Distribution of 0 and 1 in the highest level of primitive sequences over $Z/(2^e)$ (Ⅱ)

QI Wenfeng and ZHOU Jinjun
Department of Applied Mathmatics, Zhengzhou Information Engineering Institute, Zhengzhou 450002, China

Abstract The distribution of 0 and 1 is studied in the highest level a_{e-1} of primitive sequences over $Z/(2^e)$. It is proved that the proportion of 0 (or 1) in one period of a_{e-1} is between 40% and 60% for $e\geqslant 8$.

Keywords: linear recurring sequence, primitive sequence, highest levelZ sequence, distribution of 0 and 1.

LET $f(x)=x^n+c_{n-1}x^{n-1}+\cdots+c_0$ be a monic polynomial over $Z/(2^e)$. The sequence $a=(a_0, a_1, \cdots)$ satisfying the linear recursion

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

is called a linear recurring sequence over $Z/(2^e)$ generated by $f(x)$. $G(f(x))_e$ denotes the set of all sequences over $Z/(2^e)$ generated by $f(x)$ and $G'(f(x))_e=\{\boldsymbol{a}\in G(f(x))_e \mid \boldsymbol{a}\neq 0 \bmod \mathbf{2}\}$. Recursion (1) is equivalent to $f(x)\boldsymbol{a}=0=(0, 0, \cdots)$, where x is the shift operator, that is, $x\boldsymbol{a}=(a_1, a_2, a_3, \cdots)$. Sequence $\boldsymbol{a}$ over $Z/(2^e)$ has a unique binary decomposition $\boldsymbol{a}=\boldsymbol{a}_0+\boldsymbol{a}_1 2+\cdots+\boldsymbol{a}_{e-1}2^{e-1}$, where $\boldsymbol{a}_i=(a_{i0}, a_{i1}, \cdots)$ is a binary sequence with $a_{ij}=0$ or 1, and $\boldsymbol{a}_i$ is called the ith level sequence of $\boldsymbol{a}_{e-1}$ the highest level of $\boldsymbol{a}$.

For a monic polynomial $f(x)$ over $Z/(2^e)$ with degree n, if $f(0)$ (i.e. c_0) is invertible, then the period of $f(x)$ $\mathrm{per}(f(x))_e\leqslant 2^{e-1}(2^n-1)$ by ref. [1]. If $\mathrm{per}(f(x))=2^{e-1}(2^n-1)$, $f(x)$ is called a primitive polynomial over $Z/(2^e)$ with degree n and sequences in $G'(f(x))_e$ are called primitive sequences generated by $f(x)$. Ref. [2] provides a coefficient criterion for primitiveness of polynomial. Ref. [3] has shown the following entropy-preservation theorem with significance of cryptography: let $f(x)$ be a primitive polynomial over $Z/(2^e)$, $\boldsymbol{a}, \boldsymbol{b}\in G(f(x))_e$. If $\boldsymbol{a}_{e-1}=\boldsymbol{b}_{e-1}$, then $\boldsymbol{a}=\boldsymbol{b}$.

Let $f(x)$ be a primitive polynomial over $Z/(2^e)$ with degree n, $\boldsymbol{a}\in G'(f(x))_e$. Then the period $\mathrm{per}(\boldsymbol{a}_k)$ of the kth level of $\boldsymbol{a}$ is 2^kT by ref. [4], where $T=2^n-1$. By ref. [1] or [4], $x^{2^{d-1}T}-1=2^dh_d(x) \bmod f(x)$ over $Z/(2^e)$ for $1\leqslant d\leqslant e-1$, where $h_d(x)$ is a polynomial over $Z/(2^e)$ with its degree less than n and $h_d(x)\neq 0 \bmod 2$. Ref. [5] provided the following result.

Proposition A. Let $f(x)$ be a primitive polynomial over $Z/(2^e)$ with degree n, $T=2^n-1$, $\boldsymbol{a}\in G'(f(x))_e$, $d=[e/2]$, $\boldsymbol{s}=h(x)\boldsymbol{a} \bmod 2^d$. Then the proportion λ of 0 (or 1) in $\boldsymbol{a}_{e-1}$ satisfies

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

where $N(\boldsymbol{s}, 0)$ denotes the number of 0 in one period of $\boldsymbol{s}$, $h(x)=\begin{cases} h_d(x), & \text{if } e=2d, \\ h_{d+1}(x), & \text{otherwise } e=2d+1. \end{cases}$

By applying the result, ref. [5] has proved that when e is sufficiently large, most of $\boldsymbol{a}_{e-1}$ are of good distribution of 0 and 1. For example, let $e=32$ and $f(x)$ be primitive over $Z/(2^e)$. Then the proportion of sequences in $G'(f(x))_e$ with $0.498\,046\,875 \leqslant \lambda \leqslant 0.501\,953\,125$ is 99.6% at least.

In the above results, we cannot estimate the distribution of a little of $\boldsymbol{a}_{e-1}$ because it is difficult to compute the number of 0 in one period of $\boldsymbol{s} = h(x)\boldsymbol{a} \bmod 2^d$. In this note, we give an upper bound of the number of 0 in one period of primitive sequences over $Z/(2^4)$ and the proportion of 0 in one period of $\boldsymbol{a}_{e-1}$ is between 40% and 60% for $e \geqslant 8$.

First we give the generalization of Proposition A.

Theorem 1. Let $f(x)$ be a primitive polynomial over $Z/(2^e)$ with degree n, $T = 2^n - 1$, $\boldsymbol{a} \in G(f(x))_e$, $1 \leqslant d \leqslant e/2$, $\boldsymbol{s} = h_{e-d}(x)\boldsymbol{a} \bmod 2^d$. Then the proportion λ of 0 (or 1) in $\boldsymbol{a}_{e-1}$ satisfies

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

where $N(\boldsymbol{s},\ 0)$ denotes the number of 0 in one period of $\boldsymbol{s}$.

Lemma 1. Let $f(x)$ be a primitive polynomial over F_2 with degree n. $\boldsymbol{a} = (a_0,\ a_1,\ \cdots)$ and $\boldsymbol{b} = (b_0,\ b_1,\ \cdots)$ are two distinct primitive sequences generated by $f(x)$. $S_{\boldsymbol{a},\boldsymbol{b}}(u,\ v) = \{i \mid a_i = u,\ b_i = v,\ 0 \leqslant i \leqslant 2^n - 2\}$, $M_{\boldsymbol{a},\boldsymbol{b}}(u,\ v) = |S_{\boldsymbol{a},\boldsymbol{b}}(u,\ v)|$. Then $M_{\boldsymbol{a},\boldsymbol{b}}(0,\ 0) = 2^{n-2} - 1$, $M_{\boldsymbol{a},\boldsymbol{b}}(0,\ 1) = M_{\boldsymbol{a},\boldsymbol{b}}(1,\ 0) = M_{\boldsymbol{a},\boldsymbol{b}}(1,\ 1) = 2^{n-2}$.

Lemma 2. Let $f(x)$ be a primitive polynomial over F_2 with degree n, $n \geqslant 3$. $\boldsymbol{a}$, $\boldsymbol{b}$ and $\boldsymbol{c}$ are pairwise relatively distinct sequences generated by $f(x)$ and $\boldsymbol{a} + \boldsymbol{b} + \boldsymbol{c} \neq 0$. For $u,\ v,\ w \in F_2$, set $S_{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}}(u,\ v,\ w) = \{i \mid a_i = u,\ b_i = v,\ c_i = w,\ 0 \leqslant i \leqslant 2^n - 2\}$, $M_{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}}(u,\ v,\ w) = |S_{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}}(u,\ v,\ w)|$. Then

$$M_{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}}(u,\ v,\ w) = \begin{cases} 2^{n-3} - 1, & \text{if } u = v = w = 0, \\ 2^{n-3}, & \text{otherwise}. \end{cases}$$

By applying Lemma 1, Lemma 2 and the relation of leval sequences, we get the following result.

Lemma 3. Let $f(x)$ be a primitive polynomial over $Z/(2^4)$ with degree n, $n \geqslant 3$. $\boldsymbol{a}$ is a primitive sequence generated by $f(x)$ over $Z/(2^4)$. If $h_2(x) \neq 1 \bmod 2$, then the number of 0 in one period of $\boldsymbol{a}$ satisfies

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

By Theorem 1 and Lemma 3, we have the following theorem.

Theorem 2. Let $f(x)$ be a primitive polynomial over $Z/(2^e)$ with degree n, $n \geqslant 3$, $e \geqslant 8$. $\boldsymbol{a}$ is a primitive sequence generated by $f(x)$. $h_2(x)$ satisfies the conditions of Lemma 3. Then the proportion of 0 (or 1) in $\boldsymbol{a}_{e-1}$ satisfies

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

Corollary 1. The conditions are as those in Theorem 2. Then the proportion of 0 in $\boldsymbol{a}_{e-1}$ satisfies $38.281\,25\% < \lambda < 61.718\,75\%$.

To estimate λ more accurately, we shall improve Lemma 3. First we give the following Lemma 4 and Lemma 5.

Lemma 4. Let $f(x)$ be a primitive polynomial over F_2 with degree n, $n \geqslant 4$, $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$ and $\boldsymbol{d}$ are primitive sequences generated by $f(x)$. The symbol $M_{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}}(u,\ v,\ w,\ x)$ is defined as in Lemma 2. If $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$, $\boldsymbol{d}$ are pairwise relatively distinct sequences and any of $\boldsymbol{a} + \boldsymbol{b} + \boldsymbol{c}$, $\boldsymbol{a} + \boldsymbol{b} + \boldsymbol{d}$, $\boldsymbol{a} + \boldsymbol{c} + \boldsymbol{d}$, $\boldsymbol{b} + \boldsymbol{c} + \boldsymbol{d}$ and $\boldsymbol{a} + \boldsymbol{b} + \boldsymbol{c} + \boldsymbol{d}$ is not $\mathbf{0}$, then

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

Lemma 5[6]**.** Let $\boldsymbol{a}$ be a primitive sequence of degree n over $Z/(2^e)$. Then the number of 0 in one period of $\boldsymbol{a}$ satisfies $N(\boldsymbol{a},\ 0) \leqslant 2^n + 2^{n/2} - 2$.

Apllying Lemma 4, Lemma 5 and the relation among level sequences, we get the following lemma.

Lemma 6. Under the condition of Lemma 3, let $n \geqslant 4$, $h_1(x)h_2(x) \neq 1 \bmod (2,\ f(x))$, $(1 + h_1(x))h_2(x) \neq 1 \bmod (2,\ f(x))$. Then the number of 0 in one period of $\boldsymbol{a}$ satisfies

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

By Theorem 1 and Lemma 6, we have the following theorem.

Theorem 3. Let $f(x)$ be a primitive polynomial of degree n over $Z/(2^e)$, $n \geqslant 4$, $e \geqslant 8$. $\boldsymbol{a}$ is a primitive sequence over $Z/(2^e)$ generated by $f(x)$. If $h_1(x)$ and $h_2(x)$ satisfy the conditions of Lemma 6, then the proportion of 0 (or 1) in $\boldsymbol{a}_{e-1}$ satisfies

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

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

Corollary 2. The condition is as that in Lemma 3. Then the proportion λ of 0 (or 1) in $\boldsymbol{a}_{e-1}$ satisfies

(i) $40.1579\% < \lambda < 59.8421\%$ if $n \leqslant 7$;

(ii) $40.2505\% < \lambda < 59.7495\%$ if $n \geqslant 8$;

(iii) $40.6249\% < \lambda < 59.3751\%$ if $n \geqslant 30$.

Reference [5] proved that most of $\boldsymbol{a}_{e-1}$ have good ditributions. If e is sufficiently large, most of $\boldsymbol{a}_{e-1}$ have good ditributions. Corollary 2 insures other $\boldsymbol{a}_{e-1}$ against bad distributions.

Acknowledgement This work was supported by the National Natural Science Foundation of China (Grant No. 19771088) and the State Key Laboratory of Information Security, Graduate School of Chinese Academy of Science.

References

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

5 Qi Wenfeng, Zhou Jinjun, Distribution of 0 and 1 in the highest level of primitive sequences over $Z/(2^e)$, *Science in China*, Ser. A, 1997, 40(6): 606.

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

(*Received May* 18, 1997; *accepted October* 16, 1997)