On the Cycle Structure of Certain Classes of Nonlinear Shift Registers

UNJENG CHENG

Axiomatix, 9841 Airport Blvd. #912, Los Angeles, California 90045

Communicated by the Managing Editors

Received June 17, 1982

When \( m = q^t \) and \( g(x_1, x_2, \ldots, x_m) \) is a linear combination of only odd (or only even) elementary symmetric functions, then every cycle of the nonlinear shift register with feedback function \( f(x_1, x_2, \ldots, x_m) = x_1 + g(x_2, x_3, x_m) \), has a minimal period dividing \( m(q + 1) \). It is also shown that when \( g \) is derived from a cyclic code with minimum distance \( 3 \), every cycle of this shift register has a minimal period dividing \( m(q + 1) \).

1. INTRODUCTION

A general \( m \)-stage nonlinear shift register is shown in Fig. 1. If the content of this shift register at a certain time instant is \( (x_1, x_2, \ldots, x_m) \), then its successive content will be

\[
(x_2, x_3, \ldots, x_{m-1}, f(x_1, x_2, \ldots, x_m)).
\]

\((x_1, x_2, \ldots, x_m)\) is designated the state of this register. It is obvious that any state has a unique successive state. However, some states may have more than one preceding states. It was proved in [1] that all states will have a unique preceding state if and only if

\[
f(x_1, x_2, \ldots, x_m) = x_1 + g(x_2, x_3, \ldots, x_m).
\]

![Fig. 1. The general block diagram of a nonlinear shift register.](image-url)
Hence when (2) is true, any state will have a unique successive state and a unique preceding state. And this shift register will decompose all m-tuples into disjoint cycles. A major problem concerning shift registers is their cycle structure. The question to ask is that, given a shift register, what lengths its cycles should have. Very little is known about the cycle structure of nonlinear shift registers. Kjeldsen's paper [2] considers the case where $g$ is a linear combination of odd (or even) elementary symmetric functions. The general case where $g$ is an arbitrary symmetric function is considered in [5]. In this paper, we will generalize Kjeldsen's idea.

Let $\Gamma = GF(2)[x_1, x_2, \ldots, x_m]/(\sum_{i=1}^{m} (x_i + x_i^2))$ be the polynomial ring in $m$ variables over $GF(2)$. To the shift register with feedback function $f$, we associate an algebrahomomorphism $\delta_f : \Gamma \rightarrow \Gamma$ defined by

$$
\delta_f(x_i) = x_{i+1} \quad \text{if} \quad i < m,
$$

$$
\delta_f(x_m) = f(x_1, x_2, \ldots, x_m).
$$

By repeatedly applying $\delta_f$, one can generate a $\delta_f$-function sequence

$$
x_1, \delta_f(x_1), \delta_f^2(x_1), \delta_f^3(x_1), \ldots, \delta_f^k(x_1), \ldots.
$$

The key idea, introduced in [2], in the following derivation is that, for some feedback function $f(x_1, x_2, \ldots, x_m)$, $\delta_f$-function sequence can be modeled by a linear shift register. Hence this shift register will have a cycle structure similar to that of the linear shift register. The basic technique is to choose a proper $g(x_2, x_3, \ldots, x_m)$ and a proper subspace $A$ in $\Gamma$ such that

$$
g(x_2, x_3, \ldots, x_m) \in A
$$

and

$$
\delta_f : A \rightarrow A.
$$

When this is true, it is evident that any term in the $\delta_f$-function sequence will be a linear combination of $x_1, x_2, \ldots, x_m$ and functions in $A$.

The period of $\delta_f$ is defined to be the least integer $t$ such that $\delta_f^t(x_1) = x_1$. And it is denoted by $p(\delta_f)$. The following results are important. They were proved in [2].

**Lemma 1.** Let $g, h \in \Gamma$. Then $h$ is a divisor of $g$ if and only if $hg = g$.

**Theorem 2.** The $\delta_f$ is an isomorphism if and only if (2) is true.

From now on, we will always assume that (2) is true.

**Theorem 3.** The $p(\delta_f)$, is equal to the least common multiple of all cycle lengths of this shift register.
For any \( h(x_1, x_2, \ldots, x_m) \in \mathcal{F} \), we can write

\[
h(x_1, x_2, \ldots, x_m) = h_1(x_1, x_2, \ldots, x_{m-1}) + x_m h_2(x_1, x_2, \ldots, x_{m-1}).
\]  

(6)

Then

\[
\delta_f(h(x_1, x_2, \ldots, x_m)) = h_1(x_2, x_3, \ldots, x_m) + x_1 h_2(x_2, x_3, \ldots, x_m)
\]
\[
+ g(x_2, x_3, \ldots, x_m) h_2(x_2, x_3, \ldots, x_m).
\]  

(7)

Define an algebra homomorphism \( \hat{S} \) by

\[
\hat{S}(x_i) = x_{(i) modm + 1}, \quad 1 \leq i \leq m,
\]  

(8)

i.e., \( \hat{S} \) is the cyclic shift operator of the variables \( x_1, x_2, \ldots, x_m \). Further, define an operator \( \hat{D} \) by

\[
\hat{D}(h(x_1, x_2, \ldots, x_m)) = \hat{S}(h_2(x_1, x_2, \ldots, x_{m-1})).
\]  

(9)

Then (7) can be written as

\[
\delta_f(h(x_1, x_2, \ldots, x_m)) = \hat{S}(h(x_1, x_2, \ldots, x_m))
\]
\[
+ g(x_2, x_3, \ldots, x_m) \hat{D}(h(x_1, x_2, \ldots, x_m)).
\]  

(10)

Equation (10) will be frequently used in our subsequent derivation.

2. The Case Where \( g(x_2, x_3, \ldots, x_{q+1}) \) Is A Symmetric Function in \( x_1, x_2, \ldots, x_{q+1} \)

Let the elementary symmetric functions be

\[
S_j(x_2, x_3, \ldots, x_m) = \sum_{2 \leq i_1 < i_2 < \cdots < i_j \leq m} x_{i_1} x_{i_2} \cdots x_{i_j} \quad \text{for } 0 \leq j \leq m - 1.
\]  

(11)

The following lemma was proved in [2].

**Lemma 4.** For any odd integer \( j, 0 \leq j \leq m - 1 \), one has

\[
S_j(x_2, x_3, \ldots, x_m) = S_1(x_2, x_3, \ldots, x_m) S_{j-1}(x_3, x_4, \ldots, x_m).
\]  

(12)

Lemma 4 can be rewritten into a more general form. We state it as a corollary.

**Corollary.** Given any odd integer \( j \), let \( k \geq j \) and \( i_1 < i_2 < \cdots < i_k \). One has

\[
S_j(x_{i_1}, x_{i_2}, \ldots, x_{i_k}) = S_1(x_{i_1}, x_{i_2}, \ldots, x_{i_k}) S_{j-1}(x_{i_1}, x_{i_2}, x_{i_{r+1}}, \ldots, x_{i_k}).
\]  

(13)
Let us consider the case with
\[ m = qt, \quad \text{where} \quad q \geq 3 \quad \text{and} \quad t \geq 1, \quad \text{and} \quad g(x_2, x_3, \ldots, x_m) = \sum_{k=0}^{(q-2)/2} d_k S_{2k+1}(x_{t+1}, x_{2t+1}, \ldots, x_{(q-1)t+1}), \]
where \( d_k \in GF(2) \) and \( d_k, k \geq 1, \) are not all zero. (14)

In this case, the basis of \( A \) (cf. (4), (5)) is
\[ g, \hat{S}g, \hat{S}^2g, \ldots, \hat{S}^{m-1}g. \] (15)

The key step is to prove that
\[ \delta_j(\hat{S}^jg) \in A \quad \text{for all} \quad j, \quad 0 \leq j \leq m - 1. \] (16)

The first term on the right-hand side of (10) gives
\[ \hat{S}(\hat{S}^jg) = \hat{S}^{j+1}g \in A \quad \text{for all} \quad j, \quad 0 \leq j \leq m - 1. \] (17)

Hence the only problem left is to prove that the second term on the right-hand side of (10) belongs to \( A. \) By (8)
\[ \hat{S}^j S_{2k+1}(x_{t+1}, x_{2t+1}, \ldots, x_{(q-1)t+1}) = S_{2k+1}(x_{(t+j) \mod m+1}, x_{((q-1)t+j) \mod m+1}). \] (18)

**Lemma 5.** Let \( g \) be defined as in (14). Then, for \( 0 \leq j \leq m - 1, \)
\[ \delta_j(\hat{S}^j(g)) = \hat{S}^{j+1}(g) + g \quad \text{if} \quad j = rt - 1, \quad 1 \leq r \leq q - 1, \]
\[ = g \quad \text{if} \quad j = gt - 1, \] (19)
\[ = \hat{S}^{j+1}(g) \quad \text{otherwise}. \]

**Proof:** If \( j \notin \{t-1, 2t-1, \ldots, (q-1)t-1\}, \) then by (18), \( x_m \) is not a variable of \( \hat{S}^jg, \) and \( \delta \hat{S}^j(g) = 0 \) by (6) and (9). Lemma 5 follows from (17) in this case. Note in particular that \( g = \hat{S}^m(g) \) occurs for \( j = qt - 1 = m - 1. \)

If \( j = rt - 1, \) \( 1 \leq r \leq q - 1, \) then by (8)
\[ \hat{S}^jg = \sum_{k=0}^{(q-2)/2} d_k S_{2k+1}(x_{t+1}, x_{2t+1}, \ldots, x_{(r-1)t+1}, x_{rt+1}). \]

Accordingly,
\[ \delta \hat{S}^j(g) = \sum_{k=0}^{(q-2)/2} d_k S_{2k}(x_{t+1}, x_{2t+1}, \ldots, x_{(r-1)t+1}, \]
\[ \times x_{(r+1)t+1}, \ldots, x_{(q-1)t+1}). \]
In this case, by the Corollary to Lemma 4,

\[ S_1(x_{t+1}, x_{2t+1}, \ldots, x_{(q-1)t+1}) \dot{S}^I(g) = g. \]

From Lemma 1 it now follows that \( g \dot{S}^I(g) = g \), which combined with (10), proves the lemma also in this case. \( \square \)

Define

\[ c_i = 1 \quad \text{if} \quad i = rt - 1, \quad 1 \leq r \leq q, \]
\[ = 0 \quad \text{otherwise}. \]

Then the linear shift register of Fig. 2 models \( \delta_f \). This is a consequence of the results developed in [2] and Lemma 5.

The characteristic polynomial of the shift register in Fig. 2 equals

\[ (x^m + 1) \left( \sum_{i=0}^{q} x^{it} \right). \] (20)

**Theorem 7.** When \( m = qt \) with \( q \geq 3 \) and \( t \geq 1 \), and

\[ g(x_2, \ldots, x_m) = \sum_{k=0}^{[\frac{(q-2)/2]}{2}} d_k S_{2k+1}(x_{t+1}, \ldots, x_{(q-1)t+1}), \]

with \( g(x_2, \ldots, x_m) \neq 0 \) or \( S_1(x_{t+1}, x_{2t+1}, \ldots, x_{(q-1)t+1}) \), one has

\[ p(\delta_f) = m(q + 1). \]

**Proof.** The period of \( \delta_f \) equals the period of the shift register with characteristic polynomial (20). Now \( \sum x^{it} \) divides \( x^{(q+1)t} + 1 \). Accordingly,

\[ p(\delta_f) = [m(q + 1)t] = [m, q + 1] = m(q + 1); \]

\( [\ ] \) denotes the least common multiple. \( \square \)

---

**Fig. 2.** The linear shift register model of the \( \delta_f \)-function sequence with \( g(x_2, x_3, \ldots, x_m) \) defined by (14).
That is, the period of any cycle of this shift register will divide \( m(q+1) \). A similar generalization of Theorem 5 in [2] gives

**Theorem 8.** When \( m = qt \) with \( q \geq 3 \) and \( t \geq 1 \), and

\[
g(x_2,\ldots,x_m) = \sum_{k=0}^{\lfloor (q-2)/2 \rfloor} d_k(S_{2k}(x_{t+1} \ldots, x_{(q-1)t+1}) + S_{2k+1}(x_{t+1} \ldots, x_{(q-1)t+1})),
\]

with \( g(x_2,\ldots,x_m) \neq 0 \) or \( 1 + S_1(x_{t+1} \ldots, x_{(q-1)t+1}) \). One has

\[
p(\delta_f) = m(q+1).
\]

We give one example to illustrate this theory.

**Example 1.** One chooses \( t = 2 \) and \( q = 4 \). Then \( m = 8 \) and

\[
g(x_2, x_3, \ldots, x_8) = x_3 x_5 x_7.
\]

The basis of the proper subspace \( A \) is

\[
x_1 x_3 x_5, \quad x_1 x_3 x_7, \quad x_1 x_5 x_7, \quad x_2 x_4 x_6, \quad x_2 x_4 x_8, \quad x_2 x_6 x_8, \quad x_3 x_5 x_7, \quad x_4 x_6 x_8.
\]

It is easy to compute the following cases:

\[
\delta_f^8(x_1) = x_1 + x_3 x_5 x_7,
\]

\[
\delta_f^{16}(x_1) = x_1 + x_1 x_3 x_5 + x_3 x_5 x_7,
\]

\[
\delta_f^{24}(x_1) = x_1 + x_2 x_3 x_7 + x_1 x_3 x_7,
\]

\[
\delta_f^{32}(x_1) = x_1 + x_1 x_5 x_7 + x_3 x_5 x_7,
\]

\[
\delta_f^{40}(x_1) = x_1.
\]

On the other hand, it is easy to see that \( 40 = m(q+1) \).

3. **\( g(x_2,\ldots,x_m) \) Derived from Cyclic Code**

Let \( C \) be a cyclic code of block length \( m \) with minimum distance at least 3. Let

\[
g(x_2,\ldots,x_m) = \sum_{e \in C} \left( \prod_{i=2}^{m} (x_i + e_i) \right).
\]

The following result was proved in [2].
THEOREM 9. The period of any cycle of the nonlinear shift register with feedback function defined by (2) and (22) must be a factor of $m(m + 1)$.

This result can also be generalized as

THEOREM 10. Let $m = qt$ with $q \geq 3$ and $t \geq 1$. $C$ is a cyclic code of block length $q$ with minimum distance at least 3. If

$$g(x_2, \ldots, x_m) = \sum_{e \in C} \left( \prod_{i=2}^{q} (x_{(i-1)t+1} + e_i) \right),$$

then the period of any cycle of this register must be a factor of $m(q + 1)$.

Proof. We first make the following observation. When $e_1 \neq e_2$, one of them must be 0. Therefore, we have

$$(x + e_1)(x + e_2) = x^2 + x(e_1 + e_2) + e_1 e_2 = x^2 + x = 0.$$ 

Similar to the case with $g$ defined by (14), $\hat{D}(\hat{S}^t g) \neq 0$ only when $j = (t - 1) + rt$, $0 \leq r < q - 1$. Now

$$g(\hat{D}(\hat{S}^t g)) = \left( \sum_{e \in C} \left( \prod_{i=2}^{q} (x_{(i-1)t+1} + e_i) \right) \right) \left( \sum_{d \in C} (x_{t+1} + d_{q-r+1}) \right)$$

$$\times (x_{2t+1} + d_{q-r+2}) \cdots (x_{rt+1} + d_q)(x_{(r+2)t+1} + d_{2})$$

$$\times \cdots \times (x_{(q-1)t+1} + d_{q-r-1})$$

$$= \sum_{e \in C} \left( \prod_{i=2}^{q} (x_{(i-1)t+1} + e_i) \right)$$

$$= g.$$ 

The second equality is simply because $(e_1, e_2, \ldots, e_q)$ and $(d_{a-r}, d_{a-r+1}, \ldots, d_a, d_1, \ldots, d_{q-r-1})$ have minimum distance at least 3 whenever they are different. Therefore, (19) also holds for this case. And the theorem follows. \[\square\]

ACKNOWLEDGMENT

I would like to thank Dr. S. W. Golomb for his helpful discussion during this research.

REFERENCES


