ML-Sequences over Rings $Z/(2^e)$ * :
I. Constructions of Nondegenerative ML-Sequences
II. Injectivness of Compression Mappings of New Classes

WenFeng Qi[1], JunHui Yang[2], JingJun Zhou[1]

[1] Zhengzhou Information Engineering Institute, HeNan, China

[2]Institute of Software, Academia Sinica,
State Key Lab. of Information Security, Beijing, China
yangdai@mimi.cnc.ac.cn

Abstract

Pseudorandom binary sequences derived from the ML-sequences over the integer residue ring $Z/(2^e)$ are proposed and studied in [1-10]. This paper is divided into two parts. The first part is on the nondegenerative ML-sequences. In this part the so-called quasi-period of a ML-sequence is introduced, and it is noted that a ML-sequence may degenerate in the sense that it has the quasi-period shorter than its period, and the problem of constructing the nondegenerative ML-sequences is solved by giving a criterion for nondegenerative primitive polynomials. In the second part, based on the constructions [1, 6, 7] of some classes of injective mappings which compress ML-sequences over rings to binary sequences, some new classes of the injective compression mappings are proposed and proved.
Keywords: nondegenerate ML-sequence, quasi-period, injective compression mapping

1 Introduction

The maximal length sequences of elements in the integral residue ring $Z/(2^e)$ (ML-sequences over $Z/(2^e)$), whose definition will be recalled in the next section, and the binary sequences derived from ML-sequences are proposed and studied in [1-9]. The research shows that the binary sequences derived from ML-sequences may provide a good source of pseudorandom sequences and have a potential perspective in cryptographic applications.

The integral residue ring $Z/(2^e)$ is the set of 2^e integral residue classes $\{i \pmod{2^e} | 0 \le i < 2^e\}$, the class $i \pmod{2^e}$ will be written simply as i or any integer of the form $i + k2^e$ with k being an integer. 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) bit of b. 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 $\alpha = \{a_t\}_{t=0}^{\infty}$ has a binary decomposition

*This work was supported by Chinese Natural Science Foundation (69773015 and 19771088).

K. Ohta and D. Pei (Eds.): ASIACRYPT'98, LNCS 1514, pp. 315-326, 1998.

$\alpha = \sum_{i=0}^{e-1} \alpha_i 2^i$, where $\alpha_i = \{a_{t,i}\}_{t=0}^{\infty}$ is a binary sequence called the ith level component of α.

The highest level component sequence of a ML-sequence over $Z/(2^e)$ is the most naturally derived binary sequences. More binary sequences can be derived from a ML-sequence over $Z/(2^e)$ by mixing the bits at its highest level with the bits at the lower levels. This can provide a convenient way of generating pseudorandom binary sequences on computers when e is chosen as the processor word length. It is shown that the derived binary sequences have guaranteed large periods [5] and guaranteed large lower bound of linear complexities [4]. It is also shown that the distributions of the elements 0 and 1 of the derived binary sequences are close to be balanced [8, 9, 10]. In addition to these, it is proved [1, 6, 7] that the mapping which compresses the ML-sequences over $Z/(2^e)$ to its highest level component sequences is injective, and that a large class of mappings which compress the ML-sequences over $Z/(2^e)$ to the binary sequences by mixing the highest level component sequences with the lower level ones are also injective. The injectiveness of these compression mappings is desirable when the ML-sequences are used as a source of pseudorandom sequences, since in this case, different initial states of a ML-sequence do lead to different pseudorandom sequences.

In this paper we keep studying the ML-sequences and the compression mappings, the contents are divided into two parts. In the first part, the work is started by noticing the phenomenon that a ML-sequence may degenerate in the sense that its quasi-period (which will be defined in section 2) is shorter than its period, and that the deganerative ML-sequences are undesirable in applications. So we study the problem how to construct nondegenerative ML-sequences. As results, it is shown (Theorem 3) that an ML-sequence degenerates if and only if the corresponding primitive polynomial (*i.e.*, its minimal polynomial) degenerates in the same sense that its quasi-period (which will be defined in section 2) is shorter than its period, thus the problem constructing nondegenerate ML-sequences is reduced to the problem constructing nondegenerate primitive polynomials, and the latter is solved (Theorem 4) by giving a criterion for nondegenerative primitive polynomials. In the second part, based on the constructions [1, 6, 7] of some classes of injective compression mappings, some new classes of injective compression mappings are proposed and proved.

2 Constructions of Nondegenerative ML-Sequences

Before coming to the main topic, we recall some basic concepts and basic facts which we need. Let $\alpha = \{a_i\}_{i=0}^{\infty}$ be a sequence of elements in $Z/(2^e)$, obeying the linear recursion of the form $a_{i+n} = -\sum_{i=0}^{n-1} c_j a_{i+j} \pmod{2^e}, \forall i \geq 0$, with $(a_0, a_1, \cdots, a_{n-1})$ specifying the initial condition, and with c_j constants in $Z/(2^e)$. As usual, the monic polynomial $f(x) = x^n + \sum_{j=0}^{n-1} c_j x^j$ is called a characteristic polynomial of α, the characteristic polynomial with the least degree is called the minimal polynomial of α. The polynomial $f(x)$ has the binary decomposition $f(x) = \sum_{i=0}^{e-1} f_i(x)2^i$, where $f_i(x) = \sum_{i=0}^{n-1} c_{j,i}x^j$ and $c_j = \sum_{i=0}^{e-1} c_{j,i}2^i$ is the binary decomposition of c_j.

In this paper we always assume $c_0 \equiv 1 \pmod 2$.

Definition: The *period* of $\alpha = \{a_i\}_{i=0}^{\infty}$, denoted by $per(\alpha)$, is defined to be the least positive integer t satisfying $a_{t+i} = a_i, \forall i \geq 0$.

Definition: The *period* of $f(x)$ over $Z/(2^e)$, denoted by $per(f(x))_{2^e}$, is defined to be the least positive integer t satisfying $x^t \equiv 1 \pmod{2^e, f(x)}$.

Both of $per(f(x))_{2^e}$ and $per(\alpha)$ are upper bounded by $2^{e-1}(2^n-1)$ [5], and this upper bound is attainable.

Definition: α is called a ML-sequence of degree n if its period attains this upper bound $2^{e-1}(2^n-1)$; and the polynomial $f(x)$ is called *primitive* over $Z/(2^e)$ if $per(f(x)_{2^e}$ attains this upper bound $2^{e-1}(2^n-1)$.

If $f_0(x)$ is primitive over $Z/(2^e)$, then there exists a polynomial $r(x) \in Z/(2^e)[x]$ such that

$$x^{2^n-1} - 1 \equiv f_0(x)r(x) \pmod 2 \tag{1}$$

it is clear that $r(x) \pmod 2$ is uniquely determined; and there exists $h(x)$ over $Z/(2^e)[x]$ such that

$$\begin{aligned} x^{2^n-1} &\equiv 1 + f_0(x)r(x) + 2h(x) \\ &\equiv 1 + (f_0(x) + \textstyle\sum_{i=1}^{e-1} f_i(x)2^i)r(x) + 2(h(x) - r(x)\sum_{i=1}^{e-1} f_i(x)2^{i-1}) \\ &\equiv 1 + 2(h(x) - r(x)\textstyle\sum_{i=1}^{e-1} f_i(x)2^{i-1}) \\ &\equiv 1 + 2h_f(x) \pmod{2^e, f(x)} \end{aligned}$$

where $h_f(x) = h(x) - r(x)\sum_{i=1}^{e-1} f_i(x)2^{i-1}$, hence

$$h_f(x) \equiv h(x) - r(x)f_1(x) \pmod{2, f_0(x)} \tag{2}$$

and

$$x^{2^n-1} \equiv 1 + 2h_f(x) \pmod{2^2, f(x)} \tag{3}$$

Taking $f_1(x) = 0$ in (3), we get

$$x^{2^n-1} \equiv 1 + 2h(x) \pmod{2^2, f_0(x)} \tag{4}$$

It is also clear that both $h(x) \pmod{2, f_0(x)}$ and $h_f(x) \pmod{2, f_0(x)}$ are uniquely determined.

We know the following theorem.

Theorem 1 *[2, 5]*

1. *Let $per(f(x))_2 = T$, then $per(f(x))_{2^e} = 2^kT$, where k is an integer with $0 \leq k < e$.*

2. *α is a ML-sequence of degree n if and only if $f(x)$ is primitive over $Z/(2^e)$ and $\alpha_0 \neq 0$; and in this case, $f(x)$ is the minimal polynomial of α.*

3. *The following conditions are equivalent:*

   (a) *$f(x)$ is primitive over $Z/(2^e)$, i.e., $per(f(x))_{2^e} = 2^{e-1}(2^n - 1)$.*

   (b) *$f_0(x)$ is primitive over $Z/(2)$, and $h_f(x) \neq 0 \pmod{2, f_0(x)}$ when $e = 2$ and $h_f(x)(h_f(x)+1) \neq 0 \pmod{2, f_0(x)}$ when $e \geq 3$.*

   (c) *$f_0(x)$ is primitive over $Z/(2)$, and $f_1(x) \neq r(x)^{-1}h(x) \pmod{2, f_0(x)}$ when $e = 2$ and*

$$f_1(x) \neq \begin{cases} r(x)^{-1}h(x) \pmod{2, f_0(x)} \\ r(x)^{-1}(h(x)+1) \pmod{2, f_0(x)} \end{cases}$$

   when $e \geq 3$.

Lemma 1 *[2] Denote the formal derivative of $f_0(x)$ by $f_0'(x)$, we have*

1. *$r(x)^{-1} \equiv x f_0'(x) \pmod{2, f_0(x)}$.*

2. *Denote $f_0(x) = \sum_{i \in S} x^i$ where S is a subset of $\{i | 0 \leq i \leq n\}$, and denote $\rho(x) = (\sum_{i,j \in S, i<j} x^{i+j})^{2^{n-1}} \pmod{2, f_0(x)}$, then $r(x)^{-1}h(x) \equiv \rho(x) \pmod{2, f_0(x)}$.*

Remark 1 Based on Lemma 1, The equivalent conditions for primitive polynomials given in Theorem 1 can be easily checked.

Definition: The *quasi-period* of $\alpha = \{a_i\}_{i=0}^{\infty}$, denoted by $Qper(\alpha)$, is defined to be the least positive integer t satisfying $a_{t+i} = ca_i, \forall i \geq 0$, with $c \in Z/(2^e)$.

Definition: The *quasi-period* of $f(x)$ over $Z/(2^e)$, denoted by $Qper(f(x))_{2^e}$, is defined to be the least positive integer t satisfying $x^t \equiv c \pmod{2^e, f(x)}$ with $c \in Z/(2^e)$.

Definition: We say a ML-sequence α is *nondegenerative* if $Qper(\alpha) = per(\alpha)$; and say a primitive polynomial $f(x)$ is *nondegenerative* if $Qper(f(x))_{Z/(2^e)} = per(f(x))_{Z/(2^e)}$.

The following theorem is on the relation between the quasi-periods and the periods of the polynomials over $Z/(2^e)$.

Theorem 2 *Let $per(f(x))_2 = T$, and $per(f(x))_{2^e} = 2^k T$, then $Qper(f(x))_{2^e} = 2^m T$ for some non-negative integer m with $m \leq k$.*

Proof *Let $Qper(f(x))_{2^e} = t$, first we claim $T|t$, hence $t = bT$ for some integer b. In fact, we have $x^t \equiv c \pmod{2^e, f(x)}$ for some $c \in Z/(2^e)$; since $(2^e, f(x)) \subseteq (2, f_0(x))$, so $x^t \equiv c \pmod{2, f_0(x)}$. We claim $c \equiv 1 \pmod{2}$, hence $T|t$; otherwise, we have $c \equiv 0 \pmod{2}$, then $1 \equiv x^{(2^k T)t} \equiv x^{t(2^k T)} \equiv 0 \pmod{2, f_0(x)}$, a contradiction. Now consider the following set (where Z is the integer ring):*

$$\mathcal{T} = \{t | x^t \equiv c \pmod{2^e, f(x)}, t \in Z, c \in Z/(2^e)\} \tag{5}$$

It is clear that $\mathcal{T}$ is an ideal of Z containing 2^kT, and $bT = Qper(f(x))_{2^e}$ is the positive generator of $\mathcal{T}$, so bT must be a factor of 2^kT, thus $b = 2^m$ for an integer m with $m \leq k$. □

It is easy to prove the following theorem.

Theorem 3 *If α is an ML-sequence of degree n, then $Qper(\alpha) = Qper(f(x))_{2^e}$, as a consequence, α is nondegenerative degenerate if and only if $f(x)$ is nondegenerative.*

Based on Theorem 1 and 2, the problem constructing nondegenerative ML-sequences is reduced to the problem constructing nondegenerative primitive polynomials. The latter can be solved by the following Theorem, which gives a criterion for nondegenerative primitive polynomials.

Theorem 4 *Let $f(x)$ be primitive over $Z/(2^e)$, and let $h(x) \pmod{2, f_0(x)}$ be the polynomial defined as (4). We have*

1. *When $e = 2$, then the following conditions are equivalent:*
   - *(a) $f(x)$ is nondegenerative.*
   - *(b) $h_f(x) \neq 1 \pmod{2, f_0(x)}$.*
   - *(c) $f_1(x) \neq r(x)^{-1}(1 + h(x)) \pmod{2, f_0(x)}$.*
2. *When $e \geq 3$ and n is odd, then $f(x)$ is always nondegenerative.*
3. *When $e \geq 3$ and n is even, then the following conditions are equivalent:*
   - *(a) $f(x)$ is nondegenerative.*
   - *(b) $h_f(x)(1 + h_f(x)) \neq 1 \pmod{2, f_0(x)}$.*
   - *(c)*
$$f_1(x) \neq \begin{cases} r(x)^{-1}(x^{(2^n-1)/3} + h(x)) & \pmod{2, f_0(x)} \\ r(x)^{-1}(1 + x^{(2^n-1)/3} + h(x)) & \pmod{2, f_0(x)} \end{cases}$$

Proof *Write $T = 2^n - 1$. Taking squares on the two sides of the equation (3), we get*
$$x^{2T} \equiv 1 + 2^2 h_f(x)(h_f(x) + 1) \pmod{2^3, f(x)}$$
continueing this way we get
$$x^{2^{i-2}T} \equiv 1 + 2^{i-1} h_f(x)(h_f(x) + 1) \pmod{2^i, f(x)}, \forall i \leq e$$
In particular, we get
$$x^{2^{e-2}T} \equiv 1 + 2^{e-1} h_f(x)(h_f(x) + 1) \pmod{2^e, f(x)} \tag{6}$$

For $e = 2$, we have

$$\begin{aligned}
& Qper(f(x))_{2^e} < per(f(x))_{2^e} \\
\longleftrightarrow\ & Qper(f(x))_{2^2} = T \text{ (by Theorem 2)} \\
\longleftrightarrow\ & c \equiv x^T \equiv 1 + 2h_f(x) \pmod{2^2, f(x)} \text{ (by (3))} \\
\longleftrightarrow\ & 2h_f(x) \equiv 2b \pmod{2^2, f(x)}, b = 0 \text{or} 1 \pmod 2 \\
\longleftrightarrow\ & h_f(x) \equiv 1 \pmod{2, f_0(x)} \text{ (by the assumption and Theorem 1)} \\
\longleftrightarrow\ & f_1(x) \equiv r(x)^{-1}(1 + h(x)) \pmod{2, f_0(x)} \text{ (by (2))}
\end{aligned}$$

For $e \geq 3$, we get

$$\begin{aligned}
& Qper(f(x))_{2^e} < per(f(x))_{2^e} \\
\longleftrightarrow\ & Qper(f(x))_{2^e} | 2^{e-2}T \\
\longleftrightarrow\ & c \equiv x^{2^{e-2}T} \equiv 1 + 2^{e-1}h_f(x)(h_f(x)+1) \pmod{2^e, f(x)}(by(6)) \\
\longleftrightarrow\ & 2^{e-1}h_f(x)(h_f(x)+1) \equiv 2^{e-1}b \pmod{2^e, f(x)}, b = 0or1 \\
\longleftrightarrow\ & h_f(x)(h_f(x)+1) \equiv 1 \pmod{2, f_0(x)} \\
& \text{(by the assumption and Theorem 1).}
\end{aligned}$$

If we identify $(Z/(2))[x]/(f_0(x))$ to the finite field $GF(2^n)$, then it is clear that the fact "$h_f(x)(h_f(x)+1) \equiv 1 \pmod{2, f_0(x)}$" holds true if and only if $h_f(x)$ is a root of the irreducible polynomial x^2+x+1 over $Z/(2) = GF(2)$, i.e., one of the two elements of order 3. It is known that there exists such $h_f(x)$ if and only if n is even. Hence the item 2. is true. Now for the item 3., we know that the two roots of x^2+x+1 are $x^{T/3} \pmod{2, f_0(x)}$ and $1 + x^{T/3} \pmod{2, f_0(x)}$ (the two elements of order 3), so "$h_f(x)(h_f(x)+1) \equiv 1 \pmod{2, f_0(x)}$" holds true if and only if $h_f(x) \equiv x^{T/3} \pmod{2, f_0(x)}$ or $1+x^{T/3} \pmod{2, f_0(x)}$, which is further equivalent to the conditions shown in (3c)(by (2)). □

Remark 2 Based on Lemma 1, The equivalent conditions for nonprimitive primitive polynomials given in Theorem 4 can be easily checked.

In studying the injective compression mappings, the so-called strongly primitive polynomial is introduced [1], it is defined to be the primitive polynomial with $h_f(x) \neq 1 \pmod{2, f_0(x)}$ when $e = 2$, and to be the primitive polynomial with $h_f(x)(h_f(x)+1) \neq 1 \pmod{2, f_0(x)}$ when $e \geq 3$. Now from Theorem 3 we get imeadiately

Corollary 1 *$f(x)$ is strongly primitive if and only if $f(x)$ is nondegenerative primitive, i.e., $Qper(f(x))_{2^e} = per(f(x))_{2^e}$.*

3 Compressing Mappings on ML-Sequences

Let $f(x)$ be a primitive polynomial of degree n over $Z/(2^e)$, We denote $G(f(x))_{2^e}$ the set of all sequences over $Z/(2^e)$ generated by $f(x)$, $S(f(x))_{2^e} = \{\alpha \in G(f(x)) \mid \alpha_0 \neq \mathbf{0}\}$ the set of all ML-sequences over $Z/(2^e)$ generated by $f(x)$ and $GF(2)^\infty$ the set of all sequences over $GF(2)$. For $\alpha \in G(f(x))_{2^e}$, we denote α_i the ith level component of α. Set $T = 2^n - 1$, by (3), we have

$$x^{2^{k-1}T} - 1 = 2^k h_k(x) \pmod{f(x), 2^e}$$

where $k = 1, 2, \ldots, e-1$, $\deg h_k(x) < n$ and $h_k(x) \neq 0 \pmod 2$. In fact $h_1(x) = h_f(x) \pmod 2$, $h_2(x) = \ldots = h_{e-1}(x) = h_f(x)(h_f(x)+1) \pmod{2, f(x)}$.

Let $\alpha = \{a_i\}_{i=0}^{\infty}$ and $\beta = \{b_i\}_{i=0}^{\infty}$ be two sequences over $Z/(2^e)$, define $\alpha + \beta = \{a_i + b_i\}_{i=0}^{\infty}$, $\alpha\beta = \{a_i b_i\}_{i=0}^{\infty}$ and $x\alpha = \{a_i\}_{i=0}^{\infty} = \{a_{i+1}\}_{i=0}^{\infty}$. For $g(x) = \sum_{j=0}^{n} c_j x^j$ over $Z/(2^e)$, then $g(x)\alpha = g(x)\{a_i\}_{i=0}^{\infty} = \{\sum_{j=0}^{n} c_j a_{j+i}\}_{i=0}^{\infty}$.

[1, 6, 7] propose the following injectiveness theorem.

Theorem 5 *[1, 6, 7] Let $f(x)$ be a primitive polynomial over $Z/(2^e)$, $\alpha, \beta \in G(f(x))_{2^e}$,then $\alpha = \beta$ if and only if $\alpha_{e-1} = \beta_{e-1}$. If $f(x)$ is strongly primitive over $Z/(2^e)$, $\varphi(x_0, x_1, \ldots, x_{e-1}) = x_{e-1} + cx_{e-2} + \eta(x_0, x_1, \ldots, x_{e-3})$ is a Boolean function of e variables, where $\eta(x_0, x_1, \ldots, x_{e-3})$ is a Boolean function of $e-2$ variables, $c = 0$ or 1, then for $\alpha, \beta \in G(f(x))_{2^e}$, $\alpha = \beta$ if and only if $\varphi(\alpha_0, \alpha_1, \ldots, \alpha_{e-1}) = \varphi(\beta_0, \beta_1, \ldots, \beta_{e-1})$ over $GF(2)$.*

By theorem 5, the compression mapping x_{e-1} or $x_{e-1}+cx_{e-2}+\eta(x_0, \ldots, x_{e-3})$ on $G(f(x))_{2^e}$ is injective, that is, the binary sequence α_{e-1} or $\alpha_{e-1} + c\alpha_{e-2} + \eta(\alpha_0, \alpha_1, ..., \alpha_{e-3})$ can uniquely determine its original sequence α, in other words, α_{e-1} or $\alpha_{e-1} + c\alpha_{e-2} + \eta(\alpha_0, \alpha_1, \ldots, \alpha_{e-3})$ contains all information of α.

We study the injectiveness of general compression mappings in this section. Let $\varphi(x_0, ..., x_{e-1})$ be a Boolean function with e variables, if the mapping

$$\varphi : \begin{cases} G(f(x))_{2^e} \to GF(2)^{\infty} \\ \alpha = \alpha_0 + \alpha_1 2 + \ldots + \alpha_{e-1}2^{e-1} \mapsto \varphi(\alpha_0, \ldots, \alpha_{e-1}) \end{cases}$$

is injective, then $\varphi(x_0, ..., x_{e-1})$ contains x_{e-1} clearly, *i.e.*, $\varphi(x_0, \ldots, x_{e-2}, 0) \neq \varphi(x_0, \ldots, x_{e-2}, 1)$.

Definition: Let $B = \{x_0^{i_0} x_1^{i_1} \ldots x_{e-1}^{i_{e-1}}$ — $i_k = 0$ or 1, $k = 0, 1, \ldots, e-1\}$ be the set of all single terms of Boolean functions of e variables, define the order in B as follows:

$$x_0^{i_0} x_1^{i_1} \ldots x_{e-1}^{i_{e-1}} > x_0^{j_0} x_1^{j_1} \ldots x_{e-1}^{j_{e-1}}$$

provided that

$$i_0 + i_1 \cdot 2 + \ldots + i_{e-1} \cdot 2^{e-1} > j_0 + j_1 \cdot 2 + \ldots + j_{e-1} \cdot 2^{e-1}$$

Lemma 2 *[10] Let $f(x)$ be a strongly primitive polynomial of degree n over $Z/(2^e)$, $e \geq 3$, $\varphi(x_0, x_1, \ldots, x_{e-1})$ is a Boolean function of e variables and $\varphi(x_0, x_1, \ldots, x_{e-1}) \neq 0$ and 1. Let $x_{k_0} x_{k_1} \ldots x_{k_{t-1}}$ be the term of the maximal order in $\varphi(x_0, x_1, \ldots, x_{e-1})$ and the product $x_0 x_1$ of x_0 and x_1 is not a divisor of $x_{k_0} x_{k_1} \ldots x_{k_{t-1}}$, where $1 \leq t \leq e-1$, $0 \leq k_0 < k_1 < \ldots < k_{t-1} \leq e-1$. Then for $\alpha, \beta \in S(f(x))_{2^e}$, $\varphi(\alpha_0, \ldots, \alpha_{e-1}) = \varphi(\beta_0, \ldots, \beta_{e-1})$ implies $\alpha_0 = \beta_0$.*

Lemma 3 *[10] Let $f(x)$ be a primitive polynomial of degree n over $Z/(2^e)$, $e \geq 3$, $\alpha, \beta \in G(f(x))_{2^e}$ and $\alpha_0 = \beta_0$, then, for $3 \leq k \leq e-1$, over $GF(2)$*

$$(x^{2^{k-2}T} - 1)(\alpha_k + \beta_k) = (\alpha_{k-1} + \beta_{k-1})h_2(x)\alpha_0 + h_2(x)(\alpha_1 + \beta_1)$$

and

$$(x^T - 1)(\alpha_2 + \beta_2) = (\alpha_1 + \beta_1)h_1(x)\alpha_0 + h_1(x)(\alpha_1 + \beta_1)$$

Lemma 4 *[10] Let $f(x)$ be a primitive polynomial of degree n over $Z/(2^e)$, $e \geq 3$, $\alpha, \beta \in G(f(x))_{2^e}$ and $\alpha_0 = \beta_0 \neq \mathbf{0}$. If $(\alpha_1 + \beta_1)h_1(x)\alpha_0 h_2(x)\alpha_0 = h_1(x)(\alpha_1 + \beta_1)h_2(x)\alpha_0$ over $GF(2)$, then $\alpha_1 = \beta_1$*

Theorem 6 *Let $f(x)$ be a strongly primitive polynomial of degree n over $Z/(2^e)$, $e \geq 3$, $\varphi(x_0, \ldots, x_{e-1}) = x_{e-1} + \eta(x_0, \ldots, x_{e-2})$ is a Boolean function of e variables, for $\alpha, \beta \in S(f(x))_{2^e}$, if*

$$(\varphi(\alpha_0, \ldots, \alpha_{e-1}) + \varphi(\beta_0, \ldots, \beta_{e-1}))h_2(x)\alpha_0 = \mathbf{0} \tag{7}$$

then $\alpha = \beta$.

Proof *First we show $\alpha_0 = \beta_0$. Set $T = 2^n - 1$. $x^{2^{e-2}T} - 1$ acts on (7), then $(h_2(x)\alpha_0 + h_2(x)\beta_0)h_2(x)\alpha_0 = \mathbf{0}$ since $(x^{2^{e-2}T} - 1)\alpha_{e-1} = h_2(x)\alpha_0$, $(x^{2^{e-2}T} - 1)\beta_{e-1} = h_2(x)\beta_0$ and the periods of $\eta(\alpha_0, \ldots, \alpha_{e-2})$ and $\eta(\beta_0, \ldots, \beta_{e-2})$ divide $2^{e-2}T$. So $h_2(x)(\alpha_0 + \beta_0)h_2(x)\alpha_0 = \mathbf{0}$ which implies $\alpha_0 + \beta_0 = \mathbf{0}$ since $\alpha_0 + \beta_0$ is $\mathbf{0}$ or an ML-sequence. Thus $\alpha_0 = \beta_0$.*

If $e = 3$, then $\varphi(\alpha_0, \alpha_1, \alpha_2) + \varphi(\beta_0, \beta_1, \beta_2) = \alpha_2 + \beta_2 + \eta(\alpha_0, \alpha_1) + \eta(\beta_0, \beta_1)$. The period of $\alpha_1 + \beta_1$ divides T since $\alpha_0 = \beta_0$. So the period of $\eta(\alpha_0, \alpha_1) + \eta(\beta_0, \beta_1)$ divides T. Thus the period of $(\eta(\alpha_0, \alpha_1) + \eta(\beta_0, \beta_1))h_2(x)\alpha_0$ divides T. $x^T - 1$ acts on

$$(\alpha_2 + \beta_2 + \eta(\alpha_0, \alpha_1) + \eta(\beta_0, \beta_1))h_2(x)\alpha_0 = \mathbf{0} \tag{8}$$

then $\mathbf{0} = (x^T - 1)((\alpha_2 + \beta_2)h_2(x)\alpha_0) = (x^T - 1)(\alpha_2 + \beta_2)h_2(x)\alpha_0$. And by lemma 3, we have

$$(\alpha_1 + \beta_1)h_1(x)\alpha_0 h_2(x)\alpha_0 = h_1(x)(\alpha_1 + \beta_1)h_2(x)\alpha_0$$

Thus $\alpha_1 = \beta_1$ by lemma 4. So $(\alpha_2 + \beta_2)h_2(x)\alpha_0 = \mathbf{0}$ by (8). $\alpha_2 + \beta_2$ is $\mathbf{0}$ or an ML-sequence since $\alpha_1 = \beta_1$ and $\alpha_0 = \beta_0$. Therefore $\alpha_2 = \beta_2$ because the product of two ML-sequences over $GF(2)$ is not $\mathbf{0}$.

If $e > 3$, set

$$\begin{aligned} \eta_{e-2}(x_0, \ldots, x_{e-2}) &= \eta(x_0, \ldots, x_{e-2}) \\ &= x_{e-2}\eta_{e-3}(x_0, \ldots, x_{e-3}) + \mu_{e-3}(x_0, \ldots, x_{e-3}) \end{aligned}$$

and in general, we set

$$\eta_k(x_0, \ldots, x_k) = x_k \eta_{k-1}(x_0, \ldots, x_{k-1}) + \mu_{k-1}(x_0, \ldots, x_{k-1})$$

$k = e-2, e-3, \ldots, 2$. $x^{2^{e-3}T} - 1$ acts on (7), we have

$$\begin{aligned} &(x^{2^{e-3}T} - 1)(\alpha_{e-1} + \beta_{e-1} + \alpha_{e-2}\eta_{e-3}(\alpha_0, \ldots, \alpha_{e-3}) \\ + \;& \beta_{e-2}\eta_{e-3}(\beta_0, \ldots, \beta_{e-3}))h_2(x)\alpha_0 = \mathbf{0} \end{aligned}$$

that is

$$(x^{2^{e-3}T} - 1)(\alpha_{e-1} + \beta_{e-1} + \eta_{e-3}(\alpha_0, \ldots, \alpha_{e-3}) + \eta_{e-3}(\beta_0, \ldots, \beta_{e-3}))h_2(x)\alpha_0 = \mathbf{0}$$

By lemma 3,

$$\begin{aligned}&((\alpha_{e-2}+\beta_{e-2})h_2(x)\alpha_0+h_2(x)(\alpha_1+\beta_1)\\ +\quad&\eta_{e-3}(\alpha_0,\ldots,\alpha_{e-3})+\eta_{e-3}(\beta_0,\ldots,\beta_{e-3}))h_2(x)\alpha_0=\mathbf{0}\end{aligned}$$

that is

$$\begin{aligned}&((\alpha_{e-2}+\beta_{e-2}+\eta_{e-3}(\alpha_0,\ldots,\alpha_{e-3})+\eta_{e-3}(\beta_0,\ldots,\beta_{e-3}))h_2(x)\alpha_0\\ =\quad&h_2(x)(\alpha_1+\beta_1)h_2(x)\alpha_0\end{aligned}\tag{9}$$

If $e>4$, $x^{2^{e-4}T}-1$ *acts on (9) continuously, and so on, then we get*

$$\begin{aligned}&((\alpha_k+\beta_k+\eta_{k-1}(\alpha_0,\ldots,\alpha_{k-1})+\eta_{k-1}(\beta_0,\ldots,\beta_{k-1}))h_2(x)\alpha_0\\ =\quad&h_2(x)(\alpha_1+\beta_1)h_2(x)\alpha_0\end{aligned}\tag{10}$$

where $k=e-2,e-3,\ldots,2$. *Finally,* x^T-1 *acts on*

$$((\alpha_2+\beta_2+\eta_1(\alpha_0,\alpha_1)+\eta_1(\beta_0,\beta_1))h_2(x)\alpha_0=h_2(x)(\alpha_1+\beta_1)h_2(x)\alpha_0$$

and we get $(\alpha_1+\beta_1)h_1(x)\alpha_0h_2(x)\alpha_0=h_1(x)(\alpha_1+\beta_1)h_2(x)\alpha_0$. *So* $\alpha_1=\beta_1$ *by lemma 4 and* $\alpha_k=\beta_k$ *by (10),* $k=2,3,\ldots.e-2$. *Lastly,* $\alpha_{e-1}=\beta_{e-1}$ *by (7). Therefore* $\alpha=\beta$. □

Corollary 2 *Let* $f(x)$ *be a strongly primitive polynomial of degree* n *over* $Z/(2^e)$, $e\geq 3$, $\varphi(x_0,\ldots,x_{e-1})=x_{e-1}+\eta(x_0,\ldots,x_{e-2})$ *is a Boolean function of* e *variables, then for* $\alpha,\beta\in S(f(x))_{2^e},\alpha=\beta$ *if and only if* $\varphi(\alpha_0,\ldots,\alpha_{e-1})=\varphi(\beta_0,\ldots,\beta_{e-1})$

Theorem 7 *Let* $f(x)$ *be a strongly primitive polynomial of degree* n *over* $Z/(2^e)$, $e\geq 3$, $\varphi(x_0,x_1,\ldots,x_{e-1})$ *is a Boolean function of* e *variables containing* x_{e-1}, *and* $x_{k_0}x_{k_1}\ldots x_{k_{t-1}}$ *is the term of the maximal order in* $\varphi(x_0,x_1,\ldots,x_{e-1})$. *If* $x_{k_0}x_{k_1}\ldots x_{k_{t-1}}$ *is not divided by* x_0 *and* x_1, *i.e.* $k_0\geq 2$, *then the compression mapping*

$$\varphi:\begin{cases}S(f(x))_{2^e}\to GF(2)^\infty\\ \alpha=\alpha_0+\alpha_12+\ldots+\alpha_{e-1}2^{e-1}\mapsto\varphi(\alpha_0,\ldots,\alpha_{e-1})\end{cases}$$

is injective, i.e., for $\alpha,\beta\in S(f(x))_{2^e}$, *then* $\alpha=\beta$ *if and only if* $\varphi(\alpha_0,\ldots,\alpha_{e-1})=\varphi(\beta_0,\ldots,\beta_{e-1})$.

Proof *If* $t=1$, *the result follows immediately from corollary 2. Assume* $t>1$ *in the following.*

Let $\alpha,\beta\in S(f(x))_{2^e}$ *and* $\varphi(\alpha_0,\ldots,\alpha_{e-1})=\varphi(\beta_0,\ldots,\beta_{e-1})$, *then* $\alpha_0=\beta_0$ *by lemma 2.*

$\varphi(x_0,x_1,\ldots,x_{e-1})$ *contains* x_{e-1}, *that is,* $k_{t-1}=e-1$, *so let*

$$\varphi(x_0,\ldots,x_{e-1})=x_{e-1}\eta(x_0,\ldots,x_{e-2})+\lambda(x_0,\ldots,x_{e-2})\tag{11}$$

where $\eta(x_0,\ldots,x_{e-2}) \neq 0$. *The term of maximal order in* $\eta(x_0,\ldots,x_{e-2})$ *is* $x_{k_0}x_{k_1}\ldots x_{k_{t-2}}$. *Thus we set* $\eta_{k_{t-2}}(x_0,\ldots,x_{k_{t-2}}) = \eta(x_0,\ldots,x_{e-2})$ *and*

$$\eta_{k_{t-2}}(x_0,\ldots,x_{k_{t-2}}) = x_{k_{t-2}}\eta_{k_{t-3}}(x_0,\ldots,x_{k_{t-3}}) + \mu_{k_{t-2}-1}(x_0,\ldots,x_{k_{t-2}-1})$$

In general, we set

$$\eta_{k_s}(x_0,\ldots,x_{k_s}) = x_{k_s}\eta_{k_{s-1}}(x_0,\ldots,x_{k_{s-1}}) + \mu_{k_s-1}(x_0,\ldots,x_{k_s-1}) \tag{12}$$

where $s = t-2, t-1, \ldots, 2, 1$, *and*

$$\eta_{k_0}(x_0,\ldots,x_{k_0}) = x_{k_0} + \mu_{k_0-1}(x_0,\ldots,x_{k_0-1}) \tag{13}$$

Set $g_i(x) = \prod_k (x^{2^{k-1}T} - 1)$, *where* k *takes over* $k_i, k_{i+1}, \ldots, k_{t-1}$ *and* $i = 1, 2, \ldots, t-1$. $g_1(x)$ *acts on* $\varphi(\alpha_0,\ldots,\alpha_{e-1}) = \varphi(\beta_0,\ldots,\beta_{e-1})$, *then, by (11), (12) and (13), we get*

$$(\alpha_{k_0} + \beta_{k_0} + \mu_{k_0-1}(\alpha_0,\ldots,\alpha_{k_0-1}) + \mu_{k_0-1}(\beta_0,\ldots,\beta_{k_0-1}))h_2(x)\alpha_0 = \mathbf{0}$$

So $\alpha = \beta \pmod{2^{k_0+1}}$ *by theorem 6.*

(i) If $t = 2$, *then*

$$\begin{aligned} & \alpha_{e-1}\eta_{k_0}(\alpha_0,\ldots,\alpha_{k_0}) + \beta_{e-1}\eta_{k_0}(\beta_0,\ldots,\beta_{k_0}) \\ + \quad & \lambda(\alpha_0,\ldots,\alpha_{e-2}) + \lambda(\beta_0,\ldots,\beta_{e-2}) = \mathbf{0} \end{aligned}$$

that is

$$(\alpha_{e-1} + \beta_{e-1})\eta_{k_0}(\alpha_0,\ldots,\alpha_{k_0}) + \lambda(\alpha_0,\ldots,\alpha_{e-2}) + \lambda(\beta_0,\ldots,\beta_{e-2}) = \mathbf{0} \tag{14}$$

By lemma 3

$$\begin{aligned} (x^{2^{e-3}T} - 1)(\alpha_{e-1} + \beta_{e-1}) &= (\alpha_{e-2} + \beta_{e-2})h_2(x)\alpha_0 + h_2(x)(\alpha_1 + \beta_1) \\ &= (\alpha_{e-2} + \beta_{e-2})h_2(x)\alpha_0 \end{aligned}$$

$x^{2^{e-3}T} - 1$ *acts on (14) if* $e - 3 > k_0$, *then by the period of* $\eta_{k_0}(\alpha_0,\ldots,\alpha_{k_0})$ *dividing* $2^{e-3}T$,

$$\begin{aligned} & (\alpha_{e-2} + \beta_{e-2})h_2(x)\alpha_0\eta_{k_0}(\alpha_0,\ldots,\alpha_{k_0}) \\ + \quad & (\lambda_{e-3}(\alpha_0,\ldots,\alpha_{e-3}) + \lambda_{e-3}(\beta_0,\ldots,\beta_{e-3}))h_2(x) = \mathbf{0} \end{aligned}$$

that is

$$\begin{aligned} & ((\alpha_{e-2} + \beta_{e-2})\eta_{k_0}(\alpha_0,\ldots,\alpha_{k_0}) \\ + \quad & \lambda_{e-3}(\alpha_0,\ldots,\alpha_{e-3}) + \lambda_{e-3}(\beta_0,\ldots,\beta_{e-3}))h_2(x) = \mathbf{0} \end{aligned} \tag{15}$$

where $\lambda_{e-3}(x_0,\ldots,x_{e-3})$ *is determined by*

$$\begin{aligned} & \lambda_{e-2}(x_0,\ldots,x_{e-2}) = \lambda(x_0,\ldots,x_{e-2}) \\ = \quad & x_{e-2}\lambda_{e-3}(x_0,\ldots,x_{e-3}) + \sigma_{e-3}(x_0,\ldots,x_{e-2}) \end{aligned}$$

$x^{2^{e-4}} - 1$ *acts on (15) continuously if* $e-4 \geq k_0$. *In general we have*

$$((\alpha_k + \beta_k)\eta_{k_0}(\alpha_0, \ldots, \alpha_{k_0}) + \lambda_{k-1}(\alpha_0, \ldots, \alpha_{k-1}) + \lambda_{k-1}(\beta_0, \ldots, \beta_{k-1}))h_2(x) = \mathbf{0} \tag{16}$$

where $k = e-2, \ldots, k_0+2, k_0+1$. $\lambda_{k_0}(\alpha_0, \ldots, \alpha_{k_0}) = \lambda_{k_0}(\beta_0, \ldots, \beta_{k_0})$ *since* $\alpha = \beta \pmod{2^{k_0+1}}$.

By the case $k = k_0 + 1$ *in (16), we have*

$$(\alpha_{k_0+1} + \beta_{k_0+1})\lambda_{k_0}(\alpha_0, \ldots, \alpha_{k_0})h_2(x)\alpha_0 = \mathbf{0} \tag{17}$$

Since $(\alpha_{k_0+1} + \beta_{k_0+1})$ *is* $\mathbf{0}$ *or an ML-sequence over* $GF(2)$ *and* $k_0 \geq 2$, *if* $x^{2^{k-1}T} - 1$ *acts on (17), where* $k = k_0$, *then*

$$[(x^{2^{k-1}T} - 1)\eta_{k_0}(\alpha_0, \ldots, \alpha_{k_0})](\alpha_{k_0+1} + \beta_{k_0+1})h_2(x)\alpha_0 = \mathbf{0} \tag{18}$$

By $\eta_{k_0}(\alpha_0, \ldots, \alpha_{k_0}) = x_{k_0} + \mu_{k_0-1}(\alpha_0, \ldots, \alpha_{k_0-1})$, *(18) implies*

$$(\alpha_{k_0+1} + \beta_{k_0+1})h_2(x)\alpha_0 = \mathbf{0}$$

So $\alpha_{k_0+1} = \beta_{k_0+1}$. *And by (16), we obtain* $\alpha_k = \beta_k$, $k = k_0+1, \ldots, e-2$. *Finally,* $\alpha_{e-1} = \beta_{e-1}$ *by (14).*

(ii) If $t = 3, g_2(x)$ *acts on* $\varphi(\alpha_0, \ldots, \alpha_{e-1}) = \varphi(\beta_0, \ldots, \beta_{e-1})$, *then*

$$(\alpha_{k_1}\eta_{k_0}(\alpha_0, \ldots, \alpha_{k_0}) + \beta_{k_1}\eta_{k_0}(\beta_0, \ldots, \beta_{k_0}))h_2(x)\alpha_0 = \mathbf{0}$$

that is

$$(\alpha_{k_1} + \beta_{k_1})\eta_{k_0}(\alpha_0, \ldots, \alpha_{k_0})h_2(x)\alpha_0 = \mathbf{0} \tag{19}$$

As in case (i), $r_k(x) = \prod_{i=k}^{k_1-1}(x^{2^{i-1}T} - 1)$ *acts on (19), then we obtain*

$$(\alpha_k + \beta_k)\eta_{k_0}(\alpha_0, \ldots, \alpha_{k_0})h_2(x)\alpha_0 = \mathbf{0} \tag{20}$$

$k = k_1 - 1, \ldots, k_0+2, k_0+1$. *So* $(\alpha_{k_0+1} + \beta_{k_0+1})\eta_{k_0}(\alpha_0, \ldots, \alpha_{k_0})h_2(x)\alpha_0 = \mathbf{0}$. *By the process of proof in (i), we have* $\alpha_{k_0+1} = \beta_{k_0+1}$. *Thus* $\alpha_j = \beta_j, j = k_0+2, \ldots, k_1$, *by (19) and (20).*

Finally, as $r_k(x)$ *acts on (19),* $s_k(x) = \prod_{i=k}^{e-2}(x^{2^{i-1}T} - 1)$ *acts on,*

$$(\alpha_{e-1} + \beta_{e-1})\eta_{k_1}(\alpha_0, \ldots, \alpha_{k_1}) + \lambda(\alpha_0, \ldots, \alpha_{e-2}) + \lambda(\beta_0, \ldots, \beta_{e-2}) = \mathbf{0}$$

Similarly, we get $\alpha_j = \beta_j, j = k_1+1, \ldots, e-1$. *Therefore* $\alpha = \beta$. □

References

[1] M.Q.Huang, Analysis and Cryptologic Evaluation of Primitive Sequences over an Integer Residue Ring, Doctoral Dissertation of Graduate School of USTC, Academia Sinica. 1988.

[2] Z.D.Dai, M.Q.Huang, A Criterion for Primitiveness of Polynomials over $Z/(2^d)$, Chinese Science Bulletin, Vol.36,No.11,June 1991.pp.892-895.

[3] Z.D.Dai and M.Q.Huang, Linear Complexity and the Minimal Polynomials of Linear Recurring Sequences Over $Z/(m)$, System Science and Mathematical Science, Vol.4,No.1,Feb.1991. pp.51-54.

[4] Z.D.Dai, Beth T., Gollman D, Lower Bounds for the Linear Complexity of Sequences over Residue Rings, Advances in Cryptology-EUROCRYPT'90, Spring-Verlag LNCS 473 (1991), Editor: I.B. Damgard. pp.189-195.

[5] Z.D.Dai, Binary Sequences Derived from ML-Sequences over Rings I:Periods and Minimal Polynomials, J. Cryptology, Vol 5, No4, 1992, pp.193-207.

[6] M.Q.Huang, Z.D.Dai, Projective Maps of Linear Recurring Sequences with Maximal p-adic Periods, Fibonacci Quart 30(1992), No.2, pp.139-143.

[7] K.C.Zeng, Z.D.Dai and M.Q.Huang, Injectiveness of Mappings from Ring Sequences to Their Sequences of Significant Bits, Symposium on Problems of Cryptology, State Key Laboratory of Information Security, Beijing, China, 1995,pp.132-141.

[8] W.F.Qi, J.J.Zhou, Distribution of 0 and 1 in Highst Level of Primitive Sequences over $Z/(2^e)$, Science in China, Series A, 40(6),1997,606-611.

[9] W.F.Qi, J.J.Zhou, Distribution of 0 and 1 in Highst Level of Primitive Sequences over $Z/(2^e)$ (II), Chinese Science Bulletin, 43(8),1998, 633-635.

[10] W.F.Qi, Compressing Maps of Primitive Sequences over $Z/(2^e)$ and Analysis of Their Derivative Sequences, Doctoral Dissertation of ZhengZhou Information Engineering Institute, 1997.