Compressing Mappings on Primitive Sequences over $\mathbb{Z}/(2^e)$ and Its Galois Extension$^1$

Qi Wenfeng$^2$ and Zhu Xuanyong

Department of Applied Mathematics, Zhengzhou Information Engineering University,
P.O. Box 1001-745, Zhengzhou, 450002, People’s Republic of China
E-mail: wenfeng.qi@263.net, zhuxuanyong@263.net

Communicated by Rudolf Lidl

Received March 11, 2001; revised February 10, 2002; published online June 25, 2002

Let $f(x)$ be a strongly primitive polynomial of degree $n$ over $\mathbb{Z}/(2^e)$, $\eta(x_0, x_1, \ldots, x_{e-2})$ a Boolean function of $e - 1$ variables and

$$\varphi(x_0, x_1, \ldots, x_{e-1}) = x_{e-1} + \eta(x_0, x_1, \ldots, x_{e-2})$$

$G(f(x), Z/(2^e))$ denotes the set of all sequences over $\mathbb{Z}/(2^e)$ generated by $f(x)$, $F_2^\infty$ the set of all sequences over the binary field $F_2$, then the compressing mapping

$$\Phi : \begin{cases} G(f(x), Z/(2^e)) \rightarrow F_2^\infty, \\ a = a_0 + a_1 2 + \cdots + a_{e-1} 2^{e-1} \mapsto \varphi(a_0, a_1, \ldots, a_{e-1}) \mod 2 \end{cases}$$

is injective, that is, for $a, b \in G(f(x), Z/(2^e))$, $a = b$ if and only if $\Phi(a) = \Phi(b)$, i.e., $\varphi(a_0, \ldots, a_{e-1}) = \varphi(b_0, \ldots, b_{e-1}) \mod 2$. In the second part of the paper, we generalize the above result over the Galois rings.

Key Words: primitive polynomial; Galois ring; linear sequence; compressing mapping.

1. INTRODUCTION

Let $R$ be a ring, $f(x) = x^n + c_{n-1} x^{n-1} + \cdots + c_0$ a monic polynomial over $R$, the sequence $a = (a_0, a_1, a_2, \ldots)$ over $R$ satisfying the recursion

$$a_{i+n} = -(c_0 a_i + c_1 a_{i+1} + \cdots + c_{n-1} a_{i+n-1}), \quad i = 0, 1, 2, \ldots$$

$^1$The work is supported by HAIPURT and the Special Fund of National Excellently Doctoral Paper.

$^2$To whom correspondence should be addressed.
is called a linear recurring sequence of degree $n$ over $R$, generated by $f(x)$. We will use the notation $G(f(x), R)$ for the set of all sequences over $R$ generated by $f(x)$.

Let $a = (a_0, a_1, a_2, \ldots)$ and $b = (b_0, b_1, b_2, \ldots)$ be sequences over $R$ and $c \in R$, define

$$a + b = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots),$$
$$c_0 = (c_0 a_0, c_1 a_1, c_2 a_2, \ldots),$$
$$c_0 b = (a_0 b_0, a_1 b_1, a_2 b_2, \ldots)$$

and the shift operator $x$ of sequence as $x a = (a_1, a_2, a_3, \ldots)$ and $x^k a = (a_k, a_{k+1}, a_{k+2}, \ldots)$ for $k = 0, 1, 2, \ldots$. Then for any polynomial $f(x)$ over $R$, $a \in G(f(x), R)$ if and only if $f(x) a = 0$.

Let $f(x)$ be a monic polynomial of degree $n$ over $Z/(2^e)$ with $f(0) \neq 0 \mod 2$, then there exists a positive integer $P$ such that $f(x)$ divides $x^P - 1$ over $Z/(2^e)$. The least such $P$ is called the period of $f(x)$ over $Z/(2^e)$ and denoted by $\text{per}(f(x))$. The period of $f(x)$ is upper bounded by $2^{e-1}(2^n - 1)$, where $n = \deg f(x)$. A monic polynomial $f(x)$ of degree $n$ over $Z/(2^e)$ is called a primitive polynomial if $\text{per}(f(x)) = 2^{e-1}(2^n - 1)$.

Let $f(x)$ be a primitive polynomial of degree $n$ over $Z/(2^e)$, $T = 2^n - 1$, then $f(x) \mod 2$ is a primitive polynomial over the binary field $\mathbb{F}_2$ and for $i = 1, 2, \ldots, e - 1$, we have

$$x^{2^i - T} - 1 \equiv 2^i h_i(x) \mod f(x), \quad (1)$$

where $h_i(x)$ is a polynomial over $Z/(2^e)$ of degree less than $n$ such that $h_i(x) \not\equiv 0 \mod 2$. Furthermore,

$$h_2(x) \equiv \cdots \equiv h_{e-1}(x) \mod 2,$$

$$h_2(x) \equiv h_1(x) + h_1(x)^2 \mod (2, f(x)). \quad (2)$$

If $e \geq 3$ and $h_2(x) \not\equiv 1 \mod 2$ or $e = 2$ and $h_1(x) \not\equiv 1 \mod 2$, then $f(x)$ is called a strongly primitive polynomial over $Z/(2^e)$ (see [1, 3]).

Any element $a$ in $Z/(2^e)$ has a unique binary decomposition as $a = a_0 + a_1 2 + \cdots + a_{e-1} 2^{e-1}$, $a_i \in \{0, 1\}$. Similarly, a sequence $a$ over $Z/(2^e)$ has a unique binary decomposition as $a = a_0 + a_1 2 + \cdots + a_{e-1} 2^{e-1}$, where $a_i = (a_{i0}, a_{i1}, a_{i2}, \ldots)$ is a binary sequence over $\{0, 1\}$. The sequence $a_i$ is called the $i$th level component of $a$, and $a_{e-1}$ the highest level component of $a$.

There are many papers to discuss the properties of the level component of $a$, please refer to [1–5, 7, 8].
In the first part of the paper, we prove the following result. Let $f(x)$ be a strongly primitive polynomial of degree $n$ over $\mathbb{Z}/(2^e)$, $\eta(x_0, x_1, \ldots, x_{e-2})$ a Boolean function of $e - 1$ variables and

$$\varphi(x_0, x_1, \ldots, x_{e-1}) = x_{e-1} + \eta(x_0, x_1, \ldots, x_{e-2}).$$

$F_2^\infty$ denotes the set of all sequences over the binary field $F_2$, then the compressing map

$$\Phi : \begin{cases} G(f(x), \mathbb{Z}/(2^e)) \rightarrow F_2^\infty, \\ a = a_0 + a_12 + \cdots + a_{e-1}2^{e-1} \mapsto \varphi(a_0, a_1, \ldots, a_{e-1}) \mod 2 \end{cases}$$

is injective, that is, for $a, b \in G(f(x), \mathbb{Z}/(2^e))$, $a = b$ if and only if $\varphi(a_0, \ldots, a_{e-1}) \equiv \varphi(b_0, \ldots, b_{e-1}) \mod 2$.

In the second part of the paper, we generalize the above result to the one over Galois rings.

2. INJECTIVENESS OF COMPRESSION MAPPINGS OVER $\mathbb{Z}/(2^e)$

Huang [3] and Huang and Dai [4] proposed the following injectiveness theorem.

**Theorem 1.** Let $f(x)$ be a primitive polynomial over $\mathbb{Z}/(2^e)$, then the mapping

$$\Phi : \begin{cases} G(f(x), \mathbb{Z}/(2^e)) \rightarrow F_2^\infty, \\ a = a_0 + a_12 + \cdots + a_{e-1}2^{e-1} \mapsto a_{e-1} \end{cases}$$

is injective, that is, for $a, b \in G(f(x), \mathbb{Z}/(2^e))$, $a = b$ if and only if $a_{e-1} = b_{e-1}$.

**Remark 1.** Theorem 1 implies that $a_{e-1}$ contains all information of the original sequence $a$.

**Lemma 1** (Dai [1]). Let $f(x)$ be a primitive polynomial of degree $n$ over $\mathbb{Z}/(2^e)$, $T = 2^n - 1$, $a = a_0 + a_12 + \cdots + a_{e-1}2^{e-1} \in G(f(x), \mathbb{Z}/(2^e))$ and $a_0 \neq 0$, then $\per(a_i) = 2^iT$, especially $\per(a_{e-1}) = 2^{e-1}T = \per(a) = \per(f(x))$.

**Lemma 2** (Dai [1]). Let $f(x)$ be a primitive polynomial of degree $n$ over $\mathbb{Z}/(2^e)$, $T = 2^n - 1$, $a = a_0 + a_12 + \cdots + a_{e-1}2^{e-1} \in G(f(x), \mathbb{Z}/(2^e))$, then $(x^{2^{i-1}T} - 1)a_i \equiv h_i(x)a_0 \mod 2$ for $i = 1, 2, \ldots, e - 1$. That is, by (2),

$$(x^{2^{i-1}T} - 1)a_i \equiv \begin{cases} h_1(x)a_0 \mod 2 & \text{if } i = 1, \\ h_2(x)a_0 \mod 2 & \text{if } i \geq 2. \end{cases}$$
Lemma 3. Let $S$ be a positive integer, $y$ a sequence over the ring $R$ with its period dividing $S$, then for any sequence $v$ over $R$, $(x^S - 1)(v) = y(x^S - 1)v$.

The proof is easy.

Lemma 4. Let $f(x)$ be a primitive polynomial of degree $n$ over the finite field $F_2$, and $g = (a_0, a_1, \ldots) \in G(f(x), F_2)$. If $a$, $b$, and $c$ are linear independent over $F_2$, then the number of zeros in \{ $a_0 b_0, a_1 b_1, \ldots, a_{T-1} b_{T-1}$ \} is smaller than the one in \{ $a_0 b_0 c_0, a_1 b_1 c_1, \ldots, a_{T-1} b_{T-1} c_{T-1}$ \}, where $T = 2^n - 1$. Thus $a b \neq a c$.

The proof is easy.

Lemma 5. Let $f(x)$ be a primitive polynomial of degree $n$ over $\mathbb{Z}/(2^e)$, $\eta(x_0, x_1, \ldots, x_{e-2})$ a Boolean function of $e - 1$ variables and

$$\varphi(x_0, x_1, \ldots, x_{e-1}) = x_{e-1} + \eta(x_0, x_1, \ldots, x_{e-2}).$$

If $\varphi(a_0, \ldots, a_{e-1}) \equiv \varphi(b_0, \ldots, b_{e-1}) \mod 2$ for $a, b \in G(f(x), \mathbb{Z}/(2^e))$, then $a_0 \equiv b_0$.

Proof. Set $T = 2^n - 1$. The periods of $\eta(a_0, \ldots, a_{e-2})$ and $\eta(b_0, \ldots, b_{e-2})$ divide $2^{e-2} T$, so, by $x^{2^{e-2} T} - 1$ acting on $\varphi(a_0, \ldots, a_{e-1}) \equiv \varphi(b_0, \ldots, b_{e-1})$ mod 2, we get

$$(x^{2^{e-2} T} - 1) a_{e-1} \equiv (x^{2^{e-2} T} - 1) b_{e-1} \mod 2.$$

Since $\text{per}(g_i) = 2^i T$ for $0 \leq i \leq e - 2$, by $x^{2^{e-2} T} - 1 \equiv 2^{e-1} h_{e-1}(x) \mod f(x)$ acting on $g$ and $b$, respectively, we have

$$(x^{2^{e-2} T} - 1) a_{e-1} \cdot 2^{e-1} = 2^{e-1} h_{e-1}(x) g_0,$$

$$(x^{2^{e-2} T} - 1) b_{e-1} \cdot 2^{e-1} = 2^{e-1} h_{e-1}(x) b_0,$$

that is,

$$(x^{2^{e-2} T} - 1) a_{e-1} \equiv h_{e-1}(x) g_0 \mod 2,$$

$$(x^{2^{e-2} T} - 1) b_{e-1} \equiv h_{e-1}(x) b_0 \mod 2.$$

So $h_{e-1}(x) g_0 \equiv h_{e-1}(x) b_0 \mod 2$. Since $h_{e-1}(x) \neq 0 \mod(2, f(x))$, we have $a_0 = b_0$. $\blacksquare$

Theorem 2. Let $f(x)$ be a strongly primitive polynomial of degree $n$ over $\mathbb{Z}/(2^e)$, $\eta(x_0, x_1, \ldots, x_{e-2})$ a Boolean function of $e - 1$ variables and

$$\varphi(x_0, x_1, \ldots, x_{e-1}) = x_{e-1} + \eta(x_0, x_1, \ldots, x_{e-2}),$$

\begin{itemize}
  \item \end{itemize}
then the compressing map

\[
\Phi : \begin{cases} 
G(f(x), Z/(2^e)) \rightarrow F_2^\infty, \\
\bar{a} = a_0 + a_12 + \cdots + a_{e-1}2^{e-1} \mapsto \phi(a_0, a_1, \ldots, a_{e-1}) \mod 2
\end{cases}
\]

is injective, that is, for \(a, b \in G(f(x), Z/(2^e))\), \(a = b\) if and only if \(\phi(a_0, \ldots, a_{e-1}) \equiv \phi(b_0, \ldots, b_{e-1}) \mod 2\).

\textbf{Proof.} Let \(a, b \in G(f(x), Z/(2^e))\) with \(\phi(a_0, \ldots, a_{e-1}) \equiv \phi(b_0, \ldots, b_{e-1}) \mod 2\) we shall prove \(a = b\). Since \(h_2(x) \equiv \cdots \equiv h_{e-1}(x) \mod 2\), we set \(h(x) = h_2(x) \mod 2\) which is a polynomial over the field \(F_2\).

Since \(a_0 = b_0\) by Lemma 5, it suffices to consider the case \(a_0 = b_0 \neq 0\). Set \(\eta_{e-2}(x_0, x_1, \ldots, x_{e-2}) = \eta(x_0, x_1, \ldots, x_{e-2})\), then

\[
\eta_{e-2}(x_0, x_1, \ldots, x_{e-2}) = x_{e-2}\eta_{e-3}(x_0, x_1, \ldots, x_{e-3}) + \psi_{e-3}(x_0, x_1, \ldots, x_{e-3}).
\]

In general, we have

\[
\eta_i(x_0, x_1, \ldots, x_i) = x_i\eta_{i-1}(x_0, x_1, \ldots, x_{i-1}) + \psi_{i-1}(x_0, x_1, \ldots, x_{i-1}),
\]

where \(\eta_{i-1}(x_0, x_1, \ldots, x_{i-1})\) and \(\psi_{i-1}(x_0, x_1, \ldots, x_{i-1})\) are Boolean functions with \(i\) variables, \(i = 1, 2, \ldots, e - 1\).

Firstly, we consider the case \(e \geq 4\). Since

\[
a_{e-1} + a_{e-2}\eta_{e-3}(a_0, \ldots, a_{e-3}) + \psi_{e-3}(a_0, \ldots, a_{e-3})
\]

\[
\equiv b_{e-1} + b_{e-2}\eta_{e-3}(b_0, \ldots, b_{e-3}) + \psi_{e-3}(b_0, \ldots, b_{e-3}) \mod 2
\]

and the periods of \(\psi_{e-3}(a_0, \ldots, a_{e-3})\) and \(\psi_{e-3}(b_0, \ldots, b_{e-3})\) divide \(2^{e-3}T\), it follows

\[
(x^{2^{e-3}T} - 1)\psi_{e-3}(a_0, \ldots, a_{e-3}) \equiv 0 \mod 2,
\]

\[
(x^{2^{e-3}T} - 1)\psi_{e-3}(b_0, \ldots, b_{e-3}) \equiv 0 \mod 2
\]

and

\[
(x^{2^{e-3}T} - 1)(a_{e-1} + a_{e-2}\eta_{e-3}(a_0, \ldots, a_{e-3}))
\]

\[
\equiv (x^{2^{e-3}T} - 1)(b_{e-1} + b_{e-2}\eta_{e-3}(b_0, \ldots, b_{e-3})) \mod 2.
\]
implies
\[(x^{2^{e-3}T} - 1)q_{e-1} + \eta_{e-3}(q_0, \ldots, q_{e-3})h(x)q_0 \equiv (x^{2^{e-3}T} - 1)b_{e-1} + \eta_{e-3}(b_0, \ldots, b_{e-3})h(x)q_0 \bmod 2,\]

that is,
\[(x^{2^{e-3}T} - 1)(a_{e-1} + b_{e-1}) \equiv [\eta_{e-3}(q_0, \ldots, q_{e-3}) + \eta_{e-3}(b_0, \ldots, b_{e-3})]h(x)q_0 \bmod 2. \tag{5}\]

On the other hand, by \(x^{2^{e-3}T} - 1 \equiv 2^{e-2}h_{e-2}(x) \bmod f(x)\) acting on \(a = q_0 + q_12 + \cdots + q_{e-1}2^{e-1}\), we get
\[(x^{2^{e-3}T} - 1)(a_{e-2} + q_{e-1}2)2^{e-2} \equiv 2^{e-2}h_{e-2}(x)(q_0 + q_12),\]

that is,
\[(x^{2^{e-3}T} - 1)(a_{e-2} + q_{e-1}2) \equiv h_{e-2}(x)(q_0 + q_12) \bmod 2^2. \tag{6}\]

Let \(h_{e-2}(x)(q_0 + q_12) \equiv u + v2 \bmod 2^2\), where \(u\) and \(v\) are the 0th and 1th level components of \(h_{e-2}(x)(q_0 + q_12)\), respectively, then \(u \equiv h(x)q_0 \bmod 2\). By (6),
\[x^{2^{e-3}T}a_{e-2} + (x^{2^{e-3}T} - 1)a_{e-1}2 \equiv a_{e-2} + u + v2 \bmod 2^2\]

and so
\[(x^{2^{e-3}T} - 1)a_{e-1} \equiv v + a_{e-2} \cdot u \bmod 2. \tag{7}\]

Similarly,
\[(x^{2^{e-3}T} - 1)b_{e-1} \equiv w + b_{e-2} \cdot u \bmod 2, \tag{8}\]

where \(h_{e-2}(x)(b_0 + b_12) \equiv u + w2 \bmod 2^2\) and \(u \equiv h_{e-2}(x)b_0 \equiv h(x)q_0 \bmod 2\). Since \(a_0 = b_0, v + w \equiv h(x)(a_1 + b_1) \bmod 2\). By (7) and (8),
\[(x^{2^{e-3}T} - 1)(a_{e-1} + b_{e-1}) \equiv (a_{e-2} + b_{e-2})h(x)q_0 + h(x)(a_1 + b_1) \bmod 2. \tag{9}\]

Comparing with (5), it follows that
\[(a_{e-2} + b_{e-2})h(x)q_0 \equiv h(x)(a_1 + b_1)[\eta_{e-3}(q_0, \ldots, q_{e-3}) + \eta_{e-3}(b_0, \ldots, b_{e-3})]h(x)q_0 \bmod 2. \tag{10}\]
If \( e \geq 5 \), then \( x^{2e-4T} - 1 \equiv 2^{e-3}h_{e-3}(x) \mod f(x) \) acts on \( \eta = \eta_0 + \eta_12 + \cdots + \eta_{e-1}2^{e-1} \) and \( b = b_0 + b_12 + \cdots + b_{e-1}2^{e-1} \). It follows that
\[
(x^{2e-4T} - 1)(\eta_0 + \eta_12) \equiv h_{e-3}(\eta_0 + \eta_12) \mod 2^2,
\]
(11)
\[
(x^{2e-4T} - 1)(\eta_0 + \eta_12) \equiv h_{e-3}(\eta_0 + \eta_12) \mod 2^2.
\]
(12)

Similar to (9), we get
\[
(x^{2e-4T} - 1)(\eta_0 + \eta_12) \equiv h_{e-3}(\eta_0 + \eta_12) \mod 2.
\]
(13)

Multiplying (13) by \( h(x)\eta_0 \), since \( \text{per}(h(x)\eta_0) \) divides \( T \), we obtain
\[
(x^{2e-4T} - 1)(\eta_0 + \eta_12) h(x)\eta_0 \equiv h(x)(\eta_0 + \eta_12) h(x)\eta_0 \mod 2.
\]
(14)

By (10) and (3), we have
\[
(x^{2e-4T} - 1)(\eta_0 + \eta_12) h(x)\eta_0 \equiv h(x)(\eta_0 + \eta_12) h(x)\eta_0 \mod 2.
\]
(15)

Now, we show \( h(x)(\eta_0 + \eta_12) \equiv h(x)(\eta_0 + \eta_12) \mod 2 \). If \( \eta_1 = \eta_12 \), then
\[
(x^{2e-4T} - 1)(\eta_0 + \eta_12) h(x)\eta_0 \equiv h(x)(\eta_0 + \eta_12) \equiv 0 \mod 2.
\]

If \( \eta_1 \neq \eta_12 \), then 0th level component of \( \eta - \eta_12 \) is 0 and 1th level component \( \eta - \eta_12 \) is \( \eta_0 + \eta_12 \mod 2 \). Thus \( \eta_0 + \eta_12 \) is a primitive sequence generated by \( f(x) \) over \( F_2 \), so is \( h(x)(\eta_0 + \eta_12) \). Let \( h(x)\eta_0 = (u_0, u_1, u_2, \ldots) \) and
\( h(x)(q_1 + b_1) = (s_0, s_1, s_2, \ldots) \) over \( F_2 \), then by (10), \( s_i = 0 \) if \( u_i = 0 \). And since \( h(x)(q_1 + b_1) \) and \( h(x)q_0 \) are primitive sequences generated by \( f(x) \) over \( F_2 \), we get \( h(x)q_0 \equiv h(x)(q_1 + b_1) \mod 2 \), that is \( q_1 + b_1 \equiv q_0 \mod 2 \). So

\[
 h(x)(q_1 + b_1)h(x)q_0 \equiv h(x)(q_1 + b_1) \mod 2.
\]

Then, (15) implies

\[
 (a_{e-3} + b_{e-3})h(x)q_0 \equiv h(x)(q_1 + b_1) + [\eta_{e-4}(q_0, \ldots, a_{e-4}) + \eta_{e-4}(b_0, \ldots, b_{e-4})]h(x)q_0 \mod 2.
\]

In general, we have

\[
 (a_{e-i} + b_{e-i})h(x)q_0 \equiv h(x)(q_1 + b_1) + [\eta_{e-i-1}(q_0, \ldots, a_{e-i-1}) + \eta_{e-i-1}(b_0, \ldots, b_{e-i-1})]h(x)q_0 \mod 2,
\]

where \( i = 2, 3, \ldots, e - 2 \). Finally, by \( x^T - 1 \equiv 2h_1(x) \mod f(x) \) acting on \( a \) and \( b \), similar to (9), we have

\[
 (x^T - 1)(a_2 + b_2) \equiv (a_1 + b_1)(x)q_0 + h_1(x)(q_1 + b_1) \mod 2,
\]

which implies

\[
 (x^T - 1)[(a_2 + b_2)h(x)q_0] \equiv (a_1 + b_1)h(x)q_0 + h_1(x)(q_1 + b_1)h(x)q_0 \mod 2.
\]

On the other hand, by (16) in the case of \( i = e - 2 \),

\[
 (a_2 + b_2)h(x)q_0 \equiv h(x)(q_1 + b_1) + [\eta_1(q_0, q_1) + \eta_1(b_0, b_1)]h(x)q_0 \mod 2
\]

and \( \eta_1(x_0, x_1) = x_1\eta_0(x_0) + \psi_0(x_0) \), we have

\[
 (x^T - 1)[(a_2 + b_2)h(x)q_0] \\
 \equiv (x^T - 1)[(\eta_1(q_0, q_1) + \eta_1(b_0, b_1))h(x)q_0 + h(x)(q_1 + b_1)] \\
 \equiv (x^T - 1)[a_1\eta_0(q_0) + b_1\eta_0(b_0)]h(x)q_0 \\
 \equiv \eta_1(q_0)h(x)q_0(\eta_1(x_0)h(x)q_0 + h_1(x)b_0) \equiv 0 \mod 2.
\]

So (18) implies

\[
 (a_1 + b_1)h_1(x)q_0h(x)q_0 \equiv h_1(x)(q_1 + b_1)h(x)q_0 \mod 2.
\]
If \( a_1 \neq b_1 \), then \( a_1 + b_1 \equiv a_0 \mod 2 \) and the above equation implies
\[
A_0 h_1(x)h_0(x)g_0 \equiv h_1(x)g_0 h(x)g_0 \mod 2.
\] (20)

It is clear that \( a_0, h_1(x)g_0 \) and \( h(x)g_0 \) are linear independent over \( F_2 \), since
\[
h(x) \equiv h_1(x) + h_1(x)^2 \mod 2, \quad h_1(x) \neq 0 \mod 2 \quad \text{and} \quad h(x) \neq 0, 1 \mod 2.
\]
So, by Lemma 4, (20) is not true. Thus \( a_1 = b_1 \) and by (19),
\[
(a_2 + b_2) h(x)g_0 \equiv 0 \mod 2,
\]
which implies \( a_2 = b_2 \). And by (16) again, we have
\[
(h(x)g_0) e_0 \equiv 0 \mod 2,
\]
which implies \( e_0 = b_{e-1} \), \( i = e - 3, e - 4, \ldots, 2 \). Finally \( a_{e-1} = b_{e-1} \) since \( a_k = b_k, k = 0, 1, \ldots, e - 2 \), and \( \varphi(g_0, \ldots, g_{e-1}) \equiv \varphi(h_0, \ldots, h_{e-1}) \mod 2 \). Therefore, \( a = b \).

Secondly, we consider the case \( e = 3 \). We have \( \varphi(x_0, x_1, x_2) = x_2 + \eta(x_0, x_1) \) and \( \eta(x_0, x_1) = x_1 \eta_0(x_0) + \psi_0(x_0) \). Since \( \varphi(g_0, a_1, b_2) \equiv \varphi(b_0, b_1, b_2) \) and \( a_0 = b_0 \), it follows that
\[
a_2 + b_2 \equiv (a_1 + b_1) \eta_0(a_0) \mod 2.
\] (21)

By Lemmas 3 and 2,
\[
(x^T - 1)(a_2 + b_2) \equiv (x^T - 1)((a_1 + b_1) \eta_0(a_0))
\]
\[
\equiv \eta_0(a_0)(x^T - 1)(a_1 + b_1)
\]
\[
\equiv \eta_0(a_0)(h_1(x)g_0 + h_1(x)b_0) \equiv 0 \mod 2.
\]

By (17), we have
\[
h_1(x)(a_1 + b_1) \equiv (a_1 + b_1) h_1(x)g_0 \mod 2.
\]

If \( a_1 + b_1 \equiv 0 \mod 2 \), then \( a_1 + b_1 \mod 2 \) is a primitive sequence over \( F_2 \); and since \( h_1(x) \not\equiv 0 \mod 2 \), \( h_1(x)(a_1 + b_1) \) and \( h_1(x)g_0 \) are also primitive sequences over \( F_2 \). This condition is in contradiction with the above equation. So \( a_1 + b_1 \equiv 0 \mod 2 \), and by (21), we have \( a_2 = b_2 \) and \( a = b \).

Finally, considering the case \( e = 2 \), we have \( \varphi(x_0, x_1) = x_1 + \eta(x_0) \). So \( \varphi(g_0, a_1) \equiv \varphi(b_0, b_1) \mod 2 \) and \( a_0 = b_0 \) imply \( a_1 = b_1 \). Hence \( a = b \).

3. COMPRESSION MAPPINGS OVER GALOIS RINGS

Let \( p \) be a prime, \( Z_p \) the \( p \)-adic integer ring and \( Q_p \) the \( p \)-adic number field. Let \( K \) be an unramified extension of \( Q_p \) with degree \( r \), \( R \) the integer ring of \( K \), then \( GR(p^e, r) = R / p^e R \) is called a Galois ring, where \( e \) is a positive integer.
**Remark 2.** (1) Let \( g(x) \) be a monic polynomial over \( \mathbb{Z}/(p^e) \) with degree \( r \). If \( g(x) \mod p \) is irreducible over \( F_p \), then \( A[x]/(g(x)) \cong \text{GR}(p^e, r) \), where \( A = \mathbb{Z}/(p^e) \).

(2) \( \text{GR}(p^e, 1) = \mathbb{Z}/(p^e) \).

(3) \( \text{GR}(p^e, r) \) is a local ring with the maximal ideal

\[
(p) = p\text{GR}(p^e, r) = \{ px \mid x \in \text{GR}(p^e, r) \}
\]

and \( \text{GR}(p, r) = \text{GR}(p^e, r)/(p) = F_{p^e} \) is a finite field of \( p^e \) elements.

(4) Let \( \Omega = \{ x \in \text{GR}(p^e, r) \mid x^r = x \} \), then \( \Omega \) consists of \( p^e \) elements, which are distinct modulo \( p \). So the mapping \( \Omega \to F_{p^e}, x \mapsto x \mod p \) is bijective. Furthermore, each element \( x \) in \( \text{GR}(p^e, r) \) may be written uniquely as

\[
x = x_0 + x_1 p + \cdots + x_{e-1} p^{e-1},
\]

where \( x_i \in \Omega \). We call \( \Omega \) the \( p \)-adic coordinate set of \( \text{GR}(p^e, r) \) (see [5]).

(5) Let \( \varrho \) be a sequence over \( \text{GR}(p^e, r) \), then \( \varrho \) may be written uniquely as

\[
\varrho = \varrho_0 + \varrho_1 p + \cdots + \varrho_{e-1} p^{e-1},
\]

where \( \varrho_i = (a_{i0}, a_{i1}, \ldots) \) is a sequence over \( \Omega \), \( i = 0, 1, \ldots, e-1 \). The sequence \( \varrho_i \) is called \( i \)th level component of \( \varrho \) and \( \varrho_{e-1} \) the highest level component of \( \varrho \).

Now we set \( p = 2 \) and let \( f(x) \) be a monic polynomial over \( \text{GR}(2^e, r) \). If \( f(0) \neq 0 \mod 2 \), then there exists a positive integer \( P \) such that \( f(x) \) divides \( x^P - 1 \) and the least such \( P \) is called the period of \( f(x) \) over \( \text{GR}(2^e, r) \), denoted by \( \text{per}(f(x)) \). For a monic polynomial \( f(x) \) over \( \text{GR}(2^e, r) \) with degree \( n \), the period of \( f(x) \) is upper bounded by \( 2^{e-1}(2^m - 1) \) and \( f(x) \) is called a primitive polynomial if \( \text{per}(f(x)) = 2^{e-1}(2^m - 1) \). Let \( f(x) \) be a primitive polynomial of degree \( n \) over \( \text{GR}(2^e, r) \), then \( f(x) \mod 2 \) is a primitive polynomial over \( F_2 \). Let \( \varrho \) be a sequence over \( \text{GR}(2^e, r) \), generated by a primitive polynomial \( f(x) \) of degree \( n \) with \( \varrho \neq 0 \mod 2 \), then \( \text{per}(\varrho) = \text{per}(f(x)) = 2^{e-1}T \) and \( \text{per}(\varrho_i) = 2^i T \) where \( T = 2^m - 1, \ i = 0, 1, \ldots, e-1 \). Especially \( \text{per}(\varrho_{e-1}) = \text{per}(\varrho) = 2^{e-1}T \).

**Lemma 6.** Let \( f(x) \) be a primitive polynomial of degree \( n \) over \( \text{GR}(2^e, r) \), \( T = 2^m - 1 \), then there exists \( h_i(x) \) over \( \text{GR}(2^e, r) \) of degree less than \( n \), \( i = 1, 2, \ldots, e-1 \), such that

\[
x^{2^{i-1}T} - 1 \equiv 2^i h_i(x) \mod f(x).
\]

Furthermore, all \( h_i(x) \neq 0 \mod 2 \), \( h_2(x) \equiv \cdots \equiv h_{e-1}(x) \mod 2 \) and \( h_2(x) \equiv h_1(x) + h_1(x)^2 \mod(2, f(x)) \).
Definition 1. Let \( f(x) \) be a primitive polynomial over \( GR(2^e, r) \). If \( e \geq 3 \) and \( \deg(h_2(x) \mod 2) \geq 1 \) or \( e = 2 \) and \( \deg(h_1(x) \mod 2) \geq 1 \), then \( f(x) \) is called a strongly primitive polynomial over \( GR(2^e, r) \).

Lemma 7. Let \( f(x) \) be a primitive polynomial over \( GR(2^e, r) \), \( \eta(x_0, x_1, \ldots, x_{e-2}) \) a function of \( e - 1 \) variables over \( F_{2^e} \) and

\[
\varphi(x_0, x_1, \ldots, x_{e-1}) = x_{e-1} + \eta(x_0, x_1, \ldots, x_{e-2}).
\]

For \( a, b \in G(f(x), GR(2^e, r)) \), if \( \varphi(a_0, \ldots, a_{e-1}) \equiv \varphi(b_0, \ldots, b_{e-1}) \mod 2 \), then \( a_0 = b_0 \).

The proof is similar to the one of Lemma 5.

Lemma 8. Let \( \Omega \) be the \( p \)-adic coordinate set of \( GR(2^e, r) \), \( \delta \in GR(2^e, r) \), \( \alpha, \beta \in \Omega \), then

1. \( \delta^{2s} \equiv \delta \mod 2 \).
2. For \( s \geq e - 1 \), \( \delta^{2s} \in \Omega \).
3. \( \alpha \beta \in \Omega \).
4. Let \( s \) be a positive integer such that \( rs \geq e - 1 \), then \( (\alpha + \beta)^{2^r} \in \Omega \), \( (\alpha \beta)^{2^{r-1}} \in \Omega \) and

\[
\alpha + \beta \equiv (\alpha + \beta)^{2^s} + 2(\alpha \beta)^{2^{r-1}} \mod 2^2.
\]

Proof. (1) Let \( \delta = \lambda + 2\xi \), where \( \lambda \in \Omega \), \( \xi \in GR(2^e, r) \). Since \( \lambda^{2^s} = \lambda \), \( \delta^{2^s} \equiv \delta \mod 2 \).

(2) If \( \delta \equiv 0 \mod 2 \), then \( \delta = 2\xi \), where \( \xi \in GR(2^e, r) \). Since \( 2^s \geq 2^{e-1} \geq e \), we have \( \delta^{2^s} = 0 \in \Omega \). If \( \delta \not\equiv 0 \mod 2 \), then \( \delta = \lambda + 2\xi \), where \( \lambda \in \Omega \), \( \xi \in GR(2^e, r) \). So \( \delta^{2^s} = (\lambda + 2\xi)^{2^s} = \lambda^{2^s} + 2^{1+s} \lambda^{2^{s-1}} \xi + \cdots = \lambda^{2^s} \in \Omega \).

(3) \( (\alpha \beta)^{2^s} = \alpha^{2^s} \beta^{2^s} = \alpha \beta \), so \( \alpha \beta \in \Omega \).

(4) By (2) and (3), \( (\alpha + \beta)^{2^s} \in \Omega \), \( (\alpha \beta)^{2^{s-1}} \in \Omega \). Since

\[
(\alpha + \beta)^{2^s} \equiv \alpha^{2^s} + \beta^{2^s} + 2\alpha^{2^{s-1}} \beta^{2^{s-1}} \mod 2^2,
\]

we have

\[
(\alpha + \beta)^{2^s} \equiv \alpha^{2^s} + \beta^{2^s} + 2\alpha^{2^{s-1}} \beta^{2^{s-1}} \\
\equiv \alpha + \beta + 2(\alpha^{2^{s-1}})^{2^s-1}(\beta^{2^{s-1}})^{2^s-1} \\
\equiv \alpha + \beta + 2(\alpha \beta)^{2^{s-1}} \mod 2^2.
\]

So \( \alpha + \beta \equiv (\alpha + \beta)^{2^s} + 2(\alpha \beta)^{2^{s-1}} \mod 2^2 \).
Lemma 9. Let \( f(x) \) be a primitive polynomial of degree \( n \) over the finite field \( F_{2^n} \), \( \psi = (u_0, u_1, \ldots, u_t) \in G(f(x), F_{2^n}) \) and \( \psi \neq 0 \). If \( v_i = 0 \) implies \( u_i = 0 \), then there exists \( c \in F_{2^n} \) such that \( u = c \psi \).

Proof. If \( u = 0 \), then we set \( c = 0 \) and get \( u = c \psi \). Now assume \( u \neq 0 \), then \( \psi \neq 0 \) by the condition. Since \( f(x) \) is a primitive polynomial of degree \( n \) and \( u \) and \( \psi \) are generated by \( f(x) \), there exists a nonnegative integer \( k \) such that \( (u_k, u_{k+1}, \ldots, u_{k+n-1}) = (0, 0, \ldots, 0, a) \) and \( (v_k, v_{k+1}, \ldots, v_{k+n-1}) = (0, 0, \ldots, 0, b) \), where \( a \neq 0 \) and \( b \neq 0 \). Then it is clear that \( u = c \psi \), where \( c = ab^{-1} \).

Lemma 10. Let \( f(x) \) be a primitive polynomial of degree \( n \) over \( GR(2^e, r) \), \( T = 2^m - 1 \), \( a = a_0 + a_1 \cdot 2 + \cdots + a_{e-1} \cdot 2^{e-1} \in G(f(x), GR(2^e, r)) \) and \( a_0 \neq 0 \), then \( \text{per}(a_j) = 2^i T \), especially \( \text{per}(a_{e-1}) = 2^{e-1} T = \text{per}(a) = \text{per}(f(x)) \).

The proof is similar to one of Lemma 1 cited from [1].

Lemma 11. Let \( f(x) \) be a strongly primitive polynomial over \( GR(2^e, r) \), \( e \geq 3 \), \( a, b \in G(f(x), GR(2^e, r)) \) and \( a_0 = b_0 \neq 0 \). If there exists \( c \in F_{2^n} \) such that \( a_1 + b_1 = c a_0 \mod 2 \) and

\[
\frac{a_0 h_1(x) g_0(h_2(x) g_0)^2}{c(h_1(x) g_0)^2} (h_2(x) g_0)^2 \equiv 0 \mod 2,
\]

(23)

where \( h_1(x) \) and \( h_2(x) \) is defined by (22), then \( a_1 = b_1 \), i.e. \( c = 0 \).

Proof. Assume \( a_1 \neq b_1 \), that is, \( c \neq 0 \).

If \( a_0, h_1(x) g_0 \) and \( h_2(x) g_0 \) are linear independent over \( F_{2^n} \), then, by Lemma 4,

\[
\frac{a_0 h_1(x) g_0(h_2(x) g_0)^2}{c(h_1(x) g_0)^2} (h_2(x) g_0)^2 \equiv 0 \mod 2,
\]

that is a contradiction. Now suppose that \( a_0, h_1(x) g_0 \) and \( h_2(x) g_0 \) are linear dependent over \( F_{2^n} \). Since \( g_0 \) is an m-sequence generated by \( f(x) \) over \( F_{2^n} \), \( \deg(h_1(x) \mod 2) \geq 1 \), \( \deg(h_2(x) \mod 2) \geq 1 \) and \( h_1(x) \neq h_2(x) \mod 2 \), we conclude that any two of \( g_0, h_1(x) g_0 \) and \( h_2(x) g_0 \) are linear independent over \( F_{2^n} \). Thus, we can assume \( a_0 = c_1 h_1(x) g_0 + c_2 h_2(x) g_0 \) over \( F_{2^n} \), where \( c_1 \) and \( c_2 \) are nonzero elements in \( F_{2^n} \). We write \( g_0 = (a_0, a_1, a_2, \ldots) \), \( c_1 h_1(x) g_0 = (\gamma_0, \gamma_1, \gamma_2, \ldots) \), \( c_2 h_2(x) g_0 = (\gamma_0, \gamma_1, \gamma_2, \ldots) \) over \( F_{2^n} \). Since \( c_1 h_1(x) g_0 \) and \( c_2 h_2(x) g_0 \) are linear independent over \( F_{2^n} \), there exists nonnegative integer \( t \) such that \( \beta_t = \gamma_t \neq 0 \). Then \( \theta_t \neq 0 \) in \( c(h_1(x) g_0)^2 (h_2(x) g_0)^2 = (\theta_0, \theta_1, \theta_2, \ldots) \) such that \( \theta_t = \beta_t + \gamma_t = 2 \beta_t = 0 \), by (23), we get a contradiction.

Lemma 12. Let \( g(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0 \in F_2[x] \), \( f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0 \) and \( u \) a sequence over \( F_{2^n} \). Then \( (g(x) u)^2 = f(x) u^2 \).

Especially, \( ((x^k - 1) u)^2 = (x^k - 1)(u^2) \) for any positive integer \( k \).

The proof is easy.
THEOREM 3. Let \( f(x) \) be a strongly primitive polynomial of degree \( n \) over \( \text{GR}(2^e, r) \), \( \varphi(x_0, x_1, \ldots, x_{e-1}) = x_{e-1} + \eta(x_0, x_1, \ldots, x_{e-2}) \), where \( \eta(x_0, x_1, \ldots, x_{e-2}) \) is a function of \( e - 1 \) variables over \( F_{2^e} \). Set \( \eta_{e-2}(x_0, x_1, \ldots, x_{e-2}) = \eta(x_0, x_1, \ldots, x_{e-2}) \). If \( \eta_{e-2}(x_0, x_1, \ldots, x_{e-2}) \) satisfies

\[
\begin{align*}
\eta_{e-2}(x_0, x_1, \ldots, x_{e-2}) &= x_{e-2}\eta_{e-3}(x_0, x_1, \ldots, x_{e-3}) + \psi_{e-3}(x_0, x_1, x_{e-3}) \\
\end{align*}
\]

and

\[
\eta_i(x_0, x_1, \ldots, x_i) = x_i\eta_{i-1}(x_0, x_1, \ldots, x_{i-1}) + \psi_{i-1}(x_0, x_1, \ldots, x_{i-1}),
\]

where \( i = 1, 2, \ldots, e - 2 \), \( \eta_{i-1}(x_0, x_1, \ldots, x_{i-1}) \) and \( \psi_{i-1}(x_0, x_1, \ldots, x_{i-1}) \) are functions of \( i \) variables over \( F_{2^e} \), then the compression mapping

\[
\Phi : \left\{ \begin{array}{l}
G(f(x), \text{GR}(2^e, r)) \rightarrow F_{2^e}^\infty, \\
\quad a = a_0 + a_1 2 + \cdots + a_{e-1} 2^{e-1} \mapsto \varphi(a_0, a_1, \ldots, a_{e-1}) \mod 2
\end{array} \right.
\]

is injective, that is, for \( a, b \in G(f(x), \text{GR}(2^e, r)) \), \( a = b \) if and only if \( \varphi(a_0, \ldots, a_{e-1}) \equiv \varphi(b_0, \ldots, b_{e-1}) \mod 2 \).

Proof. Let \( a, b \in G(f(x), \text{GR}(2^e, r)) \) satisfying

\[
\varphi(a_0, \ldots, a_{e-1}) \equiv \varphi(b_0, \ldots, b_{e-1}) \mod 2.
\]

By Lemma 7, \( a_0 = b_0 \). It is not harmful to assume \( a_0 \neq 0 \).

(1) Assume \( e \geq 4 \). Since \( h_2(x) \equiv \cdots \equiv h_{e-1}(x) \mod 2 \), we set \( h(x) = h_i(x) \mod 2 \) over \( F_{2^e} \), \( 2 \leq i \leq e - 1 \).

Since

\[
\begin{align*}
a_{e-1} + a_{e-2}\eta_{e-3}(a_0, \ldots, a_{e-3}) + \psi_{e-3}(a_0, \ldots, a_{e-3}) \\
\equiv b_{e-1} + b_{e-2}\eta_{e-3}(b_0, \ldots, b_{e-3}) + \psi_{e-3}(b_0, \ldots, b_{e-3}) \mod 2
\end{align*}
\]

and by Lemma 10 the periods of \( \psi_{e-3}(a_0, \ldots, a_{e-3}) \) and \( \psi_{e-3}(b_0, \ldots, b_{e-3}) \) divide \( 2^{e-3}T \), where \( T = 2^n - 1 \), by \( x^{2^{e-3}T} - 1 \) acting on (24), we can get

\[
\begin{align*}
(x^{2^{e-3}T} - 1)(a_{e-1} + a_{e-2}\eta_{e-3}(a_0, \ldots, a_{e-3})) \\
\equiv (x^{2^{e-3}T} - 1)(b_{e-1} + b_{e-2}\eta_{e-3}(b_0, \ldots, b_{e-3})) \mod 2.
\end{align*}
\]

Furthermore, by Lemma 3, we have

\[
\begin{align*}
(x^{2^{e-3}T} - 1)a_{e-1} + \eta_{e-3}(a_0, \ldots, a_{e-3})(x^{2^{e-3}T} - 1)a_{e-2} \\
\equiv (x^{2^{e-3}T} - 1)b_{e-1} + \eta_{e-3}(b_0, \ldots, b_{e-3})(x^{2^{e-3}T} - 1)b_{e-2} \mod 2.
\end{align*}
\]
Since \( g_0 = b_0 \) and by Lemma 6 \( x^{2^{e-3}r} - 1 \equiv 2^{e-2}h_{e-2}(x) \mod f(x) \), it follows that

\[
(x^{2^{e-3}r} - 1)g_{e-2} \equiv h(x)g_0 \equiv h(x)b_0 \equiv (x^{2^{e-3}r} - 1)b_{e-2} \mod 2.
\]

So (26) implies that

\[
(x^{2^{e-3}r} - 1)(a_{e-1} + b_{e-1}) \equiv \eta_{e-3}(a_0, \ldots, a_{e-3}) + \eta_{e-3}(b_0, \ldots, b_{e-3})h(x)g_0 \mod 2. \tag{27}
\]

By \( x^{2^{e-3}r} - 1 \equiv 2^{e-2}h_{e-2}(x) \mod f(x) \) acting on \( a = a_0 + a_12 + \cdots + a_{e-1}2^{e-1}, \)

\[
(x^{2^{e-3}r} - 1)(a_{e-2} + a_{e-1}2) \equiv h_{e-2}(x)(a_0 + a_12) \mod 2^2. \tag{28}
\]

Let

\[
h_{e-2}(x)(a_0 + a_12) \equiv u + v2 \mod 2^2 , \tag{29}
\]

where \( u \) and \( v \) are 0th and 1th level components of \( h_{e-2}(x)(a_0 + a_12) \), respectively. It is clear that \( u \equiv h_{e-2}(x)g_0 \mod 2 \). So, by (28)

\[
x^{2^{e-3}r}a_{e-2} + (x^{2^{e-3}r} - 1)a_{e-1}2 \equiv a_{e-2} + u + v2 \mod 2^2. \tag{30}
\]

By Lemma 8, \( a_{e-2} + u \equiv (a_{e-2} + u)^{2^s} + 2(a_{e-2}u)^{2^s-1} \mod 2^2 \), where \( s \) is a positive integer such that \( rs \geq e - 1 \). Since \( (a_{e-2} + u)^{2^s} \) is a sequence over \( \Omega \), by (30), it follows that

\[
(x^{2^{e-3}r} - 1)a_{e-1} \equiv v + (ua_{e-2})^{2^s-1} \mod 2. \tag{31}
\]

Similarly, we have

\[
(x^{2^{e-3}r} - 1)b_{e-1} \equiv w + (ub_{e-2})^{2^s-1} \mod 2, \tag{32}
\]

where \( w \) is determined by

\[
h_{e-2}(x)(b_0 + b_12) \equiv u + v2 \mod 2^2. \tag{33}
\]

Since \( g_0 = b_0 \), by (29) and (33), it follows that \( v + w = h(x)(a_1 + b_1) \mod 2 \), and by (31) and (32), we have

\[
(x^{2^{e-3}r} - 1)(a_{e-1} + b_{e-1}) \equiv y^{2^s-1} (a_{e-2} + b_{e-2})^{2^s-1} + h(x)(a_1 + b_1) \mod 2. \tag{34}
\]
By (27) and $u \equiv h(x)g_0 \mod 2$,

$$u^{2^{r-1}}(a_{e-2} + b_{e-2})^{2^{r-1}} \equiv \left[ \eta_{e-3}(a_0, \ldots, a_{e-3}) + \eta_{e-3}(b_0, \ldots, b_{e-3}) \right] u + h(x)(a_1 + b_1) \mod 2. \quad (35)$$

Then

$$u(a_{e-2} + b_{e-2}) \equiv \left[ u^{2^{r-1}}(a_{e-2} + b_{e-2})^{2^{r-1}} \right]^2 \equiv \left[ \eta_{e-3}(a_0, \ldots, a_{e-3}) + \eta_{e-3}(b_0, \ldots, b_{e-3}) \right]^2 u^2$$

$$+ [h(x)(a_1 + b_1)]^2 \mod 2. \quad (36)$$

If $e \geq 5$, $x^{2^{e-4}r} - 1 \equiv 2^{e-3}h_{e-3}(x) \mod f(x)$ acts on $a$ and $b$ continuously. Then

$$(x^{2^{e-4}r} - 1)(a_{e-3} + a_{e-2}2) \equiv h_{e-3}(x)(a_0 + a_12) \mod 2^2,$$

$$(x^{2^{e-4}r} - 1)(b_{e-3} + b_{e-2}2) \equiv h_{e-3}(x)(b_0 + b_12) \mod 2^2.$$

Similar to (34), we have

$$(x^{2^{e-4}r} - 1)(a_{e-2} + b_{e-2}) \equiv u^{2^{r-1}}(a_{e-3} + b_{e-3})^{2^{r-1}} + h(x)(a_1 + b_1) \mod 2 \quad (37)$$

and so

$$[ (x^{2^{e-4}r} - 1)(a_{e-2} + b_{e-2})] u \equiv u^{2^{r-1}}(a_{e-3} + b_{e-3})^{2^{r-1}} + uh(x)(a_1 + b_1) \mod 2.$$

Since $\text{per}(u) = T$, we have

$$(x^{2^{e-4}r} - 1)[(a_{e-2} + b_{e-2})u]$$

$$\equiv uu^{2^{r-1}}(a_{e-3} + b_{e-3})^{2^{r-1}} + uh(x)(a_1 + b_1) \mod 2. \quad (38)$$
And by (36), it follows that
\[(a_{e-2} + b_{e-2})u\]
\[\equiv u^2[a_{e-3} \eta_{e-4}(a_0, \ldots, a_{e-4}) + b_{e-3} \eta_{e-4}(b_0, \ldots, b_{e-4}) + \psi_{e-4}(a_0, \ldots, a_{e-4}) + \psi_{e-4}(b_0, \ldots, b_{e-4})]^2 + [h(x)(a_1 + b_1)]^2 \mod 2.\]

The periods of \((\psi_{e-4}(a_0, \ldots, a_{e-4}) + \psi_{e-4}(b_0, \ldots, b_{e-4}))^2 u^2\) and \((h(x)(a_1 + b_1))^2\) divide \(2^{e-4}T\), so it follows that
\[(x^{2^{e-4}T} - 1)(a_{e-2} + b_{e-2})u\]
\[\equiv (x^{2^{e-4}T} - 1)[a_{e-3} \cdot \eta_{e-4}(a_0, \ldots, a_{e-4}) + b_{e-3} \cdot \eta_{e-4}(b_0, \ldots, b_{e-4})]^2 u^2 \mod 2.\]

Comparing with (38) and by Lemma 12 we get
\[\eta_{e-4}(a_0, \ldots, a_{e-4})(x^{2^{e-4}T} - 1)a_{e-3} + \eta_{e-4}(b_0, \ldots, b_{e-4})(x^{2^{e-4}T} - 1)b_{e-3}]^2 u^2\]
\[\equiv u \cdot u^{2^{e-1}}(a_{e-3} + b_{e-3})^{2^{e-1}} + u \cdot h(x)(a_1 + b_1) \mod 2.\]

Since \((x^{2^{e-4}T} - 1)a_{e-3} \equiv h_{e-3}(x)g_0 \equiv u \mod 2\), then
\[\eta_{e-4}(a_0, \ldots, a_{e-4}) + \eta_{e-4}(b_0, \ldots, b_{e-4})]^{4} u^8\]
\[\equiv u \cdot u^{2^{e-1}}(a_{e-3} + b_{e-3})^{2^{e-1}} + u \cdot h(x)(a_1 + b_1) \mod 2.\]

So
\[\eta_{e-4}(a_0, \ldots, a_{e-4}) + \eta_{e-4}(b_0, \ldots, b_{e-4})]^{4} u^8\]
\[\equiv [u \cdot u^{2^{e-1}}(a_{e-3} + b_{e-3})^{2^{e-1}} + u \cdot h(x)(a_1 + b_1)]^2\]
\[\equiv u^2 \cdot u(a_{e-3} + b_{e-3}) + u^2[h(x)(a_1 + b_1)]^2 \mod 2,\]
that is,
\[u(a_{e-3} + b_{e-3})u^2 \equiv [\eta_{e-4}(a_0, \ldots, a_{e-4}) + \eta_{e-4}(b_0, \ldots, b_{e-4})]^{4} u^8\]
\[+ u^2[h(x)(a_1 + b_1)]^2 \mod 2.\] \hspace{1cm} (39)

Let \(u \equiv (u_0, u_1, \ldots) \mod 2\), \(h(x)(a_1 + b_1) = (w_0, w_1, \ldots) \mod 2\), by (36), it follows that if \(u_i = 0\), then \(w_i \equiv 0\). So by Lemma 9, \(h(x)(a_1 + b_1) \equiv c u \mod 2\)
for some $c \in \mathbb{F}_{2^r}$, and (39) implies

$$u(a_{e-3} + b_{e-3}) \equiv u^6[\eta_{e-4}(a_0, \ldots, a_{e-4}) + \eta_{e-4}(b_0, \ldots, b_{e-4})]^4$$

$$+ [h(x)(a_1 + b_1)]^2 \mod 2.$$ 

From the above discussion, we deduce the following formula:

$$u(a_{e-i} + b_{e-i}) \equiv u^k(\eta_{e-i-1}(a_0, \ldots, a_{e-i-1}) + \eta_{e-i-1}(b_0, \ldots, b_{e-i-1}))^{2^{i-1}}$$

$$+ [h(x)(a_1 + b_1)]^2 \mod 2,$$  \hspace{1cm} (40)

where $k_i$ is a positive integer, $i = 2, 3, \ldots, e - 2$. Take $i = e - 2$, then

$$u(a_2 + b_2) \equiv u^{2^{e-2}}[\eta_1(a_0, a_1) + \eta_1(b_0, b_1)]^{2^{e-3}} + [h(x)(a_1 + b_1)]^2 \mod 2. \hspace{1cm} (41)$$

Finally, $x^T - 1 \equiv 2h_1(x) \mod f(x)$ acts on $a$ and $b$. Similar to (34), we have

$$(x^T - 1)(a_2 + b_2) \equiv (h_1(x)a_0)^{2^{e-1}}(a_1 + b_1)^{2^{e-1}} + h_1(x)(a_1 + b_1) \mod 2,$$ \hspace{1cm} (42)

which deduces

$$(x^T - 1)(a_2 + b_2)u \equiv (h_1(x)a_0)^{2^{e-1}}(a_1 + b_1)^{2^{e-1}}u + h_1(x)(a_1 + b_1)u \mod 2. \hspace{1cm} (43)$$

Since $\eta_1(x_0, x_1) = x_1\eta_0(x_0) + \psi_0(x_0)$ and $h(x)(a_1 + b_1) \equiv cu \mod 2$, (41) implies

$$(x^T - 1)(a_1 \cdot \eta_0(a_0) + b_1 \cdot \eta_0(b_0))^{2^{e-3}}u^{k_e-2}$$

$$\equiv (h_1(x)a_0)^{2^{e-1}}(a_1 + b_1)^{2^{e-1}}u + h_1(x)(a_1 + b_1)u \mod 2. \hspace{1cm} (44)$$

Since $(x^T - 1)a_1 \equiv (x^T - 1)b_1 \equiv h_1(x)a_0 \mod 2$ and $\eta_0(a_0) \equiv \eta_0(b_0) \mod 2$, we have

$$(x^T - 1)(a_1 \cdot \eta_0(a_0) + b_1 \cdot \eta_0(b_0))^{2^{e-3}}u^{k_e-2}$$

$$\equiv [(x^T - 1)a_1 \cdot \eta_0(a_0) + (x^T - 1)b_1 \cdot \eta_0(b_0)]^{2^{e-3}}u^{k_e-2} \equiv 0 \mod 2.$$
So (44) implies
\[(h_1(x)g_0)^{2^{r-1}}(a_1 + b_1)^{2^{r-1}}u + h_1(x)(a_1 + b_1)u \equiv 0 \text{ mod } 2\]
and then
\[(h_1(x)(a_1 + b_1))^2u^2 \equiv [(h_1(x)g_0)^{2^{r-1}}(a_1 + b_1)^{2^{r-1}}u]^2 \equiv h_1(x)g_0(a_1 + b_1)u^2 \text{ mod } 2. \tag{45}\]

Because \(h(x)(a_1 + b_1) \equiv cu \text{ mod } 2\) and \(h_2(x)g_0 \equiv u \text{ mod } 2\), \(h(x)(a_1 + b_1) \equiv ch(x)g_0 \equiv h(x)(cg_0)\), which implies \(a_1 + b_1 \equiv cg_0 \text{ mod } 2\). And (45) implies that
\[a_0 \cdot h_1(x)g_0(h_2(x)g_0)^2 \equiv c(h_1(x)(g_0))^2(h_2(x)g_0)^2 \text{ mod } 2.\]

By Lemma 11, we get \(a_1 = b_1\). Thus \(u(a_2 + b_2) \equiv 0 \text{ mod } 2\) by (41). Since \(a_0 = b_0\), \(a_1 = b_1\), it follows that \(a_2 + b_2\) is a primitive sequence over \(F_{2^r}\) or zero sequence. And since \(u\) is a primitive sequence over \(F_2\), we get \(a_2 + b_2 \equiv 0 \text{ mod } 2\), that is, \(a_2 = b_2\). So by (40), it follows that \(a_j = b_j, j = 3, \ldots, e - 2\). Finally, by the condition \(\varphi(g_0, \ldots, g_{e-1}) \equiv \varphi(b_0, \ldots, b_{e-1}) \text{ mod } 2\), we have \(a_{e-1} = b_{e-1}\), and then \(a = b\).

(2) Assume \(e = 3\), then \(\varphi(x_0, x_1, x_2) = x_2 + \eta(x_0, x_1)\) and \(\eta(x_0, x_1) = x_1\eta_0(x_0) + \psi_0(x_0)\). Since \(\varphi(g_0, a_1, g_2) \equiv \varphi(b_0, b_1, b_2)\) and \(a_0 = b_0\), it follows that
\[a_2 + b_2 \equiv (a_1 + b_1)\eta_0(g_0) \text{ mod } 2. \tag{46}\]

By Lemmas 3 and 6,
\[(x^T - 1)(a_2 + b_2) \equiv (x^T - 1)((a_1 + b_1)\eta_0(g_0)) \equiv \eta_0(a_0)(x^T - 1)(a_1 + b_1) \equiv \eta_0(a_0)(h_1(x)g_0 + h_1(x)b_0) \equiv 0 \text{ mod } 2.\]

By (42), we have \(h_1(x)(a_1 + b_1) \equiv (a_1 + b_1)^{2^{r-1}}h_1(x)(a_0)^{2^{r-1}} \text{ mod } 2\), and so
\[(h_1(x)(a_1 + b_1))^2 \equiv [(a_1 + b_1)^{2^{r-1}}(h_1(x)g_0)^{2^{r-1}}]^2 \equiv (a_1 + b_1)h_1(x)g_0 \text{ mod } 2.\]

If \(a_1 + b_1 \not\equiv 0 \text{ mod } 2\), that is, \(a_1 + b_1 \text{ mod } 2\) and \(h_1(x)(a_1 + b_1)\) are primitive sequences over \(F_{2^r}\). Since \(\deg(h_1(x) \text{ mod } 2) \geq 1\), it
follows that and $a_1 + b_1 \equiv 0 \mod 2$; Furthermore, by (46), $a_2 = b_2$ and $a = b$.

(3) Assume $e = 2$, then $\varphi(x_0, x_1) = x_1 + \eta(x_0)$. So $\varphi(a_0, a_1) \equiv \varphi(b_0, b_1) \mod 2$ and $a_0 = b_0$ imply $a_1 = b_1$. Hence $a = b$. ■.

Remark 3. Theorems 2 and 3 show that the binary sequence $\varphi(a_0, \ldots, a_{e-1})$ contains all information of the original sequence $a$. We guess that for any $\eta$, Theorem 3 is also correct.

REFERENCES