科 学 通 报
第 42 卷 第 18 期 Chinese Science Bulletin 1997 年 9 月

【研究简报】

环Z/(2^e)上本原序列最高权位的0，1分布(Ⅱ)

戚文峰 周锦君
(郑州信息工程学院应用数学系，郑州 450002)

关键词 线性递归序列 本原序列 最高权位序列 0，1 分布

设 $f(x)=x^n+c_{n-1}x^{n-1}+\cdots+c_0$ 是 $Z/(2^e)$上首一多项式，适合关系式

$$a_{i+n}=-(c_0a_i+c_1a_{i+1}+\cdots+c_{n-1}a_{i+n-1}),\ i=0,1,2,\cdots \tag{1}$$

的 $Z/(2^e)$上序列 $\boldsymbol{a}=(a_0,a_1,\cdots)$称由 $f(x)$生成的线性递归序列，由 $f(x)$生成的 $Z/(2^e)$上的所有序列的集合记为 $G(f(x))_e$，并记 $G'(f(x))_e=\{\boldsymbol{a}\in G(f(x))_e\mid \boldsymbol{a}\neq\boldsymbol{0} \bmod 2\}$. 递归式(1)等价于关系式 $f(x)\boldsymbol{a}=\boldsymbol{0}=(0,0,\cdots)$，其中 x 表示移位算子，即 $x\boldsymbol{a}=(a_1,a_2,a_3,\cdots)$. $Z/(2^e)$上序列 $\boldsymbol{a}$ 有唯一权位分解 $\boldsymbol{a}=\boldsymbol{a}_0+\boldsymbol{a}_12+\cdots+\boldsymbol{a}_{e-1}2^{e-1}$，其中 $\boldsymbol{a}_i=(a_{i0},a_{i1},\cdots)$是 0，1 序列，并称 $\boldsymbol{a}_i$ 是 $\boldsymbol{a}$ 的第 i 权位序列，称 $\boldsymbol{a}_{e-1}$为 $\boldsymbol{a}$ 的最高权位序列.

对 $Z/(2^e)$上首一 n 次多项式 $f(x)$，若 $f(0)$(即 c_0)是可逆元，则由文献[1]，$f(x)$的周期 $\mathrm{per}(f(x))_e\leqslant 2^{e-1}(2^n-1)$. 当 $\mathrm{per}(f(x))=2^{e-1}(2^n-1)$时，称 $f(x)$是 $Z/(2^e)$上 n 次本原多项式，并称 $G'(f(x))_e$ 中序列为 $f(x)$生成的本原序列. 文献[2]给出了本原多项式的系数判别条件，文献[3]给出了如下具有重要密码意义的保熵定理：设 $f(x)$是 $Z/(2^e)$上 n 次本原多项式，对 $\boldsymbol{a},\boldsymbol{b}\in G(f(x))_e$，则 $\boldsymbol{a}=\boldsymbol{b}$ 当且仅当它们的最高权位序列相等，即 $\boldsymbol{a}_{e-1}=\boldsymbol{b}_{e-1}$.

设 $f(x)$是 $Z/(2^e)$上 n 次本原多项式，$\boldsymbol{a}\in G'(f(x))_e$，由文献[4]可知，$\boldsymbol{a}$ 的第 k 权位序列 $\boldsymbol{a}_k$ 的周期 $\mathrm{per}(\boldsymbol{a}_k)=2^kT$，其中 $T=2^n-1$. 由文献[1]或[4]知，对 $1\leqslant d\leqslant e-1$，$Z/(2^e)$上，$x^{2^{d-1}T}-1=2^dh_d(x)\bmod f(x)$，其中 $h_k(x)$是 $Z/(2^e)$上次数小于 n 的多项式且 $h_k(x)\neq 0 \bmod 2$. 文献[5]给出如下的结论：

命题 A 设 $f(x)$是 $Z/(2^e)$上 n 次本原多项式，$T=2^n-1$，$\boldsymbol{a}\in G'(f(x))_e$，$d=[e/2]$，$\boldsymbol{s}=h(x)\boldsymbol{a}\bmod 2^d$，则 $\boldsymbol{a}_{e-1}$中“0”(或“1”)所占的比例 λ 为

$$\frac{1}{2}-\frac{N(\boldsymbol{s},0)}{2^dT}\leqslant\lambda\leqslant\frac{1}{2}+\frac{N(\boldsymbol{s},0)}{2^dT},$$

其中 $N(\boldsymbol{s},0)$表示 $\boldsymbol{s}$ 在一个周期中“0”的个数，$h(x)=\begin{cases}h_d(x), & \text{若 } e=2d,\\ h_{d+1}(x), & \text{若 } e=2d+1.\end{cases}$

利用这一结论，文献[5]证明了当 e 足够大时，绝大部分的 $\boldsymbol{a}_{e-1}$的 0，1 分布是很好的. 例如，当 $e=32$ 时，对 $Z/(2^e)$上 n 次本原多项式 $f(x)$，$G'(f(x))_e$ 中满足 $0.498\,046\,875\leqslant\lambda\leqslant 0.501\,953\,125$ 的序列 $\boldsymbol{a}$ 至少占 $G'(f(x))_e$ 中所有序列的 99.6%. 当 e 大于 32 时结论会更好.

上面结论中，对有部分 $\boldsymbol{a}_{e-1}$的 0，1 分布没法估计，这是因为在 $\boldsymbol{s}=h(x)\boldsymbol{a} \bmod 2^d$ 的一个

周期中零的个数很难给出估计，本文对 $Z/(2^4)$上本原序列中零的个数给出一个上界，从而对 $e\geqslant 8$，序列 $\boldsymbol{a}_{e-1}$在一个周期中“0”个数所占比例在 40% 到 60% 之间.

首先把命题 A 推广到如下一般情形：

定理 1　设 $f(x)$是 $Z/(2^e)$上 n 次本原多项式，$T=2^n-1$，$\boldsymbol{a}\in G(f(x))_e$ 且 $\boldsymbol{a}_0\neq 0$，$1\leqslant d\leqslant e/2$，$\boldsymbol{s}=h_{e-d}(x)\boldsymbol{a} \bmod 2^d$，则 $\boldsymbol{a}_{e-1}$中“0”(或“1”)所占的比例 λ 为

$$\frac{1}{2}-\frac{N(\boldsymbol{s},\ 0)}{2^dT}\leqslant\lambda\leqslant\frac{1}{2}+\frac{N(\boldsymbol{s},\ 0)}{2^dT},$$

其中 $N(\boldsymbol{s},\ 0)$表示 $\boldsymbol{s}$ 在一个周期中“0”的个数.

引理 1　设 $f(x)$是 F_2 上 n 次本原多项式，$\boldsymbol{a}=(a_0,\ a_1,\cdots)$，$\boldsymbol{b}=(b_0,\ b_1,\cdots)$是由 $f(x)$生成的 2 条不同的本原序列(即是 m-序列)，记 $S_{\boldsymbol{a},\boldsymbol{b}}(u,\ v)=\{i\mid a_i=u,\ b_i=v,\ 0\leqslant i\leqslant 2^n-2\}$，$M_{\boldsymbol{a},\boldsymbol{b}}(u,\ v)=|S_{\boldsymbol{a},\boldsymbol{b}}(u,\ v)|$，则 $M_{\boldsymbol{a},\boldsymbol{b}}(0,\ 0)=2^{n-2}-1$，$M_{\boldsymbol{a},\boldsymbol{b}}(0,\ 1)=M_{\boldsymbol{a},\boldsymbol{b}}(1,\ 0)=M_{\boldsymbol{a},\boldsymbol{b}}(1,\ 1)=2^{n-2}$.

引理 2　设 $f(x)$是 F_2 上 n 次本原多项式，$n\geqslant 3$，$\boldsymbol{a}$，$\boldsymbol{b}$，$\boldsymbol{c}$ 是由 $f(x)$生成的两两不同的 m-序列且 $\boldsymbol{a}+\boldsymbol{b}+\boldsymbol{c}\neq\boldsymbol{0}$，对 u，v，$w\in F_2$，记 $S_{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}}(u,\ v,\ w)=\{i\mid a_i=u,\ b_i=v,\ c_i=w,\ 0\leqslant i\leqslant 2^n-2\}$，令 $M_{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}}(u,\ v,\ w)=|S_{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}}(u,\ v,\ w)|$，则 $M_{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}}(u,\ v,\ w)=\begin{cases}2^{n-3}-1, & \text{若 } u=v=w=0,\\ 2^{n-3}, & \text{否则.}\end{cases}$

利用引理 1、引理 2 及权位序列之间的关系得到

引理 3　设 $f(x)$是 $Z/(2^4)$上 n 次本原多项式，$n\geqslant 3$，$\boldsymbol{a}$ 是由 $f(x)$生成的 $Z/(2^4)$上本原序列，若 $h_2(x)\neq 1 \bmod 2$，则 $\boldsymbol{a}$ 在一个周期($=2^3(2^n-1)$)内“0”的个数满足

$$N(\boldsymbol{a},\ 0)\leqslant 15\cdot 2^{n-3}-8.$$

由定理 1 和引理 3 得下面的定理 2.

定理 2　设 $f(x)$是 $Z/(2^e)$上 n 次本原多项式，$n\geqslant 3$，$e\geqslant 8$，$\boldsymbol{a}$ 是由 $f(x)$生成的 $Z/(2^e)$上本原序列，$h_2(x)$满足引理 3 的条件，则 $\boldsymbol{a}_{e-1}$中“0”(或“1”)所占的比例满足

$$\frac{1}{2}-\frac{15\cdot 2^{n-6}-1}{2(2^n-1)}\leqslant\lambda\leqslant\frac{1}{2}+\frac{15\cdot 2^{n-6}-1}{2(2^n-1)}.$$

推论 1　条件同定理 2，则 $\boldsymbol{a}_{e-1}$中“0”所占的比例满足 38.281 25% $<\lambda<$ 61.718 75%.

为了更精确估计 λ，下面进一步改进引理 3，为此先给出引理 4 和引理 5.

引理 4　设 $f(x)$是 F_2 上 n 次本原多项式，$n\geqslant 4$，$\boldsymbol{a}$，$\boldsymbol{b}$，$\boldsymbol{c}$ 和 $\boldsymbol{d}$ 是由 $f(x)$生成的 m-序列，符号 $M_{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c},\boldsymbol{d}}(u,\ v,\ w,\ x)$类似引理 2 中定义，若 $\boldsymbol{a}$，$\boldsymbol{b}$，$\boldsymbol{c}$，$\boldsymbol{d}$ 两两不同且 $\boldsymbol{a}+\boldsymbol{b}+\boldsymbol{c}$，$\boldsymbol{a}+\boldsymbol{b}+\boldsymbol{d}$，$\boldsymbol{a}+\boldsymbol{c}+\boldsymbol{d}$，$\boldsymbol{b}+\boldsymbol{c}+\boldsymbol{d}$ 和 $\boldsymbol{a}+\boldsymbol{b}+\boldsymbol{c}+\boldsymbol{d}$ 都不为 $\boldsymbol{0}$，则

$$M_{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c},\boldsymbol{d}}(u,\ v,\ w,\ x)=\begin{cases}2^{n-4}-1, & \text{若 } u=v=w=0,\\ 2^{n-4}, & \text{否则.}\end{cases}$$

引理 5[6]　设 $\boldsymbol{a}$ 是 $Z/(2^e)$上 n 次本原序列且 $\boldsymbol{a}\neq 0$，则 $\boldsymbol{a}$ 在一个周期($=2(2^n-1)$)中 0 的个数 $N(\boldsymbol{a},\ 0)\leqslant 2^n+2^{n/2}-2$.

利用引理4、引理5及权位序列之间的关系得到

引理6 在引理3的条件的基础上,再假设 $n\geqslant 4$, $h_1(x)h_2(x)\neq 1 \bmod(2, f(x))$, $(1+h_1(x))h_2(x)\neq 1 \bmod(2, f(x))$, 则 $\boldsymbol{a}$ 在一个周期($=2^3(2^n-1)$)中"0"的个数满足

$$N(\boldsymbol{a}, 0)\leqslant \min\{13\cdot 2^{n-3}-8,\ 12\cdot 2^{n-3}+2^{n/2}-2\}.$$

由定理1和引理6得下面的定理3.

定理3 设 $f(x)$是 $Z/(2^e)$上 n 次本原多项式, $n\geqslant 4$, $e\geqslant 8$, $\boldsymbol{a}$ 是由 $f(x)$生成的 $Z/(2^e)$上本原序列且 $\boldsymbol{a}_0\neq 0$, $h_1(x)$和 $h_2(x)$满足引理6的条件,则 $\boldsymbol{a}_{e-1}$中"0"(或"1")所占的比例满足

$$\frac{1}{2}-\frac{6\cdot 2^{n-4}+2^{\frac{n}{2}-1}-1}{2^2(2^n-1)}\leqslant \lambda \leqslant \frac{1}{2}+\frac{6\cdot 2^{n-4}+2^{\frac{n}{2}-1}-1}{2^2(2^n-1)},$$

且

$$\frac{1}{2}-\frac{13\cdot 2^{n-6}-1}{2(2^n-1)}\leqslant \lambda \leqslant \frac{1}{2}+\frac{13\cdot 2^{n-6}-1}{2(2^n-1)}.$$

推论2 条件同定理3,则 $\boldsymbol{a}_{e-1}$中"0"(或"1")所占的比例满足

(ⅰ)当 $n\leqslant 7$ 时, $40.157\,9\% < \lambda < 59.842\,1\%$;

(ⅱ)当 $n\geqslant 8$ 时, $40.250\,5\% < \lambda < 59.749\,5\%$;

(ⅲ)当 $n\geqslant 30$ 时, $40.624\,9\% < \lambda < 59.375\,1\%$.

文献[5]指出当 e 充分大,绝大多数的 $\boldsymbol{a}_{e-1}$具有好的分布,推论2又保证其他的 $\boldsymbol{a}_{e-1}$不会有太差的分布.

致谢 本工作为中国科学院研究生院信息安全国家重点实验室资助项目.

参 考 文 献

1 Ward M. The arithmetical theory of linear recurring sequences. Trans Amer Math Soc, 1933, 35(6): 600

2 Dai Zongduo, Huang Minqiang. A criterion for primitiveness of polynomials over Z mod 2^d. Chinese Science Bulletin, 1991, 36(11): 892

3 Huang Minqiang, Dai Zongduo. Projective maps of linear recurring sequences with maximal p-adic periods. Fibonacci Quart, 1992, 30(2): 139

4 戚文峰,周锦君. 环$\mathbb{Z}/(2^e)$上本原序列最高权位的0,1分布. 中国科学,A辑,1997,27(4): 311

5 Dai Zongduo. Binary sequences derived from ML-sequences over rings I: periods and minimal polynomials. Journal of Cryptology, 1990, 5(2): 193

6 Kuzmin A S. The distribution of elements on cycles of linear recurrents over rings of residues. Russian Mathmatical Survey, 1992, 47(6): 219

(1996-12-09 收稿,1997-06-18 收修改稿)