ABSTRACT

$E_k(x_2,\ldots,x_n)$ is defined by $E_k(a_2,\ldots,a_n) = 1$ if and only if $\sum_{i=2}^{n} a_i = k$.

We determine the periods of sequences generated by the shift registers with the feedback functions

$$x_1 + E_k(x_2,\ldots,x_n)$$

and

$$x_1 + E_k(x_2,\ldots,x_n) + E_{k+1}(x_2,\ldots,x_n)$$

over the field GF(2) .

1. Introduction

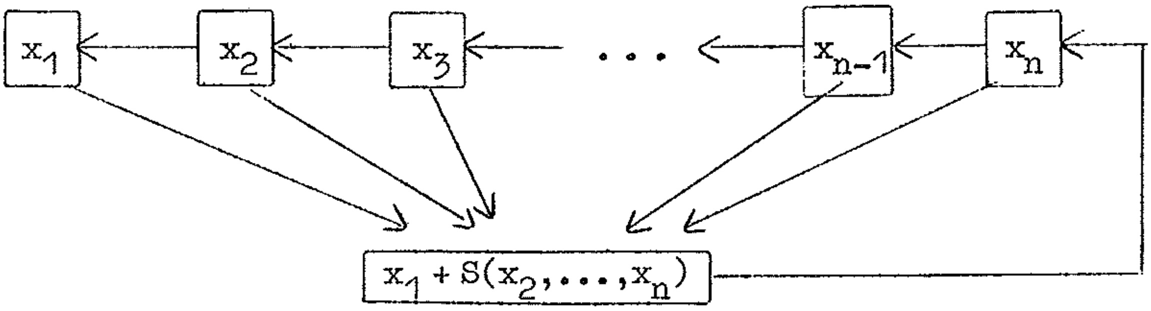

fig. 1

In this paper we study only shift registers over the field $GF(2) = \{0,1\}$ characterized by $1+1 = 0+0 = 0$ and $0+1 = 1$. Let $S(x_2,\ldots,x_n)$ be a symmetric polynomial. Fig. 1 shows a symmetric shift register of n stages with feedback function $x_1 + S(x_2,\ldots,x_n)$. If the contents of the register at a certain time instant are $\vec{x} = (x_1,\ldots,x_n)$, then the succeeding contents of the register are $\vec{x}' = (x_1',\ldots,x_n')$ given by the formula:

$$x_i' = x_{i+1} \quad \text{if} \quad i < n \quad \text{and} \quad x_n' = x_1 + S(x_2,\ldots,x_n) .$$

The general problem is: If the contents of the shift register are $\vec{a} = (a_1,\ldots,a_n)$ how many times must the register be shifted before its contents again are $\vec{a}$. The minimal number of times the register must be shifted until this happens, is called the minimal period of $\vec{a}$. The general problem is equivalent to finding the minimal periods of the sequences $(a_t)_{t=1}^{\infty}$ satisfying the nonlinear difference equation

$$a_{n+t} = a_t + S(a_{1+t},\dots,a_{n-1+t}) \quad \text{for} \quad t > 0 \,.$$

For a general treatment of non-linear shift registers see [2].

We shall in this paper determine the periods of the sequences generated by some symmetric shift registers. The paper is inspired by Kjeldsen who studied such registers in [3].

The weight $w(\vec{a})$ of a vector $\vec{a} = (a_1,\dots,a_n)$ is defined by $w(\vec{a}) = \sum_{i=1}^{n} a_i$. We define $E_k(x_2,\dots,x_n)$ for $k \in \{0,\dots,n-1\}$ by the following equivalens:

$$E_k(a_2,\dots,a_n) = 1 \text{ if and only if } w(a_2,\dots,a_n) = k \,.$$

We give a brief outline of the paper. In section 2 we show that it suffices to determine the periods when $S = \sum_{k=p}^{p+s} E_k$. If these periods are known, the periods of all the symmetric shift registers can be determined. In section 3 we determine the periods when $S = E_k$ and give an alternative proof of some of the results given by Kjeldsen in [3]. In section 4 we determine the periods when $S = E_k + E_{k+1}$.

We denote $\vec{b} = (b_1,\dots,b_n) \in \{0,1\}$ also by $\vec{b} = b_1 \dots b_n$.

2. Reduction of the general problem

Let S_p be the homogeneous symmetric polynomial of degree p in the variables $x_2,\dots,x_n$ where $p \in \{0,1,\dots,n-1\}$;

$$S_p(x_2,\dots,x_n) = \sum_{2\leq i_1<\dots<i_p\leq n} x_{i_1}\cdots x_{i_p} .$$

The next lemma shows that $\{E_k : k \in \{0,\dots,n-1\}\}$ is a basis for the vector space of all the symmetric polynomials in the variables $x_2,\dots,x_n$. Besides the lemma shows how to obtain the coordinates with respect to this basis.

Lemma 2.1 Let $p \in \{0,\dots,n-1\}$.
Then,

$$S_p = \sum_{k=o}^{n-1} \binom{k}{p} (\mathrm{mod}\, 2) E_k .$$

$\binom{k}{p}$ denotes the binominal coefficient.

Proof: Suppose $w(a_2,\dots,a_n) = k$ and $a_{j_1} = \dots = a_{j_k} = 1$.
Then,

$$S_p(a_2,\dots,a_n) = \sum_{\substack{2\leq i_1<\dots<i_p\leq n \\ \{i_1,\dots,i_p\}\subset\{j_1,\dots,j_k\}}} a_{i_1}\cdots a_{i_p} = \binom{k}{p}(\mathrm{mod}\, 2)$$

since every term in the sum is equal to 1, and since it is $\binom{k}{p}$ terms in the sum.

We get

$$S_p = \sum_{k=o}^{n-1} \binom{k}{p} (\mathrm{mod}\, 2) E_k ,$$

and we have proved the assertion.

Q.E.D.

We define intervals in the set of the integers $\mathbb{Z}$ in the usual way by $[q,t] = \{i : i \in \mathbb{Z} \text{ and } q \leq i \leq t\}$.

Theorem 2.2 Let S be the symmetric polynomial in the variables $x_2,\dots,x_n$ given by

$$S = \sum_{k \in M} E_k$$

and

$M = \bigcup_{i=1}^{f} [q_i,t_i]$ where q_i and t_i are integers such that $t_i + 1 < q_{i+1}$ for $i \in \{1,\dots,f-1\}$.

Let $\vec{a} = (a_1,\dots,a_n)$ be fixed and let $P(S,\vec{a})$ be the minimal period of $\vec{a}$ with respect to the shift register with feedback function $x_1 + S(x_2,\dots,x_n)$.

a) If $w(\vec{a}) \in [q_i,t_i+1]$, then $P(S,\vec{a})$ is equal to the minimal period of $\vec{a}$ with respect to the shift register generated by $x_1 + \sum_{k=q_i}^{t_i} E_k$.

b) If $w(\vec{a}) \notin \bigcup_{i=1}^{f} [q_i,t_i+1]$, then $P(S,\vec{a})$ is equal to the minimal period of $\vec{a}$ with respect to the pure cycling shift register with feedback function x_1.

By Lemma 2.1 every symmetric polynomial is on the form

$$S = \sum_{k=o}^{n-1} a_k E_k \quad \text{where} \quad a_k \in \{0,1\}.$$

By Theorem 2.2 it is sufficient to determine the periods of the sequences generated by polynomials on the form

$$S = \sum_{k=q}^{q+s} E_k \quad \text{where} \quad 0 \leq q \leq q+s \leq n-1.$$

In the last chapters we shall solve this problem for $s = 0$ and $s = 1$.

Proof of Thm. 2.2: If $\vec{b} = (b_1,\dots,b_n)$ are the contents of the shift register with feedback function S, $\vec{b}' = (b_1',\dots,b_n')$ are the succeeding contents of the register.

If $w(\vec{b}) \in [q_i, t_i+1]$, we observe that

$$w(\vec{b}') \in [q_i, t_i+1]$$

and

$$b_1 + S(b_2,\dots,b_n) = b_1 + \sum_{k=q_1}^{t_i} E_k\,(b_2,\dots,b_n)\ .$$

By this observation a) follows.

If $w(\vec{b}) \notin \bigcup_{i=1}^{f} [q_i, t_i+1]$, we observe that

$$w(\vec{b}') \notin \bigcup_{i=1}^{f} [q_i, t_i+1]$$

and

$$b_1 + S(b_2,\dots,b_n) = b_1\ .$$

By this observation b) follows.

Q.E.D.

3. The situation $S = E_k$.

Theorem 3.1 Suppose $n > 3$.

Let $\vec{a} = (a_1,\dots,a_n) \in \{0,1\}^n$ and $k \in \{0,1,\dots,n-1\}$. Further, let $P(E_k,\vec{a})$ be the minimal period of $\vec{a}$ with respect to the shift register with the feedback function $x_1 + E_k(x_2,\dots,x_n)$.

a) If $w(\vec{a}) \in \{k,k+1\}$, $P(E_k,\vec{a})$ divides $n+1$.

b) If $w(\vec{a}) \notin \{k,k+1\}$, $P(E_k,\vec{a})$ divides n.

c) There exists $\vec{a}$ such that $P(E_k,\vec{a})$ is equal to respectively n and $n+1$.

Before the proof of the theorem we must show a lemma and introduce some notations. Let $1_t = 11\dots1$ (resp. $0_t = 00\dots0$) denote a string of t consecutive 1's (resp. 0's).

Definition 3.2 If A is a finite sequence of numbers, then $l(A)$ is the length of A.

Definition 3.3 $\mu : \{0,1\}^n \to \{0,1\}^n$ is defined by $\mu(\vec{b}) = \vec{b}'$, where b' is the successor of $\vec{b}$ in the shift register with the feedback function $x_1 + E_k(x_2,\dots,x_n)$. Let $\mu_p^i(\vec{b})$ be coordinate number p of $\mu^i(\vec{b})$.

Lemma 3.4 Let $\vec{a} = (a_1,\dots,a_n) \in \{0,1\}^n$. Suppose $w(\vec{a}) = k+1$ and

$$\vec{a} = 1_s 0_t B \quad \text{where} \quad s \geq 1 \quad \text{and} \quad t \geq 1 .$$

Then

$$\mu^{s+t}(\vec{a}) = B\,0\,1_s 0_{t-1} .$$

3. The situation $S = E_k$.

Theorem 3.1 Suppose $n > 3$.

Let $\vec{a} = (a_1,\ldots,a_n) \in \{0,1\}^n$ and $k \in \{0,1,\ldots,n-1\}$. Further, let $P(E_k,\vec{a})$ be the minimal period of $\vec{a}$ with respect to the shift register with the feedback function $x_1 + E_k(x_2,\ldots,x_n)$.

a) If $w(\vec{a}) \in \{k,k+1\}$, $P(E_k,\vec{a})$ divides $n+1$.

b) If $w(\vec{a}) \notin \{k,k+1\}$, $P(E_k,\vec{a})$ divides n.

c) There exists $\vec{a}$ such that $P(E_k,\vec{a})$ is equal to respectively n and $n+1$.

Before the proof of the theorem we must show a lemma and introduce some notations. Let $1_t = 11\ldots1$ (resp. $0_t = 00\ldots0$) denote a string of t consecutive 1's (resp. 0's).

Definition 3.2 If A is a finite sequence of numbers, then $l(A)$ is the length of A.

Definition 3.3 $\mu : \{0,1\}^n \rightarrow \{0,1\}^n$ is defined by $\mu(\vec{b}) = \vec{b}'$, where b' is the successor of $\vec{b}$ in the shift register with the feedback function $x_1 + E_k(x_2,\ldots,x_n)$. Let $\mu_p^i(\vec{b})$ be coordinate number p of $\mu^i(\vec{b})$.

Lemma 3.4 Let $\vec{a} = (a_1,\ldots,a_n) \in \{0,1\}^n$. Suppose $w(\vec{a}) = k+1$ and

$$\vec{a} = 1_s 0_t B \quad \text{where} \quad s \geq 1 \quad \text{and} \quad t \geq 1 .$$

Then

$$\mu^{s+t}(\vec{a}) = B\,0\,1_s 0_{t-1} .$$

Proof: Since $w(a_2,\dots,a_n) = k$, we have

$$\mu(\vec{a}) = 1_{s-1}0_t B\,0 .$$

When $s \geq 2$, we have $w(\mu_2(\vec{a}),\dots,\mu_n(\vec{a})) = k-1$, which implies

$$\mu^2(\vec{a}) = 1_{s-2}0_t B\,0\,1 .$$

We argue in the same way and get

$$\mu^s(\vec{a}) = 0_t B\,0\,1_{s-1} .$$

Since $w(\mu_2^s(\vec{a}),\dots,\mu_n^s(\vec{a})) = k$, we have

$$\mu^{s+1}(\vec{a}) = 0_{t-1}B\,0\,1_s .$$

When $t \geq 2$, we have $w(\mu_2^{s+1}(\vec{a}),\dots,\mu_n^{s+1}(\vec{a})) = k+1$, which implies

$$\mu^{s+2}(\vec{a}) = 0_{t-2}B\,0\,1_s 0 .$$

We argue in the same way and get

$$\mu^{s+t}(\vec{a}) = B\,0\,1_s 0_{t-1} .$$

Q.E.D.

Proof of thm. 3.1:

a) Suppose $w(\vec{a}) = k$ and $\vec{a} = 1_s 0 B$. By using the same method as in the proof of Lemma 3.4, we get

$$\mu^{s+1}(\vec{a}) = B\,1_{s+1} .$$

Therefore we can without loss of generality assume that $w(\vec{a}) = k+1$. We can also assume that $a_1 = 1$.

Suppose now that

$$\vec{a} = 1_{s_1}0_{t_1}\dots 1_{s_p}0_{t_p}$$

where $s_i \geq 1$ for $i \in \{1,\dots,p\}$, $t_i \geq 1$ for $i \in \{1,\dots,p-1\}$, and $w(\vec{a}) = k+1$.

$p = 1$ is a special case which follows directly from Lemma 3.4. Suppose therefore that $p > 1$. We define for $1 \leq i \leq p-1$

$$Q_i = 1_{s_i} 0_{t_i} \quad \text{and} \quad Q_i' = 0\, 1_{s_i} 0_{t_i - 1} .$$

By Lemma 3.4 we get

$$\mu^{l(Q_1)}(\vec{a}) = Q_2 \dots Q_p Q_1' .$$

By induction we get

$$\mu^{l(Q_1 \dots Q_{p-1})}(\vec{a}) = Q_p Q_1' \dots Q_{p-1}'$$

$$= 1_{s_p} 0_{t_p+1} 1_{s_1} 0_{t_1} \dots 1_{s_{p-1}} 0_{t_{p-1}-1}$$

and by Lemma 3.4

$$\mu^{n+1}(\vec{a}) = \mu^{l(Q_1 \dots Q_{p-1})+s_p+t_p+1}(\vec{a}) = \vec{a} .$$

b) If $\vec{b} = (b_1,\dots,b_n) \in \{0,1\}^n$ and $w(\vec{b}) \notin \{k,k+1\}$, we get

$$w(\mu(\vec{b})) = w(\vec{b}) \notin \{k,k+1\}$$

and

$$b_1 + E(k)(b_2,\dots,b_n) = b_1 .$$

From this observation b) follows.

c) It is readily verified that $\vec{a} = 0_{n-k-1}\, 1_{k+1}$ has minimal period $n+1$. If $k > 1$, $\vec{a} = 0_{n-1} 1$ has minimal period n. If $k = 0$ or $k = 1$, $\vec{a} = 0\, 1_{n-1}$ has minimal period n, since $n > 3$.

Q.E.D.

The following theorem has Kjeldsen proved in [3]. We give an alternative proof of his theorem.

Theorem 3.5 Let S_k be the homoheneous polynomial in the variables $x_2,\ldots,x_n$ of degree k. Suppose

$$g = \sum_{c\leq k\leq \frac{n-2}{2}} a_k S_{2k+1} \quad \text{where} \quad a_k \in \{0,1\}$$

and

$$h = \sum_{o\leq k\leq \frac{n-2}{2}} b_k(S_{2k}+S_{2k+1}) \quad \text{where} \quad b_k \in \{0,1\} .$$

Then the minimal periods of the sequences generated by g and h divides n or $n+1$.

Proof: By Lucas' theorem (Thm. 4.71 in [1])

$$\binom{2q+a}{2p+b} = \binom{2q}{2p}\binom{a}{b} \pmod 2 \quad \text{where} \quad a,b \in \{0,1\}$$

and q and p are nonnegative integers.

This implies

(1) $$\binom{2q}{2p+1} = 0 \pmod 2$$

and

(2) $$\binom{2q+1}{2p+1} = \binom{2q+1}{2p} \pmod 2 .$$

Suppose p is odd.

By Lemma 2.1

$$S_p = \sum_{\substack{q=o\\ q \text{ odd}}}^{n-1} \binom{q}{p} E_q + \sum_{\substack{q=o\\ q \text{ even}}}^{n-1} \binom{q}{p} E_q .$$

By (1)

(3) $$S_p = \sum_{\substack{q=o\\ q \text{ odd}}}^{n-1} \binom{q}{p} E_q .$$

Accordingly, $g = \sum_{s \in \Delta} E_s$ for some $\Delta \subset \{1,3,\dots\}$.

Suppose $0 \leq p \leq \frac{n-2}{2}$. (2), (3) and Lemma 2.1 imply that

$$S_{2p} + S_{2p+1} = \sum_{\substack{q=o \\ q \text{ odd}}}^{n-1} \left(\binom{q}{2p+1} + \binom{q}{2p}\right) E_q + \sum_{\substack{q=o \\ q \text{ even}}}^{n-1} \binom{q}{2p} E_q$$

$$= \sum_{\substack{q=o \\ q \text{ even}}}^{n-1} \binom{q}{2p} E_q \, .$$

Accordingly, $h = \sum_{s \in \Delta} E_s$ for some $\Delta \subset \{0,2,\dots\}$.

By Theorem 2.2 and Theorem 3.1 the theorem follows.

Q.E.D.

4. The situation $S = E_k + E_{k+1}$.

In this section we let $n \geq 4$ and $k \in \{0,\dots,n-2\}$ be fixed. We shall study only the shift register with feedback function $x_1 + (E_k + E_{k+1})(x_2,\dots,x_n)$.

<u>Definition 4.1</u> If $\vec{b} = (b_1,\dots,b_n) \in \{0,1\}^n$ are the contents of the shift register with feedback function $x_1 + (E_k + E_{k+1})(x_2,\dots,x_n)$, we shall denote the succeeding contents with $\theta(\vec{b})$:

$$\theta(\vec{b}) = (b_2,\dots,b_n,b_1 + (E_k+E_{k+1})(b_2,\dots,b_n)) .$$

Let $\theta_p^i(\vec{b})$ be the coordinate number p of $\vec{b}$.

We first sketch the idea of the proofs in this section. The next definition of the isolated ones and the blocks of vectors is essential. If we know the blocks and the isolated ones of $\vec{b}$, we are able to determine the blocks and the isolated ones of $\vec{c} = \theta^{n+2+2\alpha(\vec{b})}$, where $\alpha(\vec{b})$ is an integer dependent of $\vec{b}$. $\alpha(\vec{b})$ is often equal to zero. Next we determine the blocks and the isolated ones of

$$\theta^{(n+2)+2\alpha(\vec{c})}(\vec{c}) = \theta^{2(\alpha(\vec{b})+\alpha(\vec{c}))+2(n+2)}(\vec{b})$$

etc. At last we obtain a vector $\theta^p(\vec{b})$ with the same blocks and isolated ones as $\vec{b}$. Because every 1 in $\vec{b}$ is isolated or contained in a block, $\theta^p(\vec{b}) = \vec{b}$, and p is a period of $\vec{b}$.

A block of the vector $\vec{b}$ is a segment $b_j \dots b_t$ of $\vec{b}$ such that $b_{j-1} = 0$ or $j = 1$, the segment starts with more than one 1 , does not contain 00 and is succeeded by more than one 0 , unless we consider the last block in $\vec{b}$. In that case it need not be succeeded by zeros.

The isolated ones in $\vec{b}$, which are not contained in the blocks, are 1's which are not contained in any block and with a 0 before and after the 1 . The isolated ones in $\vec{b}$, which are contained in a block, are the 1's in the block which are succeeded by a 0 also lying in the block.

The blocks and the isolated ones are defined precisely in the next definition.

Definition 4.2 Let $\vec{b} = b_1 \ldots b_n \in \{0,1\}^n$ and define the blocks and the isolated ones of $\vec{b}$ inductively as follows:

Suppose that the blocks and the isolated ones of $b_1 \ldots b_i$ are defined. In the basis step let $i = 0$.

Let $j > i$ be the first $j > i$ such that $b_j = 1$. We have two cases.

1) $b_j = 1$ and $b_{j+1} = 0$ or $j=n$. By definition $E = b_j$ is an isolated one.

2) $b_j = b_{j+1} = 1$. We let p be the first $p > j$ such that $b_{p+1} = b_{p+2} = 0$. By definition $B = b_j \ldots b_p$ is a block. If no such p exists, the block B is defined by

$$B = b_j \ldots b_{n-1} \quad \text{if} \quad b_n = 0$$

and

$$B = b_j \ldots b_n \quad \text{if} \quad b_n = 1 .$$

We define the isolated ones contained in a block B in the following way:

Suppose $B = b_j \ldots b_p$ is a block, and put

$$\mathcal{M} = \{q \in \{j,\ldots,p\}; b_q = 0\} .$$

Then

$$E = a_{q-1} \text{ is an isolated one if and only if } q \in \mathcal{M} .$$

We illustrate the definition by the example below. $*$'s are placed above the isolated ones of $\vec{b}$ and the blocks are underlined.

$$\vec{b} = 0\overset{*}{1}0\underline{1\overset{*}{1}01\overset{*}{1}01}00\underline{111}00\overset{*}{1}00\underline{11}$$

Now we state the results.

<u>Main Lemma 4.3</u> Suppose $\vec{b} \in \{0,1\}^n$, $w(\vec{b}) = k+2$ and

$$\vec{b} = 0_{a_0} B_1 0_{a_1} \ldots B_s 0_{a_s}$$

where B_i is a block or an isolated one not contained in any block. We also suppose that $\vec{b}$ does not start with 10 .

Then $\theta^{n+2}(\vec{b})$ is equal to the vector obtained by the following changes of $\vec{b}$:

1) If B_i is an isolated one, permute B_i and the preceeding 0 .

2) If $B_i = 1Q$ is a block, substitute $B_i' = Q1$ for B_i .

<u>Theorem 4.4</u>: Suppose $\vec{b} \in \{0,1\}^n$ and $w(\vec{b}) = k+2$. Let $E(\vec{b})$ be the number of isolated ones in $\vec{b}$ and $B(\vec{b})$ the number of blocks in $\vec{b}$.

If $E(\vec{b}) > 0$ and $B(\vec{b}) > 0$,

$$2E(\vec{b}) + (n+1 - 2B(\vec{b}) - 2E(\vec{b}))(n+2)$$

is a period of $\vec{b}$ with respect to the feedback function $x_1 + (E_k + E_{k+1})(x_2,\ldots,x_n)$.

A cycle of the shift register with feedback function $x_1 + (E_k + E_{k+1})(x_2,\ldots,x_n)$ is

$$\theta(\vec{b}) \to \theta^2(\vec{b}) \to \ldots \to \theta^P(\vec{b}) = \vec{b} .$$

where P is the least positive integer such that $\theta^P(\vec{b}) = \vec{b}$. The minimal period of $\vec{b}$ is equal to the length of the cycle containing $\vec{b}$.

<u>Theorem 4.5</u> Let $\vec{b} \in \{0,1\}^n$, and let $P = P(E_k+E_{k+1},\vec{b})$ denote the minimal period of $\vec{b}$ with respect to the shift register with feedback function $x_1 + (E_k+E_{k+1})(x_2,\ldots,x_n)$.

1) If $w(\vec{b}) \notin \{k,k+1,k+2\}$, P divides n.

2) There exist $\vec{c}$ on the cycle of $\vec{b}$ such that $w(\vec{c}) = k+2$. Let $E(\vec{c})$ and $B(\vec{c})$ be respectively the number of the isolated ones and the blocks of $\vec{c}$.

   If $E(\vec{c}) = 0$, P divides $n+2$.

   If $B(\vec{c}) = 0$, P divides $n+1$.

   If $E(\vec{c}) \neq 0$ and $B(\vec{c}) \neq 0$, P divides $2E(\vec{c}) + (n+1-2E(\vec{c})-2B(\vec{c}))(n+2)$.

3) If $w(\vec{b}) \in \{k,k+1\}$, and if there does not exist any $\vec{c}$ on the cycle containing $\vec{b}$ such that $w(\vec{c}) = k+2$, P divides $n+1$.

<u>Theorem 4.6</u> Let $\vec{b} \in \{0,1\}^n$ and $P = P(E_k+E_{k+1},\vec{b})$ be the minimal period of $\vec{b}$ with respect to the shift register with feedback function $x_1 + (E_k+E_{k+1})(x_2,\ldots,x_n)$. Let

$$\mathcal{M} = \{2e+(n+1-2e-2b)(n+2):\ e,b \text{ are positive integers};\ 2b+e \leq k+2;\ 2e+4b-2 \leq n\}$$

1) P divides one of the numbers in the set $\mathcal{M} \cup \{n,n+1,n+2\}$.

2) Every element of $\mathcal{M}$ is the minimal period for a suitably chosen cycle of our shift register.

Now we illustrate by an example how the main lemma is used to prove the theorems. First we do an observation.

<u>Observation 4.7</u> If $w(\vec{b}) = k+2$ and $\vec{b} = 10Q$, $\theta^2(\vec{b}) = Q01$.

In the following example we put a * above the isolated ones and underline the blocks to see how they move and change, We use the Main Lemma 4.3 and the Observation 4.7 several times. We put $n = 22$.

$$\begin{aligned}
\vec{b} &= 0\overset{*}{1}0\underline{1\overset{*}{1}01\overset{*}{1}01}00\underline{111}00\overset{*}{1}00\underline{11}\\
\theta^{n+2}(\vec{b}) &= 1001011011001110100011\\
\theta^{n+2+2}(\vec{b}) &= 0\overset{*}{1}0\underline{1\overset{*}{1}011}00\underline{11\overset{*}{1}01}000\underline{1\overset{*}{1}01}\\
\theta^{2(n+2)+2}(\vec{b}) &= 1001011100110110001011\\
\theta^{2(n+2)+4}(\vec{b}) &= 0\overset{*}{1}0\underline{111}00\underline{1\overset{*}{1}011}000\overset{*}{1}0\underline{1\overset{*}{1}01}\\
\theta^{3(n+2)+4}(\vec{b}) &= 1001110010111001001011\\
\theta^{3(n+2)+6}(\vec{b}) &= 0\underline{111}00\overset{*}{1}0\underline{111}00\overset{*}{1}00\overset{*}{1}0\underline{1\overset{*}{1}01}\\
\theta^{4(n+2)+6}(\vec{b}) &= 0\underline{11\overset{*}{1}01}00\underline{11\overset{*}{1}01}00\overset{*}{1}00\overset{*}{1}0\underline{11}\\
\theta^{5(n+2)+6}(\vec{b}) &= 0\underline{1\overset{*}{1}011}00\underline{1\overset{*}{1}01\overset{*}{1}01}00\overset{*}{1}00\underline{11}\\
\theta^{6(n+2)+6}(\vec{b}) &= 0\overset{*}{1}0\underline{111}00\overset{*}{1}0\underline{1\overset{*}{1}01\overset{*}{1}01}000\underline{11}\\
\theta^{7(n+2)+6}(\vec{b}) &= 1001110100101101100011\\
\theta^{7(n+2)+8}(\vec{b}) &= 0\underline{11\overset{*}{1}01}00\overset{*}{1}0\underline{1\overset{*}{1}011}000\underline{1\overset{*}{1}01}\\
\theta^{8(n+2)+8}(\vec{b}) &= 0\underline{1\overset{*}{1}01\overset{*}{1}01}00\overset{*}{1}0\underline{111}000\overset{*}{1}0\underline{11}\\
\theta^{9(n+2)+8}(\vec{b}) &= 0\overset{*}{1}0\underline{1\overset{*}{1}01\overset{*}{1}01}00\underline{111}00\overset{*}{1}00\underline{11} = \vec{b}
\end{aligned}$$

This implies that $8 + 9(n+2)$ is a period of $\vec{b}$. The number of the isolated ones and blocks of $\vec{b}$ is respectively $E(\vec{b}) = 4$ and $B(\vec{b}) = 3$. We put this into the formula of Theorem 4.4. and get

$$2E(\vec{b}) + (n+1-2E(\vec{b})-2B(\vec{b}))(n+2) = 8 + (23-8-6)(n+2) = 8 + 9(n+2) .$$

Now we present the proofs of the main lemma and the theorems. But first we introduce some notations.

Definition 4.8 If $C = b_i \ldots b_j$ is a segment of $\vec{b} = (b_1, \ldots, b_n) \in \{0,1\}^n$, we define

$$h(\vec{b},C) = j , \quad v(\vec{b},C) = i , \quad \text{and} \quad \text{Place}(\vec{b}.C) = i,\ldots,j .$$

Definition 4.9 Let $p(10) = 1010\ldots 10$ denote a string of p consecutive bigrams 10.

If $\vec{b} = Pp(10)Q$ where $p \geq 1$, P does not end with 10, and Q does not start with 10, then $p(10)$ is called a sequence of isolated ones in $\vec{b}$.

Definition 4.10 Let B be a block of $\vec{b}$, x the number of 0's in B, and y the number of 1's in B. Then the mass of B is defined by

$$m(\vec{b}.B) = y - x .$$

Definition 4.11 Suppose $\theta^{n+2}(\vec{b}) = p(10)D$ where $p \geq 0$ and D does not start with 10. We define

$$\alpha(\vec{b}) = p \quad \text{and} \quad \psi(\vec{b}) = \theta^{n+2+2\alpha(\vec{b})}(\vec{b}) .$$

Definition 4.12 Let B be a block and $F = p(10)$ a sequence of isolated ones in $\vec{b}$. In the following three situations we say that F and the isolated ones in F follow B:

$$\vec{b} = CBOOFD \quad \text{or} \quad \vec{b} = OFQB \quad \text{or} \quad \vec{b} = 1FQB .$$

Definition 4.13 Let E be an isolated one and B a block in $\vec{b}$.

Define $K(\vec{b},E) = 1$ if E follows a block in $\vec{b}$, otherwise $K(\vec{b},E) = 0$.

Define $K(\vec{b},B) = p$ if B is followed by a sequence of p isolated ones, otherwise $K(\vec{b},B) = 0$.

In the rest of this section $\vec{b}$ will usually satisfy the following claim:

Claim 4.14

1) $\vec{b} \in \{0,1\}^n$ and $w(\vec{b}) = k+2$.

2) $\vec{b}$ contains at least one block and at least one isolated one.

3) $\vec{b}$ ends with a block which we denote B_{END}.

4) $\vec{b}$ does not begin with 10.

Lemma 4.15 Let $\vec{b}\{0,1\}^n$.

1) If $w(\vec{b}) = k+1$ and $\vec{b} = QC$ where $Q = 1_{s_o} 01_{s_1} \cdots 1_{s_{p-1}} 01_{s_p}$ and $s_i \geq 1$, then

$$\theta^{l(Q)}(\vec{b}) = C0Q' \quad \text{where} \quad Q' = 1_{s_o}01_{s_1}\dots 01_{s_p-1} \ .$$

2) If $w(\vec{b}) = k+2$ and $\vec{b} = 1Q00C$ where $Q = 1_{s_o}01_{s_1}\dots 01_{s_p}$, then

$$\theta^{l(Q)+3}(\vec{b}) = C00Q1 \ .$$

Proof: 1) We show 1) by induction with respect to the number of zeros in Q . If $Q = 1_s$, 1) is proved as the first part of the proof of the induction step. Suppose 1) is proved for $p = q-1$ zeros in Q , and let Q contain $p = q$ zeros. Since $w(b_2,\dots,b_n) = k$ we have

$$\theta(\vec{b}) = 1_{s_o}01_{s_1}0\dots 01_{s_p}C0 \ .$$

If $s_o \geq 2$, $w(\theta(\vec{b})_2,\dots,\theta(\vec{b})_n) = k-1$, which implies

$$\theta^2(\vec{b}) = 1_{s_o-2}01_{s_1}0\dots 01_{s_p}C01 \ .$$

By the same argument we get

$$\theta^{s_o}(\vec{b}) = 01_{s_1}0\dots 1_{s_p}C\,0\,1_{s_o-1} \ .$$

$w(\theta^{s_o}(\vec{b})_2,\dots,\theta^{s_o}(\vec{b})_n) = k$ implies

$$\theta^{s_o+1}(\vec{b}) = 1_{s_1}0\dots 01_{s_p}C\,0\,1_{s_o} \ .$$

Since we have assumed that 1) is correct when Q contains $q-1$ zeros, we get

$$\theta^{l(Q)+2}(\vec{b}) = CQ' \ ,$$

and 1) is proved.

2) Since $w(b_2,\dots,b_n) = k+1$, $\theta(\vec{b}) = Q00C0$. Since $w(\theta(\vec{b})) = k+1$ it follows from 1) that

$$\theta^{l(Q)+1}(\vec{b}) = 00C00Q' \ .$$

Simple calculation shows that

$$\theta^{l(Q)+3}(\vec{b}) = C00Q1 .$$

Q.E.D.

Proof of the Main Lemma 4.3: If $\vec{b} = B_1$, $\vec{b} = B_1 0$ or $\vec{b} = 0B_1$, the claim follows from lemma 4.15.1 by trivial computations. We assume $\vec{b} \neq B_1$, $\vec{b} \neq B_1 0$ and $\vec{b} \neq 0B_1$. We define $l_i = l(0_{a_0} B_1 \ldots B_i 0_{a_i})$. Observation 4.7 and lemma 4.15.2 imply by induction

(4) $\qquad w(\theta^{l_i}(\vec{b})) = k+2 \quad$ for $i < s$.

Suppose $i \in \{0,\ldots,s-1\}$. If B_{i+1} is an isolated one, $\theta^{l_i}(\vec{b})$ is on the form

(5) $\qquad \theta^{l_i}(\vec{b}) = B_{i+1}0R$.

If B_{i+1} is a block, $\theta^{l_i}(\vec{b})$ is on the form

(6) $\qquad \theta^{l_i}(\vec{b}) = B_{i+1}00R$,

because (6) is true trivially for $i < s-1$ since a block is succeeded by two zeros. Since $\vec{b}$ does not start with 10 , $\theta^2(\vec{b}) = TB_s00$ which implies (6) for $i = s-1$.

Suppose $B_{i+1} = 1$ is an isolated one. We observe that $\text{Place}(\vec{b},B_{i+1}) = l_i + 1$. From (4), (5) and Observation 4.7 we get

$$\theta^{l_i+2}(\vec{b}) = R01 .$$

Since $n+2 = (n-l_i)+l_i+2$, there is a one in the coordinate

$$n-(n-l_i) = l_i = \text{Place}(\vec{b},B_{i+1})-1 \quad \text{in} \quad \theta^{n+2}(\vec{b}) .$$

By (4) and (5), $w(\theta^{l_i+2}(\vec{b})) = k+2$, which implies $\theta^{l_i+3}(\vec{b}) = R'010$ for suitable R' . Since $n+2 = (n-l_i-1)+l_i+3$, there is a zero in the coordinate

$$n-(n-l_i-1) = l_i+1 = \text{Place}(\vec{b},B_{i+1}) \quad \text{in} \quad \theta^{n+2}(\vec{b}) .$$

That corresponds to the change 1).

Suppose next $B_{i+1} = 1Q$ is a block. We observe that $v(\vec{b},B_{i+1}) = l_i+1$. From (4), (6) and Lemma 4.15.2 we get $\theta^{l_i+l(B_{i+1})+2}(\vec{b}) = R00Q1$.

We have

$$v(\theta^{l_i+l(B_{i+1})+2}(\vec{b}),Q1) = n+1-l(B_{i+1}) .$$

$n+2 = n-l_i-l(B_{i+1})+(l_i+l(B_{i+1})+2)$ implies

$$v(\theta^{n+2}(\vec{b}),Q1) = n+1-l(B_{i+1})-(n-l_i-l(B_{i+1})) = l_i+1 = v(\vec{b},1Q) .$$

That corresponds to the change 2).

Q.E.D.

Lemma 4.16 Suppose $\vec{b}$ satisfies the claim 4.14.

1) If E is an isolated one in $\vec{b}$, following a block different from B_{END}, there is an isolated one in coordinate number $Place(\vec{b},E)-3$ in $\theta^{n+2}(\vec{b})$.

2) If E is an isolated one in $\vec{b}$, following B_{END} or E does not follow any block in $\vec{b}$, there is an isolated one in coordinate number $Place(\vec{b},E)-1$ in $\vec{b}$.

3) If B is a block in $\vec{b}$ different from B_{END}, there is a block B' in $\theta^{n+2}(\vec{b})$ such that

$$m(\theta^{n+2}(\vec{b}),B') = m(\vec{b},B) \quad\text{and}\quad h(\theta^{n+2}(\vec{b}),B') = h(\vec{b},B)+2K(\vec{b},B) .$$

4) There is a block B'_{END} in $\theta^{n+2}(\vec{b})$ such that

$$m(\theta^{n+2}(\vec{b}),B'_{END}) = m(\vec{b},B_{END}) \quad\text{and}\quad h(\theta^{n+2}(\vec{b}),B'_{END}) = n .$$

Proof: 1) Suppose $\vec{b} = CB00p(10)D$ where $B = 1Q$ is a block and D does not start with 10. The isolated ones, following B, are in the coordinates

(7) $\quad h(\vec{b},B)+3+2i \quad \text{for} \quad i = 0,\ldots,p-1$.

By Lemma 4.3

$$\theta^{n+2}(\vec{b}) = C'Q10p(10)D' \quad \text{where} \quad l(C') = l(C) .$$

Since Q ends with 1 , $10(p-1)(10)1$ is a segment of a block B' in $\theta^{n+2}(\vec{b})$ occupying the coordinates

$$h(\vec{b},B),\ldots,h(\vec{b},B)+2p .$$

There are isolated ones contained in B' in the coordinates

(8) $\quad h(\vec{b},B)+2i \quad \text{for} \quad i = 0,\ldots,p-1$,

since they are succeeded by zeros in B' .

(7) and (8) imply 1) .

2) We consider first the isolated ones which follow B_{END} . Suppose $\vec{b} = 0p(10)D$, where D does not start with 10 . By Lemma 4.3 , $\theta^{n+2}(\vec{b}) = p(10)D'$. We observe that the p isolated ones has been shifted one coordinate to the left as claimed.

Suppose E is an isolated one in $\vec{b}$, which does not follow any block. Then $\vec{b} = C00p(10)E0D$ where $p \geq 0$ and C might be empty. By Lemma 4.3

$$\theta^{n+2}(\vec{b}) = C'0p(10)E0D' \qquad \text{where} \quad l(C') = l(C) \quad \text{and}$$

where C' is empty or ends with a zero. We see that E is an isolated one in $\theta^{n+2}(\vec{b})$ shifted one coordinate to the left in relation to its position in $\vec{b}$.

3) Suppose now that $\vec{b} = CB00p(10)D$ where D does not start with 10 . We assume $p > 0$. Observe that $p = K(\vec{b},B)$. We assume $B = 1Q$ where $Q = q(10)T$ and T does not start with 10 . By

Lemma 4.3 we get

$$\theta^{n+2}(\vec{b}) = C'Q10p(10)0D' = C'q(10)T10p(10)0D'$$

where C' ends with two zeros or is empty and $l(C') = l(C)$. We notice that $B' = T10(p-1)(10)1$ is a block in $\theta^{n+2}(\vec{b})$ such that

$$h(\theta^{n+2}(\vec{b}),B') = h(\vec{b},B) + 2p .$$

Let x_0 and x_1 be respectively the number of 0's and 1's in T. We have

$m(\theta^{n+2}(\vec{b}),B') = (x_1+1+p) - (x_0+p) = x_1+1-x_0$,

and

$m(\vec{b},B) = (1+q+x_1) - (x_0+q) = x_1+1-x_0$,

and we are done. The case $p = 0$ is similarly proved.

4) The proof of 4) is analogous to the proof of 3).

Q.E.D.

Lemma 4.17 Let $\vec{b} \in \{0,1\}^n$ satisfy Claim 4.14.

1) If B is a block in $\vec{b}$, there is a block B' in $\psi(\vec{b})$ such that

$$h(\psi(\vec{b}),B') = h(\vec{b},B) + 2K(\vec{b},B) - 2\alpha(\vec{b}) \quad \text{and} \quad m(\psi(\vec{b}),B') = m(\vec{b},B) .$$

2) If E is an isolated one in $\vec{b}$, there is an isolated one E' in $\psi(\vec{b})$ such that

$$\mathrm{Place}(\psi(\vec{b}),E') = \mathrm{Place}(\vec{b},E) - 1 - 2K(\vec{b},E) - 2\alpha(\vec{b})(\mathrm{mod}(n+1)) .$$

3) The blocks B' and the isolated ones E' will constitute all the blocks and ones in $\psi(\vec{b})$.

Definition 4.18 Let E be an isolated one and B a block in $\vec{b} \in \{0,1\}^n$ where $\vec{b}$ satisfies Claim 4.14. We define $\psi(E) = E'$

and $\psi(B) = B'$ where E' and B' are as in Lemma 4.17.

Proof of Lemma 4.17: $\theta^{n+2}(\vec{b}) = \alpha(A)(10)D$ where D does not start with 10. By Observation 4.7

$\psi(\vec{b}) = D\alpha(A)(01)$ where $\alpha(A)(01) = 01\ldots01$ and $l(\alpha(A)(01)) = 2\alpha(A)$. We divide the proof in 4 cases.

a) B is a block different from B_{END}. By Lemma 4.16 there is a block C in $\theta^{n+2}(\vec{b})$ such that

$$h(\theta^{n+2}(\vec{b}),C) = h(\vec{b},B) + 2K(\vec{b},B) \quad\text{and}\quad m(\theta^{n+2}(\vec{b}),C) = m(\vec{b},B) .$$

This implies that there is a block B' in $\psi(\vec{b}) = \theta^{n+2+2\alpha(\vec{b})}(\vec{b})$ such that

$$h(\psi(\vec{b}),B') = h(\vec{b},B) + 2K(\vec{b},B) - 2\alpha(\vec{b}) \quad\text{and}\quad m(\psi(\vec{b}),B') = m(\vec{b},B) .$$

b) Let $B = B_{END}$. We observe that $\alpha(\vec{b}) = K(\vec{b},B_{END})$. By Lemma 4.16 there is a block C in $\theta^{n+2}(\vec{b})$ such that

(9) $$h(\theta^{n+2}(\vec{b}),C) = n \quad\text{and}\quad m(\theta^{n+2}(\vec{b}),C) = m(\vec{b},C) .$$

We have $\theta^{n+2}(\vec{b}) = \alpha(10)DC$ where D does not start with 10. By Observation 4.7 we have $\psi(\vec{b}) = DC\alpha(01)$.

We have

(10) $$\begin{aligned}&B'_{END} = C\alpha(01) \text{ is a block in } \psi(\vec{b}) \text{ such that}\\ &h(\psi(\vec{b}),B'_{END}) = n = h(\vec{b},B_{END}) + 2K(\vec{b},B_{END}) - 2\alpha(\vec{b}) .\end{aligned}$$

Let x_0 and x_1 be the number of 0's and 1's in C respectively, then by (9)

$$\begin{aligned}m(\psi(\vec{b}),B'_{END}) = (x_1+\alpha(\vec{b})) - (x_0+\alpha(\vec{b})) = x_1 - x_0 &= m(\theta^{n+2}(\vec{b}),C)\\ &= m(\vec{b},B) .\end{aligned}$$

c) Let E be an isolated one which does not follow B_{END}. By Lemma 4.16 there is an isolated one G in $\theta^{n+2}(\vec{b})$ such that

$$\text{Place}(\theta^{n+2}(\vec{b}),G) = \text{Place}(\vec{b},E) - 1 - 2K(\vec{b},E) .$$

We observe easily that there also is an isolated one E' in $\psi(\vec{b}) = \theta^{n+2+2\alpha(\vec{b})}(\vec{b})$ such that

$$\mathrm{Place}(\psi(\vec{b}),E') = \mathrm{Place}(\vec{b},E) - 1 - 2K(\vec{b},E) - 2\alpha(\vec{b}) \ .$$

d) We finally assume that $\alpha(\vec{b}) \neq 0$. If $\alpha(\vec{b}) = 0$, we are finished. We show the lemma for the $\alpha(\vec{b})$ ones in $\vec{b}$ which follows B_{END} . Those isolated ones are in the coordinates

(11) $\quad 2,\dots,2\alpha(\vec{b})$ in $\vec{b}$.

By (10) there are isolated ones in the coordinates

(12) $\quad n-2,\dots,n-2\alpha(\vec{b})$ in B'_{END} .

Let E be one of the isolated ones in (11). $\mathrm{Place}(\vec{b},E) = 2i$ for suitable $i \in \{1,\dots,\alpha(\vec{b})\}$. By (12) there is an isolated one E' in $\psi(\vec{b})$ such that

$$\mathrm{Place}(\psi(\vec{b}),E') = n-2(\alpha(\vec{b})+1-i) = \mathrm{Place}(\vec{b},E) - 3 - 2\alpha(\vec{b}) + (n+1)$$
$$= \mathrm{Place}(\vec{b},E) - 1 - 2K(\vec{b},E) - 2\alpha(\vec{b}) \ (\mathrm{mod}(n+1)) \ .$$

This completes the proof of 1) and 2).

3) We observe that

$$w(\vec{b}) = |\{\text{isolated ones in } \vec{b}\}| + \sum_{B \text{ block in } \vec{b}} m(\vec{b},B) = k+2 \ ,$$

and the same is true for $\psi(\vec{b})$. $|A|$ denotes the number of elements in A . Also

$$|\{E' : E \text{ isolated one in } \vec{b}\}| + \sum_{B \text{ block in } \vec{b}} m(\psi(\vec{b}),B') = k+2 = w(\psi(\vec{b}))$$

Accordingly the isolated ones E' and blocks B' will constitute all the blocks and ones in $\psi(\vec{b})$.

Q.E.D.

Corollary 4.18 If $\vec{b} \in \{0,1\}^n$ satisfies Claim 4.14, $\psi(\vec{b})$ also satisfies Claim 4.14.

Definition 4.19 Let $\vec{b} \in \{0,1\}^n$ satisfy Claim 4.14 and let E and B be an isolated one and a block of B respectively. If $\psi^i(E)$ follows $\psi^i(B)$ in $\psi^i(\vec{b})$, we say that E and B meets at time $i+1$.

$|A|$ denotes the number of elements of A.

Definition 4.10 Let $\vec{b} \in \{0,1\}^n$ satisfy Claim 4.14, and let E and B be an isolated one and a block in $\vec{b}$ respectively.

1) Define the distance between E and B by

$$\mathrm{DIST}_{\vec{b}}(E,B) = \mathrm{Place}(\vec{b},E) - h(\vec{b},B) - 2 \pmod{(n+1)} .$$

2) If E is to the right of B, we define

$$a_{\vec{b}}(E,B) = |\{E' : E' \text{ is an isolated one in } \vec{b} \text{ such that } h(\vec{b},B) < \mathrm{Place}(\vec{b},E') < \mathrm{Place}(\vec{b},E)\}|$$

and

$$b_{\vec{b}}(E,B) = |\{B' : B' \text{ is a block in } \vec{b} \text{ such that } h(\vec{b},B) < h(\vec{b},B') < \mathrm{Place}(\vec{b},E)\}| ,$$

If E is to the left of B, we define

$$a_{\vec{b}}(E,B) = |\{E' : E' \text{ is an isolated one in } \vec{b} \text{ such that } \mathrm{Place}(\vec{b},E') < \mathrm{Place}(\vec{b},E) \text{ or } \mathrm{Place}(\vec{b},E') > h(\vec{b},B)\}|$$

and

$$b_{\vec{b}}(E,B) = |\{B' : B' \text{ is a block in } \vec{b} \text{ such that } h(\vec{b},B') < \mathrm{Place}(\vec{b},E) \text{ or } h(\vec{b},B') > h(\vec{b},B)\}|$$

3) We define the meeting time between E and B by

$$\mathrm{TM}_{\vec{b}}(E,B) = \mathrm{DIST}_{\vec{b}}(E,B) - 2a_{\vec{b}}(E,B) - 2b_{\vec{b}}(E,B) .$$

The following lemma justifies the definition of $\mathrm{TM}_{\vec{b}}(E,B)$.

Lemma 4.21 Let $\vec{b} \in \{0,1\}^n$ satisfy Claim 4.14 , let B be a block, and let E be the first isolated one in a sequence of isolated ones in $\vec{b}$.

Then E and B meet at the time $TM_{\vec{b}}(E,B)$.

Proof: We prove it by induction with respect to $j = DIST_{\vec{b}}(E,B)$. Suppose first $j = 1$. Then we have one of the following two situations, $B = B_{END}$ and $Place(\vec{b},E) = 2$ or $B \neq B_{END}$ and $Place(\vec{b},E) = h(\vec{b},E) + 3$. In both cases $DIST_{\vec{b}}(E,B) = TM_{\vec{b}}(E,B) = 1$. By definition E and B meet at the time 1 . Consequently the basis step is correct.

Suppose the lemma is true for $DIST_{\vec{b}}(E,B) \leq j$ and that $DIST_{\vec{b}}(E,B) = j+1$. We calculate modulo $n+1$ and get

$$DIST_{\psi(\vec{b})}(\psi(E),\psi(B)) = Place(\psi(\vec{b}),\psi(E)) - h(\psi(\vec{b}),\psi(B)) - 2$$
$$= Place(\vec{b},E) - 1 - 2K(\vec{b},E) - 2\alpha(\vec{b}) - h(\vec{b},B) - 2K(\vec{b},B) + 2\alpha(\vec{b}) - 2$$
$$= (Place(\vec{b},E) - h(\vec{b},B) - 2) - 2K(\vec{b},E) - 2K(\vec{b},B) - 1$$
$$= DIST_{\vec{b}}(E,B) - 2K(\vec{b},E) - 2K(\vec{b},B) - 1 \leq j \text{ .}$$

We have

$$a_{\psi(\vec{b})}(\psi(E),\psi(B)) = a_{\vec{b}}(E,B) - K(\vec{b},B)$$

and

$$b_{\psi(\vec{b})}(\psi(E),\psi(B)) = b_{\vec{b}}(E,B) - K(\vec{b},E) \text{ .}$$

By the induction hypothesis $\psi(E)$ and $\psi(B)$ meet at the time

$$TM_{\psi(\vec{b})}(\psi(E),\psi(B)) = DIST_{\vec{b}}(E,B) - 2K(\vec{b},E) - 2K(\vec{b},B) - 1$$
$$- 2(a_{\vec{b}}(E,B) - K(\vec{b},B)) - 2(\vec{b}_{\vec{b}}(E,B) - K(\vec{b},E)) = TM_{\vec{b}}(E,B) - 1 \text{ .}$$

Hence E and B meet at the time $TM_{\vec{b}}(E,B)$.

Q.E.D.

Lemma 4.22 Let $\vec{b} \in \{0,1\}^n$ satisfy Claim 4.14 and $E(\vec{b})$ and $B(\vec{b})$ be the number of isolated ones and the number of blocks in $\vec{b}$ respectively.

Then an isolated one and a block in $\vec{b}$ meet at most once during the time $n+1-2E(\vec{b})-2B(\vec{b})$.

Proof: Suppose F is the first sequence of isolated ones to the right of B . If such a sequence does not exist, let F be the first sequence of isolated ones in $\vec{b}$. We suppose $F =$ $E_1 0 \ldots 0 E_q 0$ and that E_1 and B meet at the time x . We have

$$\psi^x(B) = Q\psi^x(E_1)0\psi^x(E_2)\ldots 0\psi^x(E_q)01 .$$

We calculate modulo $n+1$ and get

$$\mathrm{DIST}_{\psi^x(\vec{b})}(\psi^x(\vec{b}),\psi^x(E_1)) = \mathrm{Place}(\psi^x(\vec{b}),\psi^x(E_1)) - h(\psi^x(\vec{b}),\psi^x(B)) - 2$$

$$= \mathrm{Place}(\psi^x(\vec{b}),\psi^x(E_1)) - (\mathrm{Place}(\psi^x(\vec{b}),\psi^x(E_1)) + 2q) - 2 = -2-2q = n-1-2q$$

and

$$a_{\psi^x(\vec{b})}(\psi^x(\vec{b}),\psi^x(E_1)) = E(\vec{b}) - q$$

and

$$b_{\psi^x(\vec{b})}(\psi^x(\vec{b}),\psi^x(E_1)) = B(\vec{b}) - 1 .$$

By Lemma 4.21 E_1 and B meet at the time

$$\mathrm{TM}_{\psi^x(\vec{b})}(\psi^x(E_1),\psi^x(B)) = \mathrm{DIST}_{\psi^x(\vec{b})}(\psi^x(E_1),\psi^x(B)) - 2(E(\vec{b})-q) - 2(B(\vec{b})-1)$$

$$= n-1-2q-2(E(\vec{b})-q) - 2(B(\vec{b})-1) = n+1-2E(\vec{b}) - 2B(\vec{b}) .$$

Hence E_1 and B meet for the second time at the time $x + n+1 - 2E(\vec{b}) - 2B(\vec{b}) > n+1 - 2E(\vec{b}) - 2B(\vec{b})$.

Q.E.D.

Lemma 4.23 Let $\vec{b} \in \{0,1\}^n$ satisfy Claim 4.14. Suppose F is the first sequence of isolated ones to the left of a block B in $\vec{b}$. If no such sequence exist, we let F be the last sequence of ones in $\vec{b}$.
Suppose $F = E_1 0 \ldots 0 E_p 0$, and $E(\vec{b})$ and $B(\vec{b})$ is the number of isolated ones and blocks in $\vec{b}$ respectively. Then

$$TM_{\vec{b}}(E_1,B) \leq n+1-2E(\vec{b})-2B(\vec{b}) .$$

Proof: We let $q = B(\vec{b}) - b_{\vec{b}}(E,B)$. We make the following observation.

(13) Between two blocks there are at least two 0's. A block occupies at least two places. If B' is a block and E is an isolated one such that $\text{Place}(\vec{b},E) < h(\vec{b},B')$, then $h(\vec{b},B') \geq \text{Place}(\vec{b},E) + 2$.

We do not calculate modulo n+1 this time. First we suppose E_1 is to the left of B. (13) implies

$$h(\vec{b},B) \geq \text{Place}(\vec{b},E_p) + 2(q-1) + 2(q-1) + 2 = \text{Place}(\vec{b},E_1) + 2(p-1) + 4(q-1) + 2 .$$

Hence

$$DIST_{\vec{b}}(E_1,B) = \text{Place}(\vec{b},E_1) - h(\vec{b},B) - 2 + n+1$$

$$\leq \text{Place}(\vec{b},E_1) - \text{Place}(\vec{b},E_1) - 2(p-1) - 4(q-1)-2-2+n+1 = n+1-2(p-1)-4q .$$

This inequality implies (since $q \geq 1$)

$$TM_{\vec{b}}(E,B) \leq n+1-2(p-1)-4q-2(E(\vec{b})-p)-2(B(\vec{b})-q)$$

$$= n+1-2E(\vec{b})-2B(\vec{b})-2(q-1) \leq n+1-2E(\vec{b})-2B(\vec{b}) .$$

Next we suppose E_1 is to right of B. Let q' and q" be the number of blocks B' such that $h(\vec{b},B') \leq h(\vec{b},B)$ and

$h(\vec{b},B') > \mathrm{Place}(\vec{b},E_1)$ respectively. Then $q = q' + q''$ and by (13) we get

$$h(\vec{b},B) \geq 4q' - 2 \quad \text{and} \quad \mathrm{Place}(\vec{b},E_p) \leq n - 4(q''-1) - 1 \ .$$

These inequalities implies that

$$\mathrm{Place}(\vec{b},E_1) \leq n - 4(q''-1) - 1 - 2(p-1)$$

and

$$\mathrm{DIST}_{\vec{b}}(E_1,B) \leq n - 4(q''-1) - 1 - 2(p-1) - 4q' + 2 - 2 = n - 4q - 2p + 5$$

and

$$\mathrm{TM}_{\vec{b}}(E_1,B) \leq n - 4q - 2p + 5 - 2(E(\vec{b})-p) - 2(B(\vec{b})-q)$$
$$= n+1 - 2E(\vec{b}) - 2B(\vec{b}) - 2q + 4 \leq n+1 - 2E(\vec{b}) - 2B(\vec{b})$$

since $q \geq 2$. $q \geq 2$ because $q = q' + q''$, $q' \geq 1$ since $h(\vec{b},B) \leq h(\vec{b},B)$, and $q'' \geq 1$ since $h(\vec{b},B_{END}) > \mathrm{Place}(\vec{b},E_1)$.

As a consequence of the preceeding three lemmas, Lemma 4.24 follows.

Lemma 4.24 Let $\vec{b} \in \{0,1\}^n$ satisfy Claim 4.14 and let $E(\vec{b})$ and $B(\vec{b})$ be the number of isolated ones and blocks in $\vec{b}$ respectively.

Then every one and every block will meet exactly once during the time $n + 1 - 2E(\vec{b}) - 2B(\vec{b})$.

Proof of Theorem 4.4 : By using θ some times on $\vec{b}$ we can suppose that $\vec{b}$ starts with a block B . If $\vec{b} = B$, $\vec{b}$ satisfies Claim 4.14. If $\vec{b} = B0$, $\theta^{-1}(\vec{b})$ satisfies Claim 4.14. Finally we assume $\vec{b} = B00p(10)D$ where D does not start with 10 and $p \geq 0$. D might be empty. We assume $B = 1Q$. By Lemma 4.15.2 and Observation 4.7.

$$\theta^{l(B)+2+2p}(\vec{b}) = D00Q1p(01) ,$$

which satisfies Claim 4.14. Hence we can assume that $\vec{b}$ satisfies Claim 4.14.

Put $T = n+1-2E(\vec{b})-2B(\vec{b})$. If E and B is an isolated one and a block in $\vec{b}$ respectively, Lemma 4.24 implies

$$\sum_{i=o}^{T-1} K(\psi^i(\vec{b}),\psi^i(B)) = E(\vec{b}) \quad \text{and} \quad \sum_{i=o}^{T-1} K(\psi^i(\vec{b}),\psi^i(E)) = B(\vec{b}) .$$

In particular we have

$$\sum_{i=o}^{T-1} \alpha(\psi^i(\vec{b})) = \sum_{i=o}^{T-1} K(\psi^i(\vec{b}),\psi^i(B_{END})) = E(\vec{b}) .$$

Let E be an isolated one and B a block. By calculating modulo $n+1$ we get by Lemma 4.17

$$\begin{aligned}\text{Place}(\psi^T(\vec{b}),\psi^T(E)) &= \text{Place}(\vec{b},E) - \sum_{i=o}^{T-1} (1+2K(\psi^i(\vec{b}),\psi^i(E)) + 2\alpha(\psi^i(\vec{b}))) \\ &= \text{Place}(\vec{b},E) - T - 2B(\vec{b}) - 2E(\vec{b}) = \text{Place}(\vec{b},E) - (n+1) = \text{Place}(\vec{b},E)\end{aligned} \tag{14}$$

and

$$\begin{aligned}h(\psi^T(\vec{b}),\psi^T(B)) &= h(\vec{b},B) + \sum_{i=o}^{T-1} (2K(\psi^i(\vec{b}),\psi^i(B))-2\alpha(\psi^i(\vec{b}))) \\ &= h(\vec{b},B) + 2E(\vec{b}) - 2E(\vec{b}) = h(\vec{b},B)\end{aligned} \tag{15}$$

and

$$m(\psi^T(\vec{b}),\psi^T(B)) = m(\vec{b},B) . \tag{16}$$

(14), (15) and (16) imply $\psi^T(\vec{b}) = \vec{b}$. Thus, we have

$$\psi^T = \prod_{i=o}^{T-1} \theta^{n+2+2\alpha(\psi^i(\vec{b}))} = \theta^{T(n+2)+2E(\vec{b})} ,$$

and $\vec{b}$ is on a cycle of period

$$T(n+2) + 2E(\vec{b}) = 2E(\vec{b}) + (n+1-2E(\vec{b})-2B(\vec{b}))(n+2) .$$

Q.E.D.

Proof of Theorem 4.5 : 1) In this case the shift register will only cycle $\vec{b}$, hence n is a period of $\vec{b}$.

2) If $\vec{c}$ contains only blocks, Lemma 4.3 implies $\theta^{n+2}(\vec{c}) = \vec{c}$.

If $\vec{c}$ contains only isolated ones, we have two cases:

a) $\vec{c}$ contains two succeeding 0's or $\vec{c}$ start with 0 . In this case we can assume $\vec{c}$ start with 0 by using Observation 4.7. By Lemma 4.3 $\theta^{n+2}(\vec{c})$ is obtained from $\vec{c}$ by shifting every isolated one in $\vec{c}$ one coordinate to the left. Hence $\theta^{n+1}(\vec{c}) = \vec{c}$.

b) $\vec{c}$ does not contain two succeeding 0's and $\vec{c}$ does not start with 0 . If n is odd, $\vec{c} = 10 \dots 101$. By Observation 4.7 $\theta^{2}(\vec{c}) = \vec{c}$. 2 divides $n+1$ and we are done. If n is even, $\vec{c} = 1010 \dots 10$. By Observation 4.7 $\theta^{2}(\vec{c}) = 10 \dots 1001$, and we are in the case a). If $E(\vec{c}) > 0$ and $B(\vec{c}) > 0$ the claim follows from Thm.4.4.

3) Suppose $w(\vec{b}) \doteq k+1$. $\vec{b}$ cannot contain two succeeding 0's and $\vec{b}$ cannot start with 0 , because in both these cases there is a $\vec{c}$ on the same cycle as $\vec{b}$ such that $w(\vec{c}) = k+2$.

If $\vec{b} = 1_{a_1}0 \dots 01_{a_s}0$, then $\theta^{-1}(\vec{b}) = 1_{a_1+1}0 \dots 01_{a_s}$ and $w(\theta^{-1}(\vec{b})) = k+2$. Hence $\vec{b}$ must have the form $\vec{b} = 1_{a_1}0 \dots 01_{a_s}$. By Lemma 4.15.1

$$\theta^{n}(\vec{b}) = 01_{a_1}0 \dots 01_{a_s-1} .$$

Hence,

$$\theta^{n+1}(\vec{b}) = 1_{a_1}0 \dots 01_{a_s} = \vec{b} .$$

Q.E.D.

Lemma 4.25 Let $\vec{b} \in \{0,1\}^{n}$ satisfy Claim 4.14 , and suppose $\vec{b} = 0_{a}s(1100)1_{q}p(01)$ where $s(1100) = 1100 \dots 1100$ such that

$l(s(1100)) = 4s$, $a \geq 0$, $q \geq 2$, and $2s+q+p = k+2$. Let $E(\vec{b})$ and $B(\vec{b})$ be the number of isolated ones and blocks in $\vec{b}$ respectively. Then the minimal period of $\vec{b}$ is

$$P = 2p + (n+1-2(s+1)-2p)(n+2) = 2E(\vec{b}) + (n+1-2B(\vec{b})-2E(\vec{b}))(n+2) .$$

Proof: We only give the idea of the proof since it is simple but technical. We use Lemma 4.3 to show that

$$\theta^{l}(\vec{b}) \neq \vec{b} \quad \text{for} \quad l \in \{i(n+2) : 0 < i < n+1-2(s+1)-2p)\} .$$

It is not difficult to show that this is true for all $l \in \{0,\ldots,P-1\}$.

Q.E.D.

Proof of Theorem 4.6 Suppose $\vec{b}$ satisfy Claim 4.14. We observe that a block occupies at least two coordinates, between two blocks there are at least two 0's and that an isolated one is succeeded by a 0. Hence, an isolated one occupies two coordinates. Let $E(\vec{b})$ and $B(\vec{b})$ be the number of isolated ones and blocks in $\vec{b}$ respectively. By the observations we get

(17) $$2B(\vec{b}) + 2(B(\vec{b})-1) + 2E(\vec{b}) \leq n .$$

Since $w(\vec{b}) = k+2$ we have

(18) $$2B(\vec{b}) + E(\vec{b}) \leq k+2 .$$

(17), (18) and Theorem 4. imply $P \in$.

If the cycle containing $\vec{b}$ does not contain a $\vec{c}$ which satisfies Claim 4.14, we have by Theorem 4.5 that P divides one of the numbers n, $n+1$ and $n+2$.

We have now proved the first part of the theorem. By Lemma 4.25

every element in will be the minimal period of some cycle containing a suitable $\vec{b} \in \{0,1\}^n$.

Q.E.D.

References:

[1] Berlekamp, E.R.: Algebraic coding theory, McGraw-Hill, New York, 1968.

[2] Golomb, S.W.: Shift register sequences, Holden Day, San Fransisco, 1967.

[3] Kjeldsen, K.: On the Cycle Structure of a Set of Non Linear Shift Registers with Symmetric Feedback Functions, to appear in J. Comb. Theory, Ser. A.