Lower Bounds for the Linear Complexity of Sequences over Residue Rings

Zong-duo Dai[1]) Thomas Beth[2]) Dieter Gollmann[2])

[1]) University of Linköping, Sweden
on leave from Academia Sinica, Beijing, China

[2]) E.I.S.S., University of Karlsruhe, Germany

Abstract

Linear feedback shift registers over the ring $\mathbf{Z}_{2^e}$ can be implemented efficiently on standard microprocessors. The most significant bits of the elements of a sequence in $\mathbf{Z}_{2^e}^{\infty}$ constitute a binary pseudo-random sequence. We derive lower bounds for the linear complexity over $\mathbf{F}_2$ of these binary sequences.

1 Sequences over Residue Rings

For a positive integer e let $\mathbf{Z}_{2^e}$ denote the residue ring $\mathbf{Z}/(2^e)$, that is the set of integers $\{0, 1, \ldots, 2^e - 1\}$ with arithmetic operations carried out modulo 2^e. Computation in $\mathbf{Z}_{2^e}$ differs from computation in $\mathbf{F}_{2^e}$ in the way overflows are handled. In a polynomial basis representation of $\mathbf{F}_{2^e}$ we choose an irreducible polynomial from $\mathbf{F}_2[x]$ and thus define how overflows, i.e. terms of degree larger or equal e, are fed back, i.e. reduced to polynomials of degree less than e. In $\mathbf{Z}_{2^e}$ overflows modulo 2^e are simply discarded.

Sequences in $\mathbf{Z}_{2^e}^{\infty}$ are of particular interest from an application point of view as they can be generated very efficiently on microprocessors when e is the word length of the processor. A sequence $\alpha = (a_t)$ generated by a linear feedback shift register over $\mathbf{Z}_{2^e}$ obeys a linear recursion of the form

$$a_{t+n} = \sum_{j=0}^{n-1} c_j a_{t+j} \pmod{2^e} \quad \text{for } t \geq 0 \,,$$

where n is the length of the shift register and a_t, $c_j \in \mathbf{Z}_{2^e}$ (see Fig.1). Due to a result by Ward [7] the upper bound for the period of linear recursive sequences of degree n over $\mathbf{Z}_{2^e}$ is $2^{e-1}(2^n - 1)$.

Definition 1.1 Linear recursive sequences of degree n over $\mathbf{Z}_{2^e}$ with period $2^{e-1}(2^n - 1)$ are called maximal length linear sequences, in short MLL-sequences ([1,4]).

I.B. Damgard (Ed.): Advances in Cryptology - EUROCRYPT '90, LNCS 473, pp. 189-195, 1991.

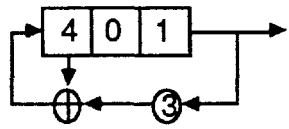

Figure 1: A linear feedback shift register over $\mathbf{Z}_8$ with feedback polynomial $f(x) = x^3 - x^2 - 3$

The period of a polynomial $f(x) \in \mathbf{Z}_{2^e}[x]$ is defined as follows.

Definition 1.2 Let $(f(x))$ denote the ideal in $\mathbf{Z}_{2^e}[x]$ generated by some polynomial $f(x) \in \mathbf{Z}_{2^e}[x]$. The period of $f(x)$ is given by

$$\mathrm{per}(f(x)) := \min\{T \geq 1 | \exists d \geq 0 : x^{T+d} - x^d \in (f(x))\} .$$

A polynomial $f(x) \in \mathbf{Z}_{2^e}[x]$ is called primitive if it has period $2^{e-1}(2^n - 1)$.

2 Binary Sequences Generated from Sequences over Residue Rings

Binary sequences α_i, $0 \leq i < e$, can be derived from sequences α over $\mathbf{Z}_{2^e}$ by

$$a_t = \sum_{i=0}^{e-1} a_{ti} 2^i , \quad a_{ti} \in \{0, 1\} ,$$
$$\alpha_i = (a_{0i}, a_{1i}, \ldots, a_{ti}, \ldots) .$$

As an example, the sequence $(1, 0, 4, 7, \ldots) \in \mathbf{Z}_{2^e}^{\infty}$ is represented by

$$\alpha_0 = (1, 0, 0, 1, \ldots)$$
$$\alpha_1 = (0, 0, 0, 1, \ldots)$$
$$\alpha_2 = (0, 0, 1, 1, \ldots) .$$

Let L be the left shift operator on the sequences $\alpha \in \mathbf{Z}_{2^e}^{\infty}$. For any polynomial

$$f(x) = \sum_{i=0}^{n} c_i x^i \in \mathbf{Z}_{2^e}[x]$$

define

$$f(L)\alpha := \sum_{i=0}^{n} c_i L^i \alpha .$$

Definition 2.1 The minimal polynomial of α is the monic polynomial $f(x) \in \mathbf{Z}_{2^e}[x]$ of lowest degree so that $f(L)\alpha = 0$.

The polynomial $f(x)$ can be decomposed into polynomials $f_i(x) \in \mathbf{F}_2[x]$ by

$$f(x) = \sum_{i=0}^{e-1} f_i(x) 2^i .$$

If $f(x)$ is a primitive polynomial then $f_0(x)$ is a primitive polynomial in $\mathbf{F}_2[x]$ and the roots of $f_0(x)$ have period $2^n - 1$.

We quote the following results relating to the period of binary sequences derived from MLL-sequences over $\mathbf{Z}_{2^e}$ ([1,4,7]).

Theorem 2.1 Let α be a MLL-sequence over $\mathbf{Z}_{2^e}$ with minimal polynomial $f(x)$ of degree n. We have

$$\mathrm{per}(\alpha_{e-1}) = \mathrm{per}(\alpha) = 2^{e-1}(2^n - 1) .$$

Let $f(x) \in \mathbf{Z}_{2^e}[x]$ be a primitive polynomial of degree n. There exist

$$2^{(e-1)n}(2^n - 1)$$

different MLL-sequences with minimal polynomial $f(x)$.

Let α and β be two MLL-sequences with minimal polynomial $f(x)$. The probability that α is a cyclic shift of β is $2^{-(n-1)(e-1)}$.

Dai [1] and Huang [4] also give upper bounds for the linear complexity of the sequence α_{e-1}. In this paper we will bound the linear complexity from below.

3 Main Lemma

Let $\alpha \in \mathbf{Z}_{2^e}^{\infty}$ be a MLL-sequence generated by some LFSR over $\mathbf{Z}_{2^e}$. A new element of the sequence α_r will be computed from the previous elements of this sequence, from the lower bit sequences, and from the carries generated by the lower bit sequences. Let β_{ij} denote the sequence of carries propagated from sequence α_i to sequence α_j and let

$$\Phi_k(x_0, x_1, \ldots, x_n) := \sum_{0 \le i_1 < i_2 < \cdots < i_k \le n} x_{i_1} x_{i_2} \cdots x_{i_k}$$

be the symmetric function of order k applied to n arguments ([6], p. 182 ff). Fig. 2 describes the decomposed computation of the sequences α_r and β_{ij}. Note that the coefficients of $f_0(x)$ act as a filter for the inputs to the Φ_k, i.e. for

$$f_0(x) = x^n + \sum_{i=0}^{n-1} c_{0,i} x^i$$

we have

$$\beta_{ij} = \Phi_{2^j}(c_{00}\alpha_i, c_{01} L\alpha_i, \ldots, c_{0,n-1} L^{n-1}\alpha_i) .$$

Let α be a MLL-sequence with minimal polynomial $f(x)$ of degree n and let θ be a root of $f_0(x)$. For any

$$e = \sum_{i=0}^{n-1} e_i 2^i \ , \ e_i \in \{0, 1\} \ ,$$

define the weight of $\rho = \theta^e$ as

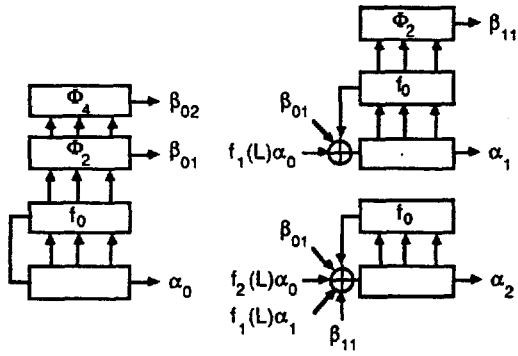

Figure 2: The carries in the generation of a sequence in $\mathbf{Z}_8^\infty$

$$w(\rho) = \sum_{i=0}^{n-1} e_i \in \mathbf{Z} \ .$$

Let $\mathbf{K}$ be the algebraic closure of $\mathbf{F}_2$. Define

$$g_m^+(x) = \prod_{\rho, w(\rho)=m} (x-\rho) \ ,$$

$$g_m^-(x) = \prod_{\rho, w(\rho)<m} (x-\rho) \ ,$$

and

$$v_\rho = (1, \rho, \rho^2, \ldots, \rho^i, \ldots) \in \mathbf{K}^\infty \ .$$

We will sketch the main step in deriving lower bounds for the linear complexity of α_{e-1}. A detailed account can be found in [2]. The sequences α_r will be decomposed into

$$\alpha_r = \alpha_r^+ + \alpha_r^- \ ,$$

where α_r^+ and α_r^- are chosen so that the minimal polynomial of α_r^+, is a divisor of $g_{2^r}^+(x)$ and the minimal polynomial of α_r^- and is a divisor of $g_{2^r}^-(x)$. Hence, we have for the linear complexity $\mathcal{L}(\alpha_r)$ of α_r

$$\mathcal{L}(\alpha_r) = \mathcal{L}(\alpha_r^+) + \mathcal{L}(\alpha_r^-) \ .$$

We will bound the linear complexity of α_r from below by determining the sequences α_r^+, $0 \le r \le e-1$. Writing $\beta_{ij} = \beta_{ij}^+ + \beta_{ij}^-$ as above, the sequence α_r^+ can be related to the carry sequences $\beta_{i,r-i}^+$ and we obtain finally

Lemma 3.1 Let $\alpha \in \mathbf{Z}_{2^e}^\infty$ be a MLL-sequence with minimal polynomial $f(x) \in \mathbf{Z}_{2^e}[x]$ of degree n, let θ be a root of $f_0(x)$. We have for any r, $2^r \le n$,

$$\alpha_r^+ = L^\tau \sum_{\rho, w(\rho)=2^r} v_\rho \ .$$

for some $\tau \ge 0$.

4 Lower bounds for the linear complexity

Let $m(x)$ be the minimal polynomial of α_{e-1}. The degree of $m(x)$ will be examined by means of the discriminant of $f(x)$ and Lemma 3.1:

Definition 4.1 The discriminant of $f(x)$, $\Delta_f(x)$, is given by

$$\Delta_f(x) \equiv \begin{cases} h_f(x) & (\mathrm{mod}\ (f_0(x),2)) \quad \text{if } e=2 \\ h_f(x)(h_f(x)+1) & (\mathrm{mod}\ (f_0(x),2)) \quad \text{if } e \geq 3 \end{cases}$$

with $h_f(x)$ determined by

$$x^{2^n-1} \equiv 1 + 2h_f(x) \quad (\mathrm{mod}\ (f(x),2^2)).$$

Lemma 4.1 ([4]) For any e, r, $2 \leq r < e-1$, we have

$$\left(L^{2^n-1}-1\right)^{2^{e-2}-2^{r-1}} \alpha_{e-1}^{+} = (\Delta_f(L)\alpha_0)\alpha_r^{+} .$$

With these preparations we embark on the analysis of the sequences α_r^{+}. We may assume

$$\alpha_0 = \sum_{\rho, w(\rho)=1} v_\rho = \sum_{i=0}^{n-1} v_{\theta^{2^i}} ,$$

hence

$$\Delta_f(L)\alpha_0 = \sum_{i=0}^{n-1} \Delta_f(\theta^{2^i}) v_{\theta^{2^i}} ,$$

and by Lemma 3.1

$$(\Delta_f(L)\alpha_0)\alpha_r^{+} = \sum_{\rho, w(\rho)=2^r+1} \sigma_\rho v_\rho \tag{1}$$

with

$$\sigma_\rho = \sum_{j=1}^{2^r+1} \Delta_f(\theta^{2^{i_j}}) \quad \text{for} \quad \rho = \theta^{2^{i_1}+2^{i_2}+\cdots+2^{i_{2^r+1}}} .$$

Write

$$\sigma_r(x) = \prod_{\substack{\rho, w(\rho)=2^r+1 \\ \sigma_\rho \neq 0}} (x-\rho) .$$

The root θ of $f_0(x)$ has period 2^n-1, therefore

$$\sigma_r(x) \mid \left(x^{2^n-1}-1\right) .$$

We define $M := \min(e-1, \log_2(n-1))$ and derive from Lemma 4.1 and from (1)

$$\sigma_r(x)^{2^{e-2}-2^{r-1}+1} \mid m(x), \ 2 \leq r \leq M .$$

This gives

$$\mathcal{L}(\alpha_{e-1}^{+}) \geq \sum_{k=2}^{M} (2^{e-2}-2^{k-1}+1) \cdot \deg \sigma_k(x) . \tag{2}$$

With $\Delta = \Delta_f(\theta)$ and

$$\mathcal{N}_k(\Delta) = \left\{ (i_1, \ldots, i_{2^k+1}) \mid 0 \leq i_1 < \cdots < i_{2^k+1} < n \ , \sum_{j=1}^{2^k+1} \Delta^{2^{i_j}} \neq 0 \right\}$$

we may rewrite (2) as follows,

Theorem 4.2 Let $\alpha \in \mathbf{Z}_{2^e}^{\infty}$ be a ML-sequence and let M be defined as above. We have

$$\mathcal{L}(\alpha_{e-1}) \geq \sum_{k=2}^{M} (2^{e-2} - 2^{k-1} + 1)|\mathcal{N}_k(\Delta)| \ .$$

It can be shown that

$$|\mathcal{N}_k(\Delta)| \leq \binom{n}{2^k+1}$$

for $2^k < n$. In fact, $|\mathcal{N}_k(\Delta)|$ is very close to this upper bound for any Δ. We consider a special case where $|\mathcal{N}_k(\Delta)|$ obtains its maximal value.

Theorem 4.3 If $\mathbf{F}_2(\Delta) = \mathbf{F}_{2^d}$ and $\left\{\Delta, \Delta^2, \ldots, \Delta^{2^{d-1}}\right\}$ is a normal basis of $\mathbf{F}_2(\Delta)$ over $\mathbf{F}_2$, then we have

$$\mathcal{L}(\alpha_{e-1}) \geq \begin{cases} \sum_{k=2}^{\lfloor \log_2 n-1 \rfloor} (2^{e-2} - 2^{k-1} + 1)\binom{n}{2^k+1} & \text{if } n < 2^{e-1} \\ \binom{n}{2^{e-1}} + \sum_{k=2}^{e-2} (2^{e-2} - 2^{k-1} + 1)\binom{n}{2^k+1} & \text{if } n \geq 2^{e-1} \ . \end{cases}$$

Proof. It suffices to prove for $k < e-1$

$$\Delta(\underline{i}) = \sum_{j=1}^{2^k+1} \Delta^{2^{i_j}} \neq 0$$

for any $\underline{i} = (i_1, i_2, \ldots, i_{2^k+1})$, $0 \leq i_1 < i_2 < \cdots < i_{2^k+1} < n$. In fact, if $\mathbf{F}_2(\Delta) = \mathbf{F}_{2^d}$, $\Delta(\underline{i})$ can be reduced to

$$\Delta(\underline{i}) = \Delta^{2^{k_1}} + \Delta^{2^{k_2}} + \cdots + \Delta^{2^{k_t}} \ ,$$

where $0 \leq k_1 < k_2 < \cdots < k_t < d$, $t \equiv 1 \pmod 2$. Since $\left\{\Delta, \Delta^2, \ldots, \Delta^{2^{d-1}}\right\}$ is a normal basis we get $\Delta(\underline{i}) \neq 0$. ∎

The lower bound given in Theorem 4.3 is quite large. For example, if $n = 2(2^k+1) < 2^{e-1}$ for some k, just one term in the right hand sum will be, ref. [5],

$$(2^{e-2} - 2^{k-1} + 1)\binom{n}{2^k+1} \geq 2^{e-3}\binom{n}{\frac{n}{2}} \geq 2^{e-3}\frac{\sqrt{\pi}}{2} \cdot \frac{2^{n+1}}{\sqrt{2\pi n}} = \frac{2^{n+e-3}}{\sqrt{2n}} \ .$$

MLL-sequences have period $2^{e-1}(2^n - 1)$ so we get

$$L(\alpha_{e-1}) \geq \frac{2^{n+e-1}}{4\sqrt{2n}} \geq \frac{\text{per}(\alpha_{e-1})}{4\sqrt{2(\log(\text{per}(\alpha_{e-1})) - e + 1)}} \ .$$

5 Conclusions

Binary sequences generated from MLL-sequences over Z_{2^e} are of particular interest from an application point of view as they can be implemented very efficiently on microprocessors when e is the word length. We have shown that the lower bounds for the linear complexity of these sequences are reasonably high. However, the reader should be aware that there exist algorithms to reconstruct sequences generated by linear congruences from truncated outputs [3] if the congruence is known. Thus, the results on sequences over residue rings rather should help to evaluate their contribution to more sophisticated designs than be taken as an argument for their security.

References

[1] Z.D.Dai, *The Binary Sequences Derived from the Sequences over the Integral Residue Ring $Z/(2^e)$. I*, Internal Report, Academia Sinica, Beijing, China

[2] Z.D.Dai, D.Gollmann *Lower Bounds for the Linear Complexity of Sequences over Residue Rings*, E.I.S.S. Report, No.90/7, 1990

[3] A.M.Frieze, J.Hastad, R.Kannan, J.C.Lagarias, A.Shamir, *Reconstructing Truncated Integer Variables Satisfying Linear Congruences*, SIAM J. Comput., Vol.17, No.2, pp.262-280, April 1988

[4] M.Q.Huang, *The Binary Sequences Derived from the Sequences over the Integral Residue Ring $Z/(2^e)$. II*, Internal Report, Academia Sinica, Beijing, China

[5] W.Peterson, E.Weldon, *Error Correcting Codes*, 2nd ed., M.I.T.Press, Cambridge, Berlin, 1986

[6] R.A.Rueppel, *Analysis and Design of Stream Ciphers*, Springer, Cambridge, Mass., 1972

[7] M.Ward, *The arithmetical theory of linear recurring sequences*, Transactions of the American Mathematical Society, Vol.35, pp.600-628, July 1933