,n)=1}}^{n}(x-\alpha^i)$，其中 α 表示 n 次本原单位根。

引理 1 设 p 是素数，则 $\Phi(p^n)=p^n-p^{n-1}$，这里 n 是正整数，$\Phi(m)$ 是 Euler 函数，表示 1,2,…,m-1 中与 m 互素的个数。

引理 2 设 p 是一个素数，m 为正整数，则 $\Phi_{p^m}(x)=\Phi_p(x^{p^{m-1}})$。

证明：由于 p 是一个素数，

$$\Phi_p(x)=\prod_{\substack{i=1\\ \gcd(i,p)=1}}^{p}(x-\alpha^i)=(\prod_{i=0}^{p-1}(x-\alpha^i))/(x-\alpha^0)=$$

$$\frac{x^p-1}{x-1}=1+x+x^2+\cdots+x^{p-1}$$

注意到 $\alpha^j=\exp(\frac{2\pi i}{p^m}j)=\exp(\frac{2\pi i}{p^m}k)=\alpha^k$，其中 $j=pk$，因此，

$$\Phi_{p^m}(x)=\frac{x^{p^m}-1}{\prod_{j=0,p\nmid j}^{p^m-1}(x-\alpha^j)}=\frac{x^{p^m}-1}{\prod_{k=0}^{p^{m-1}-1}(x-\alpha^k)}=\frac{x^{p^m}-1}{x^{p^{m-1}}-1}=\Phi_p(x^{p^{m-1}})$$

引理 3 设 p 是一个素数，m 与 n 为正整数。记 $\Phi_{p^m}(x)^2=[\Phi_{p^m}(x)]^2$，则在 $GF(2)$上，

$\Phi_{p^m}(x)^2=\Phi_{p^m}(x^2)=\Phi_p(x^{2p^{m-1}})$。

证明：因为运算在 $GF(2)$上，所以 $(1+x)^2=1+x^2$，

$$\Phi_p(x)^2=(1+x+x^2+\cdots+x^{p-1})^2=$$

$$1+x^2+x^4+\cdots+x^{2(p-1)}=\Phi_p(x^2)$$

由引理 3 可得

$\Phi_{p^m}(x)^2=\Phi_p(x^{p^{m-1}})^2=\Phi_p(x^{2p^{m-1}})=\Phi_p(x^2)^{p^{m-1}}=\Phi_{p^m}(x^2)$。

引理 4 令 l 为形如 $(p-1)\sum_{i=1}^{m}\varepsilon_i p^{i-1}$ 的正整数，$W_H(l)$ 代表 $(\varepsilon_0,\varepsilon_1,\cdots,\varepsilon_m)$ 的汉明重量；$e(x)=\prod_{i=1}^{m}(\Phi_{p^i}(x))^{\varepsilon_i}$，$0\leqslant\varepsilon_i\leqslant 2$，$1\leqslant i\leqslant m$，$W_H(e(x))$ 代表 $e(x)$ 的重量，即 $e(x)$ 中非 0 系数的个数。那么 $w(e(x))\leqslant p^{W_H(l)}$。

证明：$(\Phi_{p^i}(x))^{\varepsilon_i}=(1+x^{p^{i-1}}+x^{2p^{i-1}}+\cdots+x^{(p-1)p^{i-1}})^{\varepsilon_i}$ 至多 p 项，因此，$w(e(x))\leqslant p^{\sum_{i=1}^{m}\varepsilon_i}$。

引理 5 $1-x^{2p^m}=\left(1-x^2\right)\times\prod_{i=1}^{m}\Phi_{p^i}\left(x^2\right)=\left(1-x\right)^2\times\prod_{i=1}^{m}\Phi_{p^i}\left(x\right)^2$。

证明：

$$(1-x^2)\prod_{i=1}^{m}\Phi_{p^i}(x^2)=(1-x^2)(1+x^2+x^{2\times2}+\cdots+x^{(p-1)\times2})\prod_{i=2}^{m}\Phi_{p^i}(x^2)=$$

$$(1-x^{2p})(1+x^{2p}+x^{2*2p}+\cdots+x^{(p-1)\times2p})\prod_{i=2}^{m}\Phi_{p^i}(x^2)=\cdots=$$

$$(1-x^{2p^{m-1}})(1+x^{2p^{m-1}}+x^{2\times2p^{m-1}}+\cdots+x^{(p-1)\times2p^{m-1}})=1-x^{2p^m}$$

由式(1)和引理 5 可得，$GF(2)$上周期为 $2p^m$ 的序列的线性复杂度为如下形式：

$$LC(s)=2p^m+\varepsilon_0+(p-1)\sum_{i=1}^{m}\varepsilon_i p^{i-1}=2-\varepsilon_0+(p-1)\sum_{i=1}^{m}(2-\varepsilon_i)p^{i-1}$$

$0\leqslant\varepsilon_i\leqslant 2,\ 0\leqslant i\leqslant m$

下面定理给出了 $GF(2)$上周期 $N=2p^m$ 的 $m(s)$。

定理 设 s 为 $GF(2)$ 上周期为 $2p^n$ 的序列，这里 p 是奇素数，2 是模 p^2 的本源根。$LC(s)=2-\varepsilon_0+(p-1)\sum_{i=1}^{m}(2-\varepsilon_i)p^{i-1}$，这里 $0\leqslant\varepsilon_i\leqslant 2, 0\leqslant i\leqslant m$，则

$$m(s)\leqslant\begin{cases}p^{w_H(N-LC(s))} & \text{if } \varepsilon_0=0\\ 2p^{w_H(N-LC(s))} & \text{if } \varepsilon_0=1\\ 2p^{u-w_H(N-LC(s))} & \text{if } \varepsilon_0=1\end{cases}$$

其中，u 是 $\varepsilon_0=2$ 时使 $\varepsilon_u\leqslant 2$ 成立的最小的正整数，$1\leqslant u\leqslant m$。

证明：

(1)当 $\varepsilon_0=0$ 时，则 $s^{2p^m}=r(x)\prod_{i=1}^{m}(\Phi_{p^i}(x))^{\varepsilon_i}$，这里在 $\varepsilon_i=2$ 时，$\gcd(r(x),1-x)=1$, $\gcd(r(x),\Phi_{p^i}(x))=1$。令 $e(x)=-r(1)\prod_{i=1}^{m}(\Phi_{p^i}(x))^{\varepsilon_i}$，因为 $(1-x)\,|\,(r(x)-r(1))$，所以

$$\deg(\gcd(1-x^{2p^m},s^{2p^m}(x)+e(x)))\geqslant 1+(p-1)\sum_{i=1}^{m}\varepsilon_i p^{i-1}>$$

$$\deg(\gcd(1-x^{2p^m},s^{2p^m}(x)))$$

则 $w(e(x))$-错复杂度 $LC(s)\leqslant LC(s)-1$。

因为当 $\varepsilon_i>0$ 时，$(\Phi_{p^i}(x))^{\varepsilon_i}=\Phi_{p^i}(x^{\varepsilon_i})$，所以 $m(s)\leqslant w(e(x))\leqslant p^{w_H(N-LC(s))}$

(2)当 $\varepsilon_0=1$ 时，则 $s^{2p^m}=r(x)(1-x)^{\varepsilon_0}\prod_{i=1}^{m}(\Phi_{p^i}(x))^{\varepsilon_i}$，这里在 $\varepsilon_i=2$ 时 $\gcd(r(x),1-x)=1,\gcd(r(x),\Phi_{p^i}(x))=1$。令 $e(x)=-r(1)(1-x)\prod_{i=1}^{m}(\Phi_{p^i}(x))^{\varepsilon_i}$。因为 $(1-x)\,|\,(r(x)-r(1))$，所以

$$\deg(\gcd(1-x^{2p^m},s^{2p^m}(x)+e(x)))\geqslant 1+\varepsilon_0+(p-1)\sum_{i=1}^{m}\varepsilon_i p^{i-1}>$$

$$\deg(\gcd(1-x^{2p^m},s^{2p^m}(x)))$$

则 $w(e(x))$-错复杂度 $LC(s)\leqslant LC(s)-1$。

因为 $(1-x)^{\varepsilon_0}=1-x^{\varepsilon_0}$，所以 $m(s)\leqslant w(e(x))\leqslant p^{w_H(N-LC(s))}$。

(3)当 $\varepsilon_0=2$ 时，设 u 为 $\varepsilon_u\leqslant 2$ 成立的最小的正整数，$1\leqslant u\leqslant m$。$g(x)$ 为 $r(x)$ 整除 $\Phi_{p^u}(x)$ 的余式。$e(x)=-g(x)(1-x)^2\prod_{i=1}^{u-1}(\Phi_{p^i}(x))^{\varepsilon_i}\prod_{i=u}^{m}(\Phi_{p^i}(x))^{\varepsilon_i}$，因为 $\Phi_{p^u}(x)\,|\,(r(x)-r(1))$，所以

$$\deg(\gcd(1-x^{2p^m},s^{2p^m}(x)+e(x)))\geqslant(p-1)p^{u-1}+2+(p-1)\sum_{i=1}^{m}\varepsilon_i p^{i-1}>$$

$$\deg(\gcd(1-x^{2p^m},s^{2p^m}(x)))$$

则 $w(e(x))$-错复杂度 $LC(s)\leqslant LC(s)-1$。

因此，

$m(s)\leqslant w(e(x))\leqslant 2(p-1)p^{u-1}p^{w_H(N-LC(s))}\leqslant 2p^{u+w_H(N-LC(s))}$

例 结合魏算法，分析 $GF(2)$ 上周期为 $2p^n$ 的 2 个序列。

$s_1^N=(01101110000111100011011100111101101100111100100100111 1)$

$s_2^N=(00010011000101110010110001110011100001010101010100)$

周期序列 s_1 的周期为 54，其线性复杂度为 $LC(s_1)=52=2\times(2\times1+2\times3+2\times9)$，由定理 1 可知，$m(s_1)\leqslant 2$，通过改变 s_1 的 2 位，得到

$s_1'^N=(11001110000111100011011100111101101100111100100100111 1)$

$LC(s_1')=48<LC(s_1)$

周期序列 s_2 的周期为 50，其线性复杂度为 $LC(s_2)=49=1+4\times(2\times1+2\times5)$，由定理 1 可知，$m(s_2)\leqslant 2$，通过改变 s_2 的 2 位，得到

（下转第 169 页）