J. Cryptology (1992) 5: 193–207

Journal of Cryptology

Binary Sequences Derived from ML-Sequences over Rings I: Periods and Minimal Polynomials*

Zong-Duo Dai

Department of Mathematics, Royal Holloway and Bedford New College, University of London, Egham Hill, Egham, Surrey TW20 0EX, England

Communicated by Rainer A. Rueppel

Received 8 May 1991 and revised 29 November 1991

Abstract. We derive pseudorandom binary sequences from maximal length sequences over the integral residue rings. We prove that these derived binary sequences have guaranteed large periods, and we also obtain upper bounds on their minimal polynomials in the sense of the partial order defined by divisibility.

Key words. Maximal length sequences, Integral rings, Periods, Minimal polynomials.

1. Introduction

The so-called integral residue ring Z_{2^e} is the set of 2^e integers $\{0, 1, 2, \ldots, 2^e - 2, 2^e - 1\}$ with arithmetic operations (addition, subtraction, and multiplication) carried out modulo 2^e. Any element b belonging to Z_{2^e} has a binary decomposition as $b = \sum_{i=0}^{e-1} b_i 2^i$, $b_i \in \{0, 1\}$, where b_i is called the ith *level bit* of b, and b_{e-1} the highest level (or the most significant) bit of b. Note that b is odd if $b_0 = 1$. If a_t is an element in Z_{2^e} with the binary decomposition $a_t = \sum_{i=0}^{e-1} a_{t,i} 2^i$, then the sequence $\alpha = \{a_t\}_0^\infty$ of elements in Z_{2^e} has a binary decomposition $\alpha = \sum_{i=0}^{e-1} \alpha_i 2^i$, where $\alpha_i = \{a_{t,i}\}_{t=0}^\infty$ is a binary sequence called the ith *level component* of α.

We start by considering a maximal length (ML-) sequence (which is defined in the next section) of elements in Z_{2^e}, and we may then derive a binary sequence by picking up the bits at its highest level, or by mixing the bits at the highest level with the bits at the lower levels. This can provide a convenient way of generating pseudorandom binary sequences on general-purpose microprocessors when e is chosen as the processor word length. Now as regards the cryptologic security: the generator is a linear congruential generator and cryptanalytic techniques are avail-

* This research was supported by SERC Grant GR/F 72727. The author is on leave from the Department of Mathematics, Graduate School, Academia Sinica, 3908 Beijing, People's Republic of China.

able at least when the coefficients are known [2]. These techniques suppose that the output sequence is truncated down to the bits at a certain number of higher levels and it seems unlikely that they are practicable when only the highest bits or its mixture with the lower ones are available. There is always the worry that we may obtain a dangerously short period or small linear complexity. In this paper we show that the derived binary sequences have guaranteed large periods, and we also present upper bounds (in the sense of the partial order defined by divisibility) on their minimal polynomials [1, p. 201], [4, p. 419], [5, p. 26], from which upper bounds to their linear complexities [5, pp. 32, 182] (or linear equivalences [1, p. 199]) can be found. Computer results demonstrate that the upper bounds are tight in simple cases. We leave the lower bounds of their linear complexities and some other issues to be discussed in later papers.

2. ML-Sequences and Primitive Polynomials Over Z_{2^e}

The periods of the linear recursion sequences over Z_{2^e} were studied by Ward [6]. In this section we have a brief review on Ward's work, and then introduce the so-called ML-sequences and primitive polynomials over Z_{2^e}.

In the following, the equation $a(x) = b(x) \pmod{g(x), 2^r}$ means that there exist two polynomials $h_1(x)$ and $h_2(x)$ with integer coefficients such that $a(x) - b(x) = h_1(x)g(x) + h_2(x)2^r$, and the notation $Z_{2^e}[x]$ is the set of all polynomials with a variable x and coefficients in Z_{2^e}.

Let $\alpha = \{a_t\}_{t=0}^{\infty}$ be a sequence of elements in Z_{2^e}, obeying the linear recursion of the form $a_{t+n} = -\sum_{j=0}^{n-1} c_j a_{t+j} \pmod{2^e}, \forall t \geq 0$, with $(a_0, a_1, \ldots, a_{n-1})$ specifying the initial condition, and with c_j constants. As usual, we say that the polynomial $f(x) = x^n + \sum_{j=0}^{n-1} c_j x^j$ is a *characteristic polynomial* of α, and α is a *linear-recursion sequence of degree n* over Z_{2^e} *generated* by $f(x)$. Let $c_j = \sum_{i=0}^{e-1} c_{j,i} 2^i$ be the binary decomposition of c_j; then $f(x)$ has the binary decomposition $f(x) = \sum_{i=0}^{e-1} f_i(x)2^i$, where $f_i(x) = \sum_{j=0}^{n} c_{j,i} x^j$ is called the ith *level component* of $f(x)$.

It was proved [6] that the least period of the linear recursion sequence α of degree n over Z_{2^e}, denoted by $\mathrm{per}(\alpha)$, is a factor of $2^{e-1}\,\mathrm{per}(f_0(x))$; here $\mathrm{per}(f_0(x))$, called the period (or exponent) of the polynomial $f_0(x) \in Z_2[x]$, is defined to be the least positive integer T satisfying $x^{T+t_0} = x^{t_0} \pmod{f_0(x), 2}$ for some nonnegative integers t_0. The period $\mathrm{per}(\alpha)$ is upper bounded by $2^{e-1}(2^n - 1)$, and the upper bound $2^{e-1}(2^n - 1)$ is attained only if $f_0(x)$ is primitive over the binary field Z_2. Moreover, if it is assumed that $f_0(x)$ is primitive over Z_2, then the upper bound $2^{e-1}(2^n - 1)$ is attained if and only if at least one of the initial n elements $a_0, a_1, \ldots, a_{n-1}$ is odd (or equivalently, $\alpha_0 \neq 0$, where 0 denotes the null sequence), and $f(x)$ satisfies the following condition:

$$f_1(x) \neq \begin{cases} q(x)^{-1}r(x) & \pmod{f_0(x), 2} \quad \text{if } e = 2, \\ q(x)^{-1}(r(x) + 1) & \pmod{f_0(x), 2} \quad \text{if } e \geq 3, \end{cases} \tag{1}$$

where $q(x)$ and $r(x)$ are polynomials with integer coefficients such that

$$x^{2^{n-1}} - 1 = f_0(x)q(x) + 2r(x) \pmod{2^e}. \tag{2}$$

For later use it is convenient to notice that condition (1) on $f(x)$ is equivalent to

$$\Delta_f(x) \neq 0 \pmod{f_0(x), 2},$$

where $\Delta_f(x)$ is the polynomial with binary coefficients of degree less than n determined by

$$\Delta_f(x) = \begin{cases} h_f(x) & \pmod{f_0(x), 2}, \quad e = 2, \\ h_f(x)(h_f(x) + 1) & \pmod{f_0(x), 2}, \quad e \geq 3, \end{cases} \tag{3}$$

and $h_f(x)$ is the polynomial with binary coefficients of degree less than n determined by

$$h_f(x) = r(x) + q(x)f_1(x) \pmod{f_0(x), 2}.$$

We call $h_f(x)$ the half-discriminant of $f(x)$, and $\Delta_f(x)$ the *discriminant* of $f(x)$. A linear-recursion sequence α of degree n over Z_{2^e} is called an *ML-sequence* if its period attains the upper bound $2^{e-1}(2^n - 1)$; and a monic polynomial $f(x)$ (i.e., with the leading coefficient 1) of degree n over Z_{2^e} is called a *primitive polynomial* if $f_0(x)$ is primitive over the binary field Z_2, and $\Delta_f(x) \neq 0 \pmod{f_0(x), 2}$. When $e = 1$, these two introduced concepts become just the well-known concepts of ML-sequence and primitive polynomial over the binary field Z_2, respectively. It is clear that if $f(x)$ is primitive over Z_{2^e}, then $\sum_{i=0}^{r-1} f_i(x)2^i$ is primitive over $Z_{2^r}, 1 \leq r \leq e$.

Ward's results can be rewritten as follows.

Proposition 1 [6]. *Let $f(x) \in Z_{2^e}[x]$ be monic of degree n with binary decomposition $f(x) = \sum_{i=0}^{e-1} f_i(x)2^i$, and let α be a sequence generated by $f(x)$ over Z_{2^e} with binary decomposition $\alpha = \sum_{i=0}^{e-1} \alpha_i 2^i$. Then*

1. *α is an ML-sequence of degree n if and only if $f(x)$ is primitive over Z_{2^e}, and $\alpha_0 \neq 0$.*
2. *If α is an ML-sequence of degree n, then $\sum_{i=0}^{r-1} \alpha_i 2^i$, $1 \leq r \leq e$, is also an ML-sequence of degree n over Z_{2^r}, generated by $\sum_{i=0}^{r-1} f_i(x)2^i$.*

A large number of ML-sequences over Z_{2^e} can be generated. In fact from Proposition 1 we have

Corollary 1.

1. *For any given primitive polynomial $f(x)$ of degree n over Z_{2^e}, the total number of ML-sequences over Z_{2^e} generated by $f(x)$ is $2^{(n-1)(e-1)}$. The ML-sequences generated by $f(x)$, with randomly chosen initial n elements (with the restriction that at least one of $a_0, a_1, \ldots, a_{n-1}$ is odd), will be cyclicly inequivalent with the probability equal to $1 - 2^{-(n-1)(e-1)}$.*
2. *Any two ML-sequences generated by two different primitive polynomials over Z_{2^e} will be different.*
3. *Given a primitive polynomial $f_0(x)$ of degree n over Z_2, the total number of primitive polynomials over Z_{2^e} with $f_0(x)$ being its* 0th *component is $2^n - 1$ if $e = 2$, and $2^{n(e-2)+1}(2^{n-1} - 1)$ if $e \geq 3$.*

3. Polynomial Operators

Let $\beta = \{b_t\}_{t=0}^{\infty}$ be a sequence over Z_{2^e}, let $f(x) = \sum_{i=0}^{n} c_i x^i$ be a polynomial with coefficients in Z_{2^e}, and define $f(x)\beta = \sum_{i=0}^{n} c_i x^i \beta \pmod{2^e}$, where $x^i\beta$ is the translate of β by i steps, i.e., $x^i\beta = \{b_{i+t}\}_{t=0}^{\infty}$, and the sequence multiplication with constants c_i and sequence addition are performed component by component. Now applying $f(x)$ on β, we get a sequence $f(x)\beta$, which is the corresponding linear combination of the translates of β, specified by $f(x)$. Hence polynomials become operators on sequences, which is convenient in studying linear recursion sequences.

In the following, for any sequence $\beta = \{b_t\}_{t=0}^{\infty}$ and $\gamma = \{c_t\}_{t=0}^{\infty}$ over Z_{2^e}, the equation $\beta = \gamma \pmod{2^e}$ means $b_t = c_t \pmod{2^e}$ $\forall t$. With the polynomial operators, the fact that α is generated by $f(x)$ over Z_{2^e} can be expressed as $f(x)\alpha = 0 \pmod{2^e}$.

The minimal polynomial of a binary sequence γ, which is denoted by $m(\gamma, x)$, is defined to be the characteristic polynomial of the least possible degree. The following lemma concerning the minimal polynomials could be proved easily by means of the introduced polynomial operators; where by the notation $c^a(x)|d(x)$ we mean that $d(x)$ is divisible by $c^a(x)$, and by the notation $c^a(x)\|d(x)$ we mean that $d(x)$ is divisible by $c^a(x)$, but not by $c^{a+1}(x)$.

Lemma 1. *Let β, γ be two sequences over Z_2, let $g(x) \in Z_2[x]$, and let $g(x)\beta = \gamma \pmod 2$, moreover let $p(x) \in Z_2[x]$ be irreducible and $p(x)|m(\gamma, x)$, where $m(\gamma, x)$ is the minimal polynomial of γ. If $p^b(x)\|m(\gamma, x)$ and $p^a(x)\|g(x)$, then $p^{b+a}(x)\|m(\beta, x)$.*

Proof. Omitted. □

4. Periods of α_r

In this section let $f(x)$ be a primitive polynomial of degree n over Z_{2^e} with binary decomposition $f(x) = \sum_{i=0}^{e-1} f_i(x)2^i$, and let α be an ML-sequence generated by $f(x)$ over Z_{2^e} with binary decomposition $\alpha = \sum_{i=0}^{e-1} \alpha_i 2^i$. It follows from Proposition 1 that for any r, $0 \le r < e$, the sequence $\sum_{i=0}^{r} \alpha_i 2^i$ is an ML-sequence generated by $\sum_{i=0}^{r} f_i(x)2^i$ over $Z_{2^{r+1}}$. Hence $\mathrm{per}(\sum_{i=0}^{r} \alpha_i 2^i)$ equals $2^r(2^n - 1)$, and in particular $\mathrm{per}(\alpha_r)$ divides $2^r(2^n - 1)$. In this section it will be proved that $\mathrm{per}(\alpha_r)$ attains the maximal possible value $2^r(2^n - 1)$. We start with some lemmas.

Lemma 2.

$$m(\alpha_0, x) = m(h_f(x)\alpha_0, x) = m(\Delta_f(x)\alpha_0, x) = f_0(x),$$

where $m(\alpha_0, x)$ is the minimal polynomial of α_0 and so on.

Proof. We have

$$f(x)\alpha = 0 \pmod{2^e},$$

hence

$$f_0(x)\alpha_0 = 0 \pmod 2.$$

We know from Proposition 1 that $\alpha_0 \neq 0$, and $f_0(x)$ is primitive over Z_2, so $m(\alpha_0, x) = f_0(x)$. We see also from Proposition 1 that $\Delta_f(x) \neq 0 \pmod{f_0(x), 2}$, and then from (3) $h_f(x) \neq 0 \pmod{f_0(x), 2}$, so $m(h_f(x)\alpha_0, x) = m(\Delta_f(x)\alpha_0, x) = f_0(x)$. □

Lemma 3.

$$(x^{2^{r-1}(2^n-1)} - 1)\alpha_r = \begin{cases} h_f(x)\alpha_0 \pmod 2, & r = 1, \\ \Delta_f(x)\alpha_0 \pmod 2, & r \geq 2. \end{cases}$$

Proof. We have from (2) that

$$\begin{aligned} x^{2^n-1} &= 1 + f_0(x)q(x) + 2r(x) \\ &= 1 + [f_0(x) + 2f_1(x)]q(x) + 2[r(x) - f_1(x)q(x)] \\ &= 1 + 2h_f(x) \pmod{f(x), 2^2}. \end{aligned} \tag{4}$$

Applying both sides to α we obtain

$$x^{2^n-1}\alpha = \alpha + 2h_f(x)\alpha \pmod{2^2},$$

which leads to $x^{2^n-1}\alpha_0 = \alpha_0 \pmod 2$, and hence to $x^{2^n-1}\alpha_0 = \alpha_0$. So we have

$$\begin{aligned} (x^{2^n-1} - 1)\alpha_1 2 &= (x^{2^n-1} - 1)(\alpha_0 + \alpha_1 2) \\ &= (x^{2^n-1} - 1)\alpha \\ &= 2h_f(x)\alpha \\ &= 2h_f(x)\alpha_0 \pmod{2^2}, \end{aligned}$$

which, after cancellation of the factor 2, leads to the first equation in this lemma.

Squaring both sides of (4) we get

$$\begin{aligned} x^{2(2^n-1)} &= 1 + 2^2 h_f(x)[h_f(x) + 1] \\ &= 1 + 2^2\Delta_f(x) \pmod{f(x), 2^3}, \end{aligned}$$

and, by continuing the squaring processes, we get, in general for any $r \geq 2$,

$$x^{2^{r-1}(2^n-1)} = 1 + 2^r\Delta_f(x) \pmod{f(x), 2^{r+1}}.$$

As above, applying both sides on α we obtain

$$x^{2^{r-1}(2^n-1)}\alpha = \alpha + 2^r\Delta_f(x)\alpha \pmod{2^{r+1}},$$

which leads to

$$x^{2^{r-1}(2^n-1)} \sum_{j=0}^{r-1} \alpha_j 2^j = \sum_{j=0}^{r-1} \alpha_j 2^j \pmod{2^r},$$

and hence to

$$x^{2^{r-1}(2^n-1)}\alpha_j = \alpha_j, \qquad j < r,$$

and then to

$$(x^{2^{r-1}(2^n-1)} - 1)\alpha_r 2^r = (x^{2^{r-1}(2^n-1)} - 1)\sum_{j=0}^{r} \alpha_j 2^j = (x^{2^{r-1}(2^n-1)} - 1)\alpha$$

$$= 2^r \Delta_f(x)\alpha = 2^r \Delta_f(x)\alpha_0 \pmod{2^{r+1}},$$

which, by cancelling the factor 2^r, leads to the second equation in this lemma. □

Since $f_0^{2^{r-1}}(x) \| (x^{2^n-1} - 1)^{2^{r-1}}$ it follows from Lemmas 1–3 that

Corollary 2. *The minimal polynomial $m(\alpha_r, x)$ of α_r is divisible by $f_0^{1+2^{r-1}}(x)$, but not by $f_0^{2+2^{r-1}}(x)$, i.e., $f_0^{1+2^{r-1}}(x) \| m(\alpha_r, x)$.*

We see from Corollary 2 that $\mathrm{per}(f_0^{1+2^{r-1}}(x)) | \mathrm{per}(m(\alpha_r, x))$, since $\mathrm{per}(m(\alpha_r, x)) = \mathrm{per}(\alpha_r)$, so it follows that $\mathrm{per}(f_0^{1+2^{r-1}}(x)) | \mathrm{per}(\alpha_r)$. Since $\mathrm{per}(f_0^{1+2^{r-1}}(x)) = 2^r(2^n - 1)$ we have $2^r(2^n - 1) | \mathrm{per}(\alpha_r)$, which together with $\mathrm{per}(\alpha_r) | 2^r(2^n - 1)$ leads to

Theorem 1. $\mathrm{per}(\alpha_r) = 2^r(2^n - 1)$, $0 \le r < e$, *where* $\mathrm{per}(\alpha_r)$ *is the least period of* α_r.

5. Upper Bounds on the Minimal Polynomial $m(\alpha_r, x)$ of α_r

In this section let $f(x)$ be a primitive polynomial of degree n over Z_{2^e} with binary decomposition $f(x) = \sum_{i=0}^{e-1} f_i(x)2^i$, and let α be a sequence (not necessarily an ML-sequence) generated by $f(x)$ over Z_{2^e} with binary decomposition $\alpha = \sum_{i=0}^{e-1} \alpha_i 2^i$. An upper bound $G_r(x)$ of $m(\alpha_r, x)$ and an improved one $G_r^*(x)$ will be given, in the sense of the partial ordering defined by divisibility.

5.1. *Carry Sequences*

In this subsection we show how α_r is defined iteratively in terms of the so-called carry sequences $\beta_{r,j}$ which is defined in the following lemma.

Lemma 4. *With its initial elements $a_0, a_1, \ldots, a_{n-1}$, the binary component sequences α_r, $0 \le r \le e - 1$, of α can be defined alternatively in the following way.*

First α_0 can be deduced by the equation $f_0(x)\alpha_0 = 0 \pmod 2$. In general, assume that $\beta_{i,j}$, $0 \le i < r$, $0 \le i + j < e$, and α_i, $0 \le i \le r$, have been defined, and let $\beta_{r,j}$, $0 \le j < e - r$, be the binary sequences defined by

$$\sum_{0 \le i \le r} f_{r-i}(x) \cdot \alpha_i + \sum_{0 \le i < r} \beta_{i,r-i} = \sum_{0 \le j < e-r} \beta_{r,j} 2^j \pmod{2^{e-r}}. \tag{5}$$

Then α_{r+1} can be deduced by the following equation:

$$f_0(x)\alpha_{r+1} = \sum_{0 \le i < r+1} f_{r+1-i}(x)\alpha_i + \sum_{0 \le i < r+1} \beta_{i,r+1-i} \pmod 2. \tag{6}$$

Proof. The equation for α_0 came from Lemma 2. We claim, for r, $0 \le r < e$, that

$$\sum_{l > r} \left[\sum_{0 \le i \le l} f_{l-i}(x)\alpha_i + \sum_{0 \le i \le r} \beta_{i,l-i} \right] 2^l = 0 \pmod{2^e}, \tag{7}$$

and hence

$$\left[\sum_{0\le i\le r+1} f_{r+1-i}(x)\alpha_i + \sum_{0\le i\le r} \beta_{i,r+1-i}\right] 2^{r+1} = 0 \pmod{2^{r+2}},$$

which, by cancelling the factor 2^{r+1}, leads to (6).

We prove (7) by induction on r. For $k = 0$, (7) is obtained as follows:

$$\sum_{l>0}\left[\sum_{0\le i\le l} f_{l-i}(x)\alpha_i + \beta_{0,l}\right] 2^l = f_0(x)\alpha_0 + \sum_{l>0}\sum_{0\le i\le l} f_{l-i}(x)\alpha_i 2^l$$
$$= f(x)\alpha = 0 \pmod{2^e}.$$

Assume (7) is true for $r = k-1$; then substituting (5) with $r = k$ into (7) with $r = k-1$ we obtain

$$0 = \left[\sum_{0\le i\le k} f_{k-i}(x)\alpha_i + \sum_{0\le i\le k-1} \beta_{i,k-1}\right] 2^k$$
$$+ \sum_{l>k}\left[\sum_{0\le i\le l} f_{l-i}(x)\alpha_i + \sum_{0\le i\le k-1} \beta_{i,l-i}\right] 2^l$$
$$= \sum_{0\le j<e-k} \beta_{k,j} 2^{k+j} + \sum_{l>k}\left[\sum_{0\le i\le l} f_{l-i}(x)\alpha_i + \sum_{0\le i\le k-1} \beta_{i,l-i}\right] 2^l$$
$$= \sum_{l>k}\left[\sum_{0\le i\le l} f_{l-i}(x)\alpha_i + \sum_{0\le i\le k} \beta_{i,l-i}\right] 2^l \pmod{2^e},$$

which shows that (7) is true for $r = k$. □

In order to describe $\beta_{r,j}$ by operations modulo 2 we need the following lemma.

Lemma 5 [5]. *If $c_i \in \{0, 1\}$, $1 \le i \le N$, and $b_j \in \{0, 1\}$, $0 \le j < e$, and*

$$\sum_{i=1}^{N} c_i = \sum_{j\ge 0} b_j 2^j \pmod{2^e}, \tag{8}$$

then

$$b_j = \sum_{1\le i_1<i_2<\cdots<i_{2^j}\le N} c_{i_1} c_{i_2} \cdots c_{i_{2^j}} \pmod 2.$$

For the sake of convenience, let I_k be the index set such that $f_k(x) = \sum_{j\in I_k} x^j$, and let

$$S_r = \{\beta_{i,r-i} | 0 \le i < r\} \bigcup_{0\le i\le r} \{x^j\alpha_i | j \in I_{r-i}\}; \tag{9}$$

then we have

$$\sum_{0\le i\le r} f_{r-i}(x)\cdot\alpha_i + \sum_{0\le i<r} \beta_{i,r-i} = \sum_{\gamma\in S_r} \gamma \pmod{2^{e-r}};$$

hence (5) becomes

$$\sum_{\gamma\in S_r} \gamma = \sum_{0\le j<e-r} \beta_{r,j} 2^j \pmod{2^{e-r}}, \tag{10}$$

which is a counterpart of (8) for sequences. Since the sequence additions and products are performed component by component, we have from Lemma 5 and (10) that

Lemma 6.

$$\beta_{r,j} = \sum_{S_r} \gamma_1\gamma_2\cdots\gamma_{2^j} \pmod 2,$$

where by using the notation $\sum_{S_r}$ *we mean that the term* $\gamma_1\gamma_2\cdots\gamma_{2^j}$ *runs over all distinct* 2^jth*-order products of sequences in* S_r.

5.2. *Product Sequences*

In this subsection we briefly review the products of binary sequences. Let $a(x)$ and $b(x)$ be two polynomials over Z_2, and denote by $\Omega(a(x))$ the set of all sequences over Z_2 generated by $a(x)$. It is clear that $\Omega(a(x))$ is closed under sequence addition and the polynomial operators. It is known [1, p. 200], [4, p. 424] that $\Omega(a(x)) \subseteq \Omega(b(x))$ if and only if $a(x)|b(x)$, and a binary sequence β belongs to $\Omega(b(x))$ if and only if $m(\beta, x)|b(x)$, where $m(\beta, x)$ is the minimal polynomial of β. Define

$$\Omega(a(x))\Omega(b(x)) = \left\{ \sum_{i=1}^{m} \beta_i\gamma_i | \beta_i \in \Omega(a(x)), \gamma_i \in \Omega(b(x)), m \geq 1 \right\},$$

which is a space spanned on the products of the sequences in $\Omega(a(x))$ and $\Omega(b(x))$. We quote the results [7] on product sequences for later use.

Proposition 2 [7]. *Let* $A(x)$ *and* $B(x)$ *be two polynomials over* Z_2, *then*

$$\Omega(A(x))\Omega(B(x)) = \Omega(A(x) * B(x)),$$

where $A(x) * B(x)$ *is a polynomial determined by* $A(x)$ *and* $B(x)$ *as follows*:

1. *If* $A(x)$ *and* $B(x)$ *are both square free, assume* R_A *and* R_B *are the root sets of* $A(x)$ *and* $B(x)$ *respectively, and* $R_A \times R_B = \{\rho | \rho = \sigma\tau, \sigma \in R_A, \tau \in R_B\}$, *then*

$$A(x) * B(x) = \prod_{\rho \in R_A \times R_B} (x - \rho).$$

2. *If* $A(x) = a^{1+\lambda}(x)$ *and* $B(x) = b^{1+\mu}(x)$, *where* $a(x)$ *and* $b(x)$ *are square free, if* $\lambda = \sum_{k\geq 0} \lambda_k 2^k$ *and* $\mu = \sum_{k\geq 0} \mu_k 2^k$ *are the binary decompositions of* λ *and* μ, *respectively, if* k_0 *is the least subscript such that* $\lambda_k + \mu_k \leq 1$, $\forall k \geq k_0$, *and if* $\lambda * \mu$ *is defined by* $2^{k_0} - 1 + \sum_{k\geq k_0} (\lambda_k + \mu_k)2^k$, *then*

$$A(x) * B(x) = (a(x) * b(x))^{1+\lambda*\mu}.$$

3. *In general, if*

$$A(x) = \operatorname{lcm}\{a_i^{1+\lambda_i}(x) | 1 \leq i \leq M\} \quad \text{and} \quad B(x) = \operatorname{lcm}\{b_i^{1+\mu_j}(x) | 1 \leq j \leq N\},$$

where $a_i(x)$ *and* $b_j(x)$ *are square free, and* lcm *represents the least common multiple, then*

$$A(x) * B(x) = \operatorname{lcm}\{(a_i(x) * b_j(x))^{1+\lambda_i*\mu_j} | 1 \leq i \leq M, 1 \leq j \leq N\}.$$

5.3. *Upper Bounds $G_r(x)$ of $m(\alpha_r, x)$*

First we define a set of polynomials $g_w(x)$ and a function $\delta(i)$, which is used in Theorems 2 and 3. Let θ be a root of $f_0(x)$, and define

$$g_w(x) = \prod_{\substack{1 \le a \le 2^n - 1 \\ 1 \le w(a) \le w}} (x - \theta^a),$$

where the integer $w(a) = \sum_{i=0}^{n-1} a_i$ is derived from the binary decomposition $a = \sum_{i=0}^{n-1} a_i 2^i$. It is easy to see that

$$g_{w_1}(x) * g_{w_2}(x) = g_{w_1 + w_2}(x), \qquad w_1 \ge 1, \quad w_2 \ge 1.$$

For $i \ge 0$ define $\delta(i) = 2i - w(i)$. It is not difficult to see that $\delta(i)$ is an increasing function, and that $\delta(i) + \delta(j) \ge \delta(i * j)$.

Theorem 2 (Upper Bounds $G_r(x)$). *Define*

$$G_0(x) = f_0(x), \qquad G_r(x) = \operatorname{lcm}\{g_{2^r - \delta(i)}^{1+i}(x) | 0 \le i \le 2^{r-1}\}, \tag{11}$$

then

1. $G_{r+1}(x) = f_0(x)(G_r(x) * G_r(x))$, $r \ge 0$.
2. *The minimal polynomial $m(\alpha_r, x)$ of α_r is a factor of $G_r(x)$, i.e., $m(\alpha_r, x) | G_r(x)$.*
3. $G_r(x) = f_0(x) \prod_{0 \le i < 2^{r-1}} g_{1+r+\delta(i)}(x)$.

Proof. 1. Put

$$D_0(x) = 1, \qquad D_r(x) = \operatorname{lcm}\{g_{2^r - \delta(i)}^{1+i}(x) | 0 \le i < 2^{r-1}\}.$$

It is not difficult to see that $G_{r+1}(x)$ and $f_0(x) D_{r+1}(x)$ divide each other, so that

$$G_{r+1}(x) = f_0(x) D_{r+1}(x), \qquad r \ge 0.$$

So we need only prove

$$D_{r+1}(x) = G_r(x) * G_r(x), \qquad r \ge 0. \tag{12}$$

For any i, j, $i \le 2^{r-1}$, $j \le 2^{r-1}$, we have $i * j < 2^r$ and

$$g_{2^r - \delta(i)}^{1+i}(x) * g_{2^r - \delta(j)}^{1+j}(x) = g_{2^{r+1} - [\delta(i) + \delta(j)]}^{1+i*j}(x) | g_{2^{r+1} - \delta(i*j)}^{1+i*j}(x),$$

which leads to

$$G_r(x) * G_r(x) | D_{r+1}(x). \tag{13}$$

On the other hand, for any i, $0 \le i < 2^r$, if we write

$$i = i_0 + i_1 2^{r-1}, \qquad 0 \le i_0 < 2^{r-1}, \quad 0 \le i_1 < 2,$$

then we have

$$\delta(i) = \delta(i_0) + \delta(i_1 2^{r-1}), \qquad i = i_0 * i_1 2^{r-1}.$$

Hence it follows that

$$\begin{aligned} g_{2^{r+1} - \delta(i)}^{1+i}(x) &= g_{[2^r - \delta(i_0)] + [2^r - \delta(i_1 2^{r-1})]}^{1 + i_0 * i_1 2^{r-1}}(x) \\ &= g_{2^r - \delta(i_0)}^{1+i_0}(x) * g_{2^r - \delta(i_1 2^{r-1})}^{1+i_1 2^{r-1}}(x) | G_r(x) * G_r(x). \end{aligned}$$

Thus we have

$$D_{r+1}(x) | G_r(x) * G_r(x),$$

which together with (13) proves (12).

2. We have

$$G_i(x) | G_r(x) | G_r(x) * G_r(x), \qquad i < r, \tag{14}$$

and

$$\underbrace{G_r(x) * G_r(x) * \cdots * G_r(x)}_{2^j} | G_{r+j-1}(x) * G_{r+j-1}(x), \tag{15}$$

where (14) is an easy consequence of the definition of $G_r(x)$, and (15) can be proved by induction based on (14). We prove

$$\alpha_r \in \Omega(G_r(x)) \qquad \text{(i.e., } m(\alpha_r, x) | G_r(x))$$

together with

$$\beta_{r,j} \in \Omega(G_{r+j-1}(x) * G_{r+j-1}(x)) \tag{16}$$

by induction on r. Assume it is true for $r \le k$. Set

$$S^*_{k+1} = \{\beta_{i,k+1-i} | 0 \le i < k+1\} \bigcup_{0 \le i < k+1} \{x^j \alpha_i | j \in I_{k+1-i}\},$$

and then we have from the induction assumption and (14) that

$$\beta_{i,k+1-i} \in \Omega(G_k(x) * G_k(x)), \qquad i \le k,$$

and

$$x^j \alpha_i \in \Omega(G_i(x)) \subseteq \Omega(G_k(x)) \subseteq \Omega(G_k(x) * G_k(x)), \qquad 0 \le i \le k.$$

So we have

$$S^*_{k+1} \subseteq \Omega(G_k(x) * G_k(x)).$$

Now we have from (6) that

$$\begin{aligned} f_0(x)\alpha_{k+1} &= \sum_{0 \le i < k+1} f_{k+1-i}(x)\alpha_i + \sum_{0 \le i < k+1} \beta_{i,k+1-i} \\ &= \sum_{\gamma \in S^*_{k+1}} \gamma \pmod 2 \\ &\in \Omega(G_k(x) * G_k(x)), \end{aligned}$$

which leads to

$$\alpha_{k+1} \in \Omega(f_0(x)(G_k(x) * G_k(x))) = \Omega(G_{k+1}(x)).$$

Similarly we have

$$S_{k+1} \subseteq \Omega(G_{k+1}(x)),$$

where S_{k+1} is defined in (9). Then it follows from Lemma 6 and from (15) that

$$\begin{aligned}\beta_{k+1,j} &= \sum_{S_{k+1}} \gamma_1\gamma_2\cdots\gamma_{2^j} \pmod 2\\ &\in \underbrace{\Omega(G_{k+1}(x) * G_{k+1}(x) * \cdots * G_{k+1}(x))}_{2^j}\\ &\subseteq \Omega(G_{k+j}(x) * G_{k+j}(x)).\end{aligned}$$

Part 3 (for its proof, see Appendix 1) is an easy fact in algebra. □

5.4. *Improved Upper Bounds $G_r^*(x)$ of $m(\alpha_r, x)$*

An improved upper bound of $m(\alpha_r, x)$ is obtained by taking the greatest common divisor of $G_r(x)$ and some auxiliary characteristic polynomials of α_r. The following lemma, which comes from [3] with some modification, is used in deducing these auxiliary characteristic polynomials.

Lemma 7 [3]. *For $r > k \geq 2$, we have*

$$(x^{2^n-1} - 1)^{2^{r-2}+2^{r-3}+\cdots+2^{k-1}}\alpha_r = \varepsilon\alpha_k + \gamma,$$

where $\varepsilon = \Delta_f(x)\alpha_0$ and γ is a binary sequence in $\Omega(f_0(x) * G_1(x))$.

Proof. See Appendix 2. □

Note that

$$[\Delta_f(x)\alpha_0]\alpha_k \in \Omega(f_0(x) * G_k(x)) \pmod 2$$

and that

$$\gamma \in \Omega(f_0(x) * G_1(x)) \subseteq \Omega(f_0(x) * G_k(x)),$$

so it follows that

$$\varepsilon\alpha_k + \gamma \in \Omega(f_0(x) * G_k(x)),$$

and then it is easy to get, from Lemma 7,

Corollary 3. $m(\alpha_r, x) | [f_0(x) * G_k(x)] \cdot (x^{2^n-1} - 1)^{2^{r-1}-2^{k-1}}$, $2 \leq k \leq r-1$.

Theorem 3 (Improved Upper Bounds $G_r^*(x)$). *For $r \geq 3$, define*

$$G_r^*(x) = \gcd\{[f_0(x) * G_k(x)](x^{2^n-1} - 1)^{2^{r-1}-2^{k-1}}, G_r(x) | 2 \leq k \leq r-1\};$$

then $m(\alpha_r, x) | G_r^*(x)$, where $m(\alpha_r, x)$ is the minimal polynomial of α_r, and

$$G_r^*(x) = f_0(x)g_4(x)g_5(x)\left[\prod_{\substack{3\leq k\leq r-1\\ 2^{k-2}\leq i_k<2^{k-1}}} g_{2+k+\delta(i_k)}(x)\right]\prod_{2^{r-2}\leq i<2^{r-1}} g_{1+r+\delta(i)}(x). \quad (17)$$

Proof. It is evident from Theorem 2 and Corollary 3 that $m(\alpha_r, x) | G_r^*(x)$. Equality (17) is an easy fact in algebra (for its proof, see Appendix 2). □

6. Mixed Sequences

We now consider a binary sequence formed by mixing the highest component α_{e-1} with the lower ones as follows:

$$\gamma = k_{e-1}(x)\alpha_{e-1} + K(k_0(x)\alpha_0, k_1(x)\alpha_1, \ldots, k_{e-2}(x)\alpha_{e-2}), \tag{18}$$

where $k_i(x) \in Z_2[x]$, $k_{e-1}(x) \neq 0$, $\deg k_{e-1}(x) < n$, $K(x_0, x_1, \ldots, x_{e-2})$ is a polynomial of $e-1$ variables of degree less or equal to 1 with respect to each of the variables x_i $(0 \leq i \leq e-2)$, and $K(0, 0, \ldots, 0) = 0$. For example, taking $e = 8$, $n = 5$, $k_0(x) = x^4 + x$, $k_2(x) = 1$, $k_6(x) = x^2$, $k_7(x) = x^3 + 1$, and $K(x_0, x_1, \ldots, x_6) = x_0x_2 + x_6$, then

$$\gamma = (x^3 + 1)\alpha_7 + [(x^4 + x)\alpha_0]\alpha_2 + x^2\alpha_6.$$

From Theorem 2 it is not difficult to see that $K(k_0(x)\alpha_0, k_1(x)\alpha_1, \ldots, k_{e-2}(x)\alpha_{e-2}) \in \Omega(G_{e-2}(x) * G_{e-2}(x)) \subseteq \Omega(G_{e-1}(x))$. Hence from Theorems 1 and 2 we get

Theorem 4. *Let $f(x)$ be a primitive polynomial of degree n over Z_2, with the* 0th *component $f_0(x)$, let α be an ML-sequence generated by $f(x)$, and let γ be any mixed sequence from α as in* (18), *then we have*

1. $\mathrm{per}(\gamma) = 2^{e-1}(2^n - 1)$,
2. $m(\gamma, x) | G_{e-1}(x)$, *where $G_{e-1}(x) \in Z_2[x]$ is defined as in Theorem* 2.

Acknowledgements

The author thanks the Department of Mathematics, RHBNC, and Professor Fred Piper for their hospitality as she visited RHBNC, University of London, from July 1990 to June 1991, during which this paper was completed. The author also thanks Z. H. Liu for the communication about her discovery in her data driven study on periods of ring sequences. Thanks are also due to the referees for their interest in the paper and their helpful remarks.

Appendix 1

We say the polynomials $a_j(x)$, $0 \leq j < N$, form a decreasing (or an increasing) chain, if $a_{j+1}(x) | a_j(x)$ (or $a_j(x) | a_{j+1}(x)$) $\forall j$.

Lemma 8. *If the polynomials $a_j(x)$ and $a_{k,j}(x)$, $1 \leq k \leq M$, $0 \leq j < N$, are all square free, then we have*

1. *If $a_j(x)$, $0 \leq j < N$, form a decreasing chain, then*

$$\mathrm{lcm}\{a_j^{j+1}(x) | 0 \leq j < N\} = \prod_{0 \leq j < N} a_j(x).$$

2. *If $a_{k,j}(x)$, $0 \leq j < N$, form a decreasing* (or an increasing) *chain for each k, then*

$$\gcd\left\{\prod_{0 \leq j < N} a_{k,j}(x) | 1 \leq k \leq M\right\} = \prod_{0 \leq j < N} \gcd\{a_{k,j}(x) | 1 \leq k \leq M\}.$$

Proof. We prove only part 1; part 2 can be proved similarly. It is clear that the two sides of part 1 have the same roots. It is enough to show that each of the roots has the same multiplicity in these two sides. In fact, let ρ be one of the roots. Take it to be a root of $a_j(x)$ but not of $a_{j+1}(x)$. Then ρ has multiplicity $1+j$ in both sides. □

Lemma 9. *If the polynomials $a(x)$ and $a_j(x)$ are square free, and $a_j(x)$, $0 \le j < N$, form a decreasing* (or an increasing) *chain, then we have*

$$a(x) * \left[\prod_{0 \le j < N} a_j(x) \right] = \prod_{0 \le j < N} [a(x) * a_j(x)].$$

Proof. Without loss of generality we may assume that the $a_j(x)$, $0 \le j < N$, form a decreasing chain. It is not difficult to see from Proposition 2 that the polynomials $a(x) * a_j(x), 0 \le j < N$, form a decreasing chain. Then we have from item 1 of Lemma 8 and Proposition 2 that

$$\begin{aligned} a(x) * \prod_{0 \le j < N} a_j(x) &= a(x) * \operatorname{lcm}\{a_j^{j+1}(x) | 0 \le j < N\} \\ &= \operatorname{lcm}\{a(x) * a_j^{j+1}(x) | 0 \le j < N\} \\ &= \operatorname{lcm}\{(a(x) * a_j(x))^{j+1} | 0 \le j < N\} \\ &= \prod_{0 \le j < N} a(x) * a_j(x). \end{aligned}$$

□

Proof of Part 3 of Theorem 2. Note that $g_{2^r - \delta(i)}(x)$, $0 \le i \le 2^{r-1}$, form a decreasing chain, and so we have

$$\begin{aligned} G_r(x) &= \operatorname{lcm}\{g_{2^r-\delta(i)}^{1+i}(x) | 0 \le i \le 2^{r-1}\} \\ &= \prod_{0 \le i \le 2^{r-1}} g_{2^r-\delta(i)}(x) \\ &= f_0(x) \prod_{0 \le i < 2^{r-1}} g_{2^r-\delta(i)}(x) \\ &= f_0(x) \prod_{0 \le i < 2^{r-1}} g_{1+r+\delta(i)}(x), \end{aligned}$$

where the first equality comes from the definition in Theorem 2, the second from Lemma 8, and the fourth by the substitution $j = 2^{r-1} - 1 - i$ and $r + 1 + \delta(i) = 2^r - \delta(j)$. □

Appendix 2

Lemma 10.

1. *Let c_1, c_2, b_0, b_1 be integers equal to 0 or 1, and let $c_1 - c_2 = b_0 + b_1 2 \pmod{2^2}$, then $b_0 = c_1 + c_2 \pmod 2$, $b_1 = b_0 c_2 \pmod 2$.*
2. *Let $\gamma_1, \gamma_2, \beta_1, \beta_2$ be binary sequences, and let $\gamma_1 - \gamma_2 = \beta_0 + \beta_1 2 \pmod{2^2}$, then $\beta_0 = \gamma_1 + \gamma_2 \pmod 2$, $\beta_1 = \beta_0 \gamma_2 \pmod 2$.*

Proof. Part 1 can be checked directly. Since the sequence additions and products are performed component by component, part 2 is just a direct consequence of part 1. □

Lemma 11. *Let $r \geq 2$, and let ε_1 be the binary sequence defined by*

$$\varepsilon_1 = (x^{(2^n-1)2^{r-2}} - 1)\alpha_r + \varepsilon_0\alpha_{r-1} \pmod 2,$$

where $\varepsilon_0 = \Delta_f(x)\alpha_0 \pmod 2$. Then $\varepsilon_1 \in \Omega(G_1(x))$.

Proof. We have

$$\begin{aligned}(x^{(2^n-1)2^{r-2}} - 1)\alpha &= [(x^{(2^n-1)2^{r-2}} - 1)(\alpha_{r-1} + \alpha_r 2)]2^{r-1} \\ &= [(x^{(2^n-1)2^{r-2}}\alpha_{r-1} - \alpha_{r-1}) + (x^{(2^n-1)2^{r-2}} - 1)\cdot\alpha_r 2]2^{r-1} \\ &= [\varepsilon_0 + \varepsilon_0\alpha_{r-1}2 + (x^{(2^n-1)2^{r-2}} - 1)\alpha_r 2]2^{r-1} \\ &= (\varepsilon_0 + \varepsilon_1 2)2^{r-1} \pmod{2^{r+1}},\end{aligned}$$

where the first equality is based on the fact that $\mathrm{per}(\alpha_i)|2^{r-2}(2^n - 1), \forall i < r - 1$, and the third one based on Lemmas 3 and 10. Applying $f(x)$ to the first and last terms of the above equations we get

$$0 = f(x)(x^{(2^n-1)2^{r-2}} - 1)\alpha = f(x)\cdot(\varepsilon_0 + \varepsilon_1 2)2^{r-1} \pmod{2^{r+1}}.$$

Hence we obtain

$$f(x)(\varepsilon_0 + \varepsilon_1 2) = 0 \pmod{2^2},$$

which means the sequence $\varepsilon_0 + \varepsilon_1 2$ is generated by $f(x)$ over Z_{2^2}. Then we get from Theorem 2 that $\varepsilon_1 \in \Omega(G_1(x))$. □

Proof of Lemma 7. We prove it by induction with r decreasing. From Lemma 11, we have

$$(x^{(2^n-1)2^{r-2}} - 1)\alpha_r = \varepsilon_0\alpha_{r-1} + \varepsilon_1 \pmod 2,$$

where $\varepsilon_1 \in \Omega(G_1(x)) \subseteq \Omega(f_0(x) * G_1(x))$, hence Lemma 7 is true for $k = r - 1$. Assume it is true for $k \geq l$, $3 < l < r$, in particular we have

$$(x^{2^n-1} - 1)^{2^{r-2}+2^{r-3}+\cdots+2^{l-1}}\alpha_r = \varepsilon_0\alpha_l + \gamma, \tag{19}$$

where $\varepsilon_0 \in \Omega(f_0(x))$ and $\gamma \in \Omega(f_0(x) * G_1(x)) \subseteq \Omega(x^{2(2^n-1)} - 1)$. Then we have

$$x^{(2^n-1)2^{l-2}}\varepsilon_0 = \varepsilon_0 \quad \text{and} \quad (x^{(2^n-1)2^{l-2}} - 1)\gamma = 0.$$

Now, applying the operator $(x^{2^n-1} - 1)^{2^{l-2}} = x^{(2^n-1)2^{l-2}} - 1 \pmod 2$ on the two sides of (19), we get

$$\begin{aligned}(x^{2^n-1} - 1)^{2^{r-2}+2^{r-3}+\cdots+2^{l-1}+2^{l-2}}\alpha_r &= (x^{(2^n-1)2^{l-2}} - 1)(\varepsilon_0\alpha_l + \gamma) \\ &= \varepsilon_0[x^{(2^n-1)2^{l-2}}\alpha_l] - \varepsilon_0\alpha_l \\ &= \varepsilon_0[(x^{(2^n-1)2^{l-2}} - 1)\alpha_l] \\ &= \varepsilon_0(\varepsilon_0\alpha_{l-1} + \varepsilon_1) \\ &= \varepsilon_0\alpha_{l-1} + \varepsilon_0\varepsilon_1 \pmod 2,\end{aligned}$$

where the fourth equality comes from Lemma 11. It is clear that

$$\varepsilon_0\varepsilon_1 \in \Omega(f_0(x) * G_1(x)),$$

and thus Lemma 8 is true for $k = l - 1$. □

Proof of Equality (17) in Theorem 3. Put

$$H_{r,k}(x) = [f_0(x) * G_k(x)](x^{2^n-1} - 1)^{2^{r-1}-2^{k-1}}.$$

We have

$$\begin{aligned} f_0(x) * G_k(x) &= f_0(x) * \left[f_0(x) \prod_{0 \le i < 2^{k-1}} g_{1+k+\delta(i)}(x) \right] \\ &= [f_0(x) * f_0(x)] \prod_{0 \le i < 2^{k-1}} [f_0(x) * g_{1+k+\delta(i)}(x)] \\ &= g_2(x) \prod_{0 \le i < 2^{k-1}} g_{2+k+\delta(i)}(x), \end{aligned}$$

where the first equality comes from Theorem 2 and the second from Lemma 9. Therefore $H_{r,k}(x)$ has the following increasing chain expression:

$$H_{r,k}(x) = g_2(x) \prod_{0 \le i < 2^{r-1}} g_{k,i}(x), \tag{20}$$

where

$$g_{k,i}(x) = \begin{cases} g_{2+k+\delta(i)}(x), & 0 \le i < 2^{k-1} \\ x^{2^n-1} - 1, & 2^{k-1} \le i. \end{cases}$$

Now, based on the increasing chain expressions (part 3 of Theorem 2 and (20)) of $G_r(x)$ and $H_{r,k}(x)$, $2 \le k < r$, respectively, and Lemma 8, it is not difficult to get the expression (17) of their greatest common divisor $G_r^*(x)$, but we omit the details. □

References

[1] H. Beker and F. Piper, *Cipher Systems*, Northwood Books, London, 1982.

[2] A. M. Frieze, J. Hastad, R. Kannan, J. C. Lagarias, and A. Shamir, Reconstructing Truncated Integer Variables Satisfying Linear Congruences, *SIAM J. Comput.*, **17**, 262–280 (1988).

[3] M. Q. Huang, Analysis and Cryptology Evaluation on Primitive Sequences, Ph.D. Dissertation, Department of Mathematics, Graduate School, Academia Sinica, Beijing, 1988.

[4] R. Lidl and H. Niederreiter, *Finite Fields, Encyclopaedia of Mathematics and Its Applications*, Vol. 20, Addison-Wesley, Reading, MA, 1983.

[5] R. A. Rueppel, *Analysis and Design of Stream Ciphers*, Springer-Verlag, Berlin, 1986.

[6] M. Ward, The Arithmetical Theory of Linear Recurring Series, *Trans. Amer. Math. Soc.*, **35**, 600–628 (July 1933).

[7] N. Zierler and W. H. Mills, Products of Linear Recursive Sequences, *J. Algebra*, **27**, 147–157 (1973).