Abstract.

$E_k(x_2,\ldots,x_n)$ is defined by $E_k(a_2,\ldots,a_n) = 1$ if $\sum_{i=2}^{n} a_i = k$, else $E_k(a_2,\ldots,a_n) = 0$. We determine the periods of the sequences generated by the shift register with the feedback function $x_1 + E_k(x_2,\ldots,x_n) + E_{k+1}(x_2,\ldots,x_n) + E_{k+2}(x_2,\ldots,x_n)$ over the field $GF(2)$. We indicate also how to find the periods when the feedback function is $x_1 + E_k(x_2,\ldots,x_n) + \ldots + E_{k+p}(x_2,\ldots,x_n)$ where $p > 2$.

1. Introduction.

In this paper we study only shift registers over the field $GF(2) = \{0,1\}$ characterized by $1 + 1 = 0 + 0 = 0$ and $1 + 0 = 1$. Let $S(x_2,\dots,x_n)$ be a symmetric polynomial. A symmetric shift register of n stages with feedback function $x_1 + S(x_2,\dots,x_n)$ is the function $\theta : \{0,1\}^n \to \{0,1\}^n$ defined by

$$\theta(x_1,\dots,x_n) = (x_2,\dots,x_n,x_1 + S(x_2,\dots,x_n)) .$$

If $\theta^s(a_1,\dots,a_n) = (a_1,\dots,a_n)$, s is a period of $(a_1,\dots,a_n)$ with respect to θ. These periods are equal to the periods of the sequences $(a_t)_{t=1}^{\infty}$ satisfying the non-linear difference equation

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

For a general treatment of nonlinear shift registers see [1].

We shall in this paper extend the results of Kjeldsen [2] and Søreng [3]. I am grateful to K. Kjeldsen who inspired me to study symmetric shift registers.

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 $k \in \{0,1,\dots,n-1\}$ by

$$E_k(a_2,\dots,a_n) = 1 \quad \text{if} \quad w(a_2,\dots,a_n) = k \text{ , else}$$
$$E_k(a_2,\dots,a_n) = 0 .$$

The polynomials E_k are very important. In [3] we showed that all symmetric polynomials are of the form $\sum_{k \in \Delta} E_k$ for some $\Delta \subset \{2,\dots,n\}$. Besides, if the periods of $E_k + \ldots + E_{k+p}$ for $p \geq 0$ are known, the periods of all symmetric shift registers can be determined.

In this paper we determine the periods when $S = E_k + E_{k+1} + E_{k+2}$. In [3] we determined the periods when $S = E_k$ and $S = E_k + E_{k+1}$. By using Thm. 2.2 in [3] we therefore know the periods of all S of the form $S = \sum_{k \in \Delta} E_k$, where $\Delta \subset \{2,\ldots,n\}$ has the property

$$k,k+1,k+2 \in \Delta \Rightarrow k-1,k+3 \notin \Delta .$$

Besides this paper gives probably all ideas needed to solve the general case $S = E_k + \ldots + E_{k+p}$ for $p > 2$. In Section 4 we will indicate how to treat the general case.

In Section 2 we state the results. In Section 3 and 5 we prove them. Section 3 contains the main lines of the proofs and Section 5 contains the tecnical lemmas which are needed. In section 4 we indicate the general situation by an example.

We denote $\vec{a} = (a_1,\ldots,a_n) \in \{0,1\}^n$ also by $\vec{a} = a_1 \ldots a_n$. We denote finite sequences of numbers by capitol letters (also the empty sequence). For $s \in \{0,1,\ldots\}$ we define $s(A) = A \ldots A$ where A appears s times. We let $1_t = 1 \ldots 1$ (resp. $0_t = 0 \ldots 0$) denotes a string of t consecutive 1's (resp. 0's). We refer to the index of notation in the end of this paper.

2. Main results.

In this section we introduce the concept of blocks and the main results. In the proofs we show how the blocks of a vector $A = a_1 \ldots a_n$ moves by using θ .

Definition 2.1.

Let $A = a_1 \ldots a_n \in \{0,1\}^n$. We put $a_{n+1} = a_{n+2} = a_{n+3} = 0$. hence $a_1 \ldots a_{n+3} = A000$. We define the 3-blocks in A by the following inductive procedure:

Suppose $i=0$ or that the 3-blocks in $a_1 \ldots a_i$ are defined.

Let j be the least number $>i$ such that $a_j \ldots a_{n+3}$ starts with $11s(01)1$ for some $s \geq 0$. If such a j does not exist, we stop the procedure.

Let p be the least number $>j$ such that $a_p \ldots a_{n+3}$ starts with $00s(10)0$ for some $s \geq 0$.

By definition $a_j \ldots a_{p-1}$ is a 3-block in A . We have now defined the 3-blocks in $a_1 \ldots a_{p-1}$, and we continue the procedure.

Definition 2.2.

Let $A = a_1 \ldots a_n \in \{0,1\}^n$. Isolated 1's outside 3-blocks and isolated 0's inside 3-blocks are called 1-blocks.

11 outside 3-blocks and 00 inside 3-blocks are called 2-blocks.

We illustrate the definitions by two examples. We put one $*$ above the 1-blocks, one line above the 2-blocks and one line below the 3-blocks.

(2.1) $\quad 0\,\overline{11}0\overset{*}{1}001\underline{11\overset{*}{0}11\overset{*}{0}1\overset{*}{0}11}000\overset{*}{1}00\overline{11}000\underline{111}0$.

(2.2) $\quad \overline{1\;1}0\overset{*}{1}0\overset{*}{1}000\overline{11}000\underline{111}00\overset{*}{1}00\underline{111\overline{00}11}00\overset{*}{1}$.

The next theorem is the main result of this paper.

Theorem 2.3.

Suppose n and k are positive integers such that $0 \leq k \leq n-3$. Suppose $\theta : \{0,1\}^n \to \{0,1\}^n$ is defined by

$$\theta(x_1,\dots,x_n) = (x_2,\dots,x_n,x_{n+1}) \quad \text{where}$$
$$x_{n+1} = x_1 + E_k(x_2,\dots,x_n) + E_{k+1}(x_2,\dots,x_n) + E_{k+2}(x_2,\dots,x_n) \ .$$

We suppose $A = a_1 \dots a_n$ is such that $w(A) = k+3$ and A contains both 1- , 2- and 3-blocks.

We let γ_i be equal to the number of i-blocks in A for $i = 1,2,3$. We let a and b be the minimal positive integers such that

$$a(2n+4-4\gamma_1-6\gamma_2-8\gamma_3) = b(n+1-2\gamma_1-2\gamma_2-2\gamma_3) \ . \tag{2.3}$$

Then p defined by

$$p = a(n+2-2\gamma_2-4\gamma_2-4\gamma_3)(n+3)+4a\gamma_2+2b\gamma_1$$

is a period for A . That means $\theta^p(A) = A$.

The next theorem treats the situation that $A = a_1 \dots a_n$ does not contain 3 different types of blocks.

Theorem 2.4.

θ is defined as in Thm. 2.3. We suppose $A = a_1 \dots a_n$ satisfies $w(A) = k+3$. We let γ_i be equal to the number of i-blocks of A for $i = 1,2,3$.

a) A contains only 1- and 2-blocks. Then the following is a period

$$(n+1-2\gamma_1-2\gamma_2)(n+2)+2\gamma_1 \ .$$

b) A contains only 1- and 3-blocks. Then the following is a period

$$(n+1-2\gamma_1-2\gamma_3)(n+3)+4\gamma_1 .$$

c) A contains only 2- and 3-blocks. Then the following is a period

$$(n+2-4\gamma_2-4\gamma_3)(n+3)+4\gamma_2 .$$

d) If A contains only i-blocks, n+i is a period for $i = 1,2,3$.

We do not prove Thm. 2.4. It can be proved by using the distance functions defined in Def. 3.13 and the same ideas as in the proof of Lemma 3.15. Besides, the proof is similar to the proof of Thm. 4.4 in [3].

If $w(A) \in \{k,k+1,k+2,k+3\}$, there exist in almost all cases an integer q such that $w(\theta^q(A)) = k+3$. Then we use Thm. 2.3 or Thm. 2.4 to find a period of $\theta^q(A)$. If $w(A) < k$ or $w(A) > k+3$, we prove easily that $\theta^n(A) = A$.

Now we illustrate by three examples how Thm. 2.3 is used.

Let $n = 12$, $k = 3$ and $A = 000000101100$. We use Thm. 2.3 on $\theta^3(A) = 000101100111$. Since $\gamma_1 = \gamma_2 = \gamma_3 = 1$, (2.3) implies $10a = 7b$. We get $a=7$, $b=10$ and the period equal to

$$7\cdot(12+2-2-4-4)\cdot 15+4\cdot 7+2\cdot 10 = 468 .$$

The example (2.1) satisfies the hypothesis of the theorem with $k = 13$. In this example $n = 32$, $\gamma_1 = 5$,

$\gamma_2 = 2$ and $\gamma_3 = 2$. (2.3) implies $20a = 15b$. We get $a = 3$, $b = 4$ and the period equal to 904 .

The example (2.2) satisfies the hypothesis of the theorem with $k = 13$. In this example $n = 32$, $\gamma_1 = 4$, $\gamma_2 = 3$ and $\gamma_3 = 2$. (2.3) implies $18a = 15b$. We get $a = 5$, $b = 6$ and the period equal to 1158 .

Corollary 2.5.

θ is as in Thm. 2.3. We suppose $A = a_1 \dots a_n$ satisfies $w(A) = k+3$.

Then the minimal period of A with respect to θ is less than n^3 .

We prove Cor. 2.5 in the end of Section 5.

Quite often the periods we find in Thm. 2.3 and Thm. 2.4 are the minimal periods. However, we have not found any good hyphothesis which implies minimality. By studying the proofs we think it is possible to find such a hypothesis. The next corollary is a simple example.

Corollary 2.6.

θ is as in Thm. 2.3. We suppose $A = a_1 \dots a_n$ satisfies $w(A) = k+3$, and A contains 1 i-block for $i = 1,2,3$.

Then the period we find in Thm. 2.3 is the minimal period of A .

We prove Cor. 2.6 in the end of Section 5.

3. Main lines of the proofs.

In this section we prove Thm. 2.3. The proofs of the lemmas in this section are done in Section 5. We suppose

n and k are positive integers such that $k \leq n - 3$. The proof of Thm. 2.3 is easier if we suppose $A = a_1 \dots a_n$ satisfies the next condition.

Condition 3.1.

Let $A = a_1 \dots a_n \in \{0,1\}^n$. A satisfies Condition 3.1. if

1) $w(A) = k+3$

2) A contains 1-, 2- and 3-blocks.

3) A does not start with a 1-block or a 2-block.

4) A ends with a 3-block.

Lemma 3.2.

If $A = a_1 \dots a_n$ satisfies 1) and 2) in Cond. 3.1, there exists an integer q such that $\theta^q(A)$ satisfies Cond. 3.1.

Later in this section we define an integer $k(A)$ which is dependent of A. If A satisfies Cond. 3.1, we prove that $\theta^{n+3+k(A)}(A)$ satisfies Cond. 3.1. In the proof of Thm. 2.3 we regard $A_0 = A$, $A_1 = \theta^{n+3+k(A)}(A)$, $A_2 = \theta^{n+3+k(A_1)}(A_1)$, etc. At last we find an integer s such that $A = A_{s+1}$. Then the following is a period for A:

$$\sum_{i=0}^{s} n+3+k(A_i) = (s+1)(n+3) + \sum_{i=0}^{s} k(A_i) .$$

We calculate s and $\sum_{i=0}^{s} k(A_i)$ and get the wanted period.

The idea of the proof is to examine the blocks of $\theta^{n+3+k(A)}(A)$ when we know the blocks of A. Usually an i-block moves $k(A)+3-i$ places to the left by applying $\theta^{n+3+k(A)}$ on A . Because the blocks move with different velocities, they will meet sometimes. Therefore we must examine what happens when the blocks meet. In addition we must examine what happens when 1-blocks and 2-blocks inside a 3-block reach the left endpoint of the 3-block. We must also examine what happens when a block reaches the first place in A . In that case the block cannot move to the left. Besides, we will prove that a 3-block does not change size by applying $\theta^{n+3+k(A)}$ on A . As a measure of the size of a 3-block B we will define the mass $m(B)$ of B .

First we study how the blocks move by applying θ^{n+2} . Before we formulate the next lemma we need some definitions.

Definition 3.3.

Let $A = a_1 \dots a_n$ and $B = a_s \dots a_t$ be a piece of A . We define the left endpoint of B by $l(B) = l(A,B) = s$ and the right endpoint of B by $r(B) = r(A,B) = t$.

Definition 3.4.

Let B be a 3-block. We define the mass of B by

$m(B) =$ (the number of 1's in B) - (the number of 0's in B) .

Definition 3.5.

a) Let B_3 be a 3-block in A . Suppose A is of the form

$$A = CB_3 00s(10)0C_1 \dots C_pD$$

where $s \geq 0$, and $C_i = 10$ or $C_i = 11t(01)00$ for some $t \geq 0$.

By definition the 1- and 2-blocks in $00s(10)0C_1 \ldots C_p$ meet B_3 by applying θ^{n+2} .

b) Let B_3 be a 3-block. We suppose B_3 is of the form

$$B_3 = 11s(01)1C_1 \ldots C_pD$$

where $s \geq 0$, and $C_i = 01$ or $C_i = 00t(10)11$ for some $t \geq 0$.

By definition the 1- and 2-blocks in $11s(01)1C_1 \ldots C_p$ jump out of B_3 by applying θ^{n+2} .

c) Suppose B_2 is a 2-block in A which does not meet or jump out of a 3-block by applying θ^{n+2} . Suppose $r(A,B_2) = s$. If there are 1-blocks on the places $s+2, s+4, \ldots, s+2t$, we say that these 1-blocks meet B_2 .

Lemma 3.6.

Suppose A satisfies Cond. 3.1, and let $A^*=\theta^{n+2}(A)1 \in \{0,1\}^{n+1}$.

a) Suppose B_1 is a 1-block in A . Then there exists a 1-block $B_1{}^*$ in A^* such that

$$r(A^*,B_1{}^*) = r(A,B_1)-1-y-2z$$

where $y = 1$ if B_1 meets or jumps out of a 3-block by applying θ^{n+2}, $y = 0$ otherwise, and $z = 1$ if B_1 meets a 2-block by applying θ^{n+2}, $z = 0$ otherwise.

b) Suppose B_2 is a 2-block in A . Then there exists a 2-block $B_2{}^*$ in A^* such that

$$r(A^*,B_2{}^*) = r(A,B_2)-2y+2z$$

where $y = 1$ if B_2 meets or jumps out of a 3-block by applying

θ^{n+2} , $y = 0$ otherwise, and z is equal to the number of 1-blocks which meet B_2 by applying θ^{n+2} .

c) Suppose B_3 is a 3-block in A . Then there exists a 3-block $B_3{}^*$ in A^* such that

$$r(A^*,B_3{}^*) = r(A,B_3)+1+2\beta_1+4\beta_2$$

where β_i = the number of i-blocks which meet B_3 by applying θ^{n+2} .

$$l(A^*,B_3{}^*) = l(A,B_3) +1+2\beta_1+4\beta_2$$

where β_i = the number of i-blocks which jump out of B_3 by applying θ^{n+2} . Besides $m(B_3{}^*) = m(B_3)$.

d) $w(A^*) = k+3$. All the blocks in A^* arise from one of the blocks in A as in a), b) and c).

e) A^* is of the form

$$A^* = s(10)0C_1 \ldots C_pD$$

where $s \geq 0$, $C_i = 10$ or $C_i = 11t(01)00$ for some $t \geq 0$, and D starts with 0 or a 3-block.

Definition 3.7

Let A and $A^* = \theta^{n+2}(A)1$ be as in the previous lemma. Suppose $A^* = s(10)0C_1 \ldots C_pD$ is as in Lemma 3.6.e.

a) We define $k(A) = r(A^*,C_p)-1$.

b) We define $\varphi(A) = \theta^{n+3+k(A)}(A)$.

c) By definition the 1-blocks and 2-blocks in A , which correspond to blocks in $s(10)0C_1 \ldots C_p$, circle around by applying φ , and meet $\hat{B}_3$ by applying φ , where $\hat{B}_3$ is the last 3-block in A .

We observe that $k(A) = 2y_1 + 4y_2$ where y_i = the number of i-blocks which circle around by applying φ. Besides, $k(A)$ is the least integer s such that $\theta^{n+3+s}(A)$ satisfies Cond. 3.1.

The next definitions and lemma describe what happens to the blocks in A when we apply $\varphi = \theta^{n+3+k(A)}$ in case A satisfies Cond. 3.1.

Definition 3.8.

Suppose $A = a_1 \dots a_n$ satisfies Cond. 3.1, and let $\varphi = \theta^{n+3+k(A)}$.

If two blocks in A meet by applying θ^{n+2}, we also say that the two blocks meet by applying φ.

If a 1-block or a 2-block B jumps out of a 3-block by applying θ^{n+2}, we say that B jumps out by applying φ.

Before the lemma we must define precisely the concept that a block moves (to the left). We calculate modulo n, therefore place 0 = place n, place (-1) = place $(n-1)$, etc.

Definition 3.9.

Suppose $A = a_1 \dots a_n$ satisfies Cond. 3.1, and B is an i-block in $A(i=1,2,3)$.

Then B moves q places (to the left) by applying φ means: There exists an i-block B^{**} in $\varphi(A)$ such that

$$r(\varphi(A),B^{**}) = r(A,B) - q \pmod{n}.$$

Lemma 3.10.

Suppose $A = a_1 \dots a_n$ satisfies Cond. 3.1.

a) Let B_1 be a 1-block in A. As the main rule B_1 moves $k(A)+2$ places by applying φ. In addition we have:

If B_1 meets a 3-block, it moves 1 place extra.

If B_1 jumps out of a 3-block, it moves 1 place extra.

If B_1 meets a 2-block, it moves 2 places extra.

If B_1 circles around, it moves -1 place extra.

b) Let B_2 be a 2-block in A. As a main rule B_2 moves $k(A)+1$ places by applying φ. In addition we have:

If B_2 meets a 3-block, it moves 2 places extra.

If B_2 jumps out of a 3-block, it moves 2 places extra.

B_2 moves -2 places for each 1-block which meets B_2 by applying φ.

If B_2 circle around, it moves -2 places extra.

c) Let B_3 be a 3-block in A. As a main rule B_3 moves $k(A)$ places by applying φ. In addition we have:

B_3 moves -4 places for each 2-block which meets B_3 by applying φ.

B_3 moves -2 places for each 1-block which meets B_3 by applying φ.

d) Again let B_3 be a 3-block in A. B_3 corresponds to a 3-block B_3^{**} in $\varphi(A)$ as in c). Then

$$l(\varphi(A),B^{**}) = l(A,B) - k(A) + 2y_1 + 4y_2$$

where y_i = the number of i-blocks which jump out of B_3 by applying φ.

Definition 3.11.

Suppose A satisfies Cond. 3.1. By lemma 3.10 a block

B in A corresponds to a block B** in $\varphi(A)$. We denote B** by $\varphi(B)$.

Lemma 3.12.

Suppose A satisfies Cond. 3.1. Then $\varphi(A)$ satisfies Cond. 3.1, and all blocks in $\varphi(A)$ are equal to $\varphi(B)$ for some block B in A .

If B_3 is a 3-block in A , then $m(B_3) = m(\varphi(B_3))$.

We illustrate lemma 3.10 by seven examples. We put an asterisk above the 1-blocks, a line above the 2-blocks, and a line below the 3-blocks.

Example 1. $(k=10, k(A)=0)$ $\quad A = 000\overset{*}{1}0\overline{11}00\underline{1111\overline{00}111\overset{*}{0}111}$

$$\varphi(A) = \theta^{n+3}(A) = 0\overset{*}{1}00\overline{11}000\underline{111\overline{00}11\overset{*}{0}11111}.$$

Example 2. $(k=7, k(A)=0)$ $\quad A = 00\overline{11}0\overset{*}{1}000\underline{1111\overline{00}1\overset{*}{0}11}$

$$\varphi(A) = \theta^{n+3}(A) = 0\overset{*}{1}0\overline{11}0000\underline{111\overset{*}{0}1\overline{00}111} .$$

Example 3. $(k=8, k(A)=0)$ $\quad A = \underline{111}00\overset{*}{1}00\underline{111}000\overset{*}{1}0\underline{111}$

$$\varphi(A) = \theta^{n+3}(A) = \underline{11\overset{*}{0}11}000\underline{111\overset{*}{0}1}000\underline{111} .$$

Example 4. $(k=5, k(A)=0)$ $\quad A = 00\underline{111}000\overline{11}000\underline{111}$

$$\varphi(A) = \theta^{n+3}(A) = 00\underline{111\overline{00}11}0000\underline{111} .$$

Example 5. $(k=7, k(A)=0)$ $\quad A = 00\underline{111\overset{*}{0}11}000\underline{111\overline{00}11}$

$$\varphi(A) = \theta^{n+3}(A) = 00\overset{*}{1}00\underline{111}000\overline{11}00\underline{111} .$$

Example 6. $(k=1, k(A)=2)$ $\quad A = 00\overset{*}{1}00000\underline{111}$

$$\theta^{n+2}(A)1 = 0\overset{*}{1}0000000\underline{111}$$

$$\varphi(A) = \theta^{n+3+k(A)}(A) = 000000\underline{111\overset{*}{0}1} .$$

Example 7. $(k=2, k(A)=4)$

$$\begin{aligned}
A &= 0\overline{11}00000\underline{111} \\
\theta^{n+2}(A)1 &= 0\overline{11}000000\,\underline{111} \\
\varphi(A) = \theta^{n+3+k(A)}(A) &= 0000\underline{111\overline{00}11} \ .
\end{aligned}$$

We also illustrate the proof of Thm. 2.3 by an example with $k=3$.

$$\begin{aligned}
A &= 00\overline{11}0\overset{*}{1}0000\underline{111} \\
\varphi(A) &= 0\overset{*}{1}0\overline{11}00000\underline{111} = \theta^{n+3}(A) \\
\theta^{n+2}(\varphi(A))1 &= 10011000000111 \\
\varphi^2(A) &= 0000\underline{11\overset{*}{0}11\overline{00}11} = \theta^{2(n+3)+6}(A) \\
\varphi^3(A) &= 000\overset{*}{1}00\overline{11}00\underline{111} = \theta^{3(n+3)+6}(A) \\
\varphi^4(A) &= 0\overset{*}{1}000\overline{11}000\underline{111} = \theta^{4(n+3)+6}(A) \\
\theta^{n+2}(\varphi^4(A))1 &= 10000110000111 \\
\varphi^5(A) &= 00\overline{11}0000\underline{11\overset{*}{0}11} = \theta^{5(n+3)+8}(A) \\
\varphi^6(A) &= 0\overline{11}0000\overset{*}{1}00\underline{111} = \theta^{6(n+3)+8}(A) \\
\theta^{n+2}(\varphi^6(A))1 &= 01100010000111 \\
\varphi^7(A) &= 0\overset{*}{1}0000\underline{111\overline{00}11} = \theta^{7(n+3)+12}(A) \\
\theta^{n+2}(\varphi^7(A))1 &= 10000001100111 \\
\varphi^8(A) &= 0000\overline{11}00\underline{11\overset{*}{0}11} = \theta^{8(n+3)+14}(A) \\
\varphi^9(A) &= 000\overline{11}00\overset{*}{1}00\underline{111} = \theta^{9(n+3)+14}(A) \\
\varphi^{10}(A) &= 00\overline{11}0\overset{*}{1}0000\underline{111} = \theta^{10(n+3)+14}(A) \ .
\end{aligned}$$

Putting $n=13$ and $\gamma_1 = \gamma_2 = \gamma_3 = 1$ in (2.3) we get $12a = 8b$, and hence $a=2$ and $b=3$. By Thm. 2.3 the period is

$$2(13+2-2-4-4)(n+3)+4\cdot 2+2\cdot 3 = 10(n+3)+14$$

This is in accordance with the calculations in the example.

Part 1 of the proof of Thm. 2.3:

We prove in this first part the existence of two integers a and b satisfying (2.3) such that

$$a(n+2-2\gamma_1-4\gamma_2-4\gamma_3)(n+3) + 4a\gamma_2 + 2b\gamma_1$$

is a period.

In the second part we prove that a and b can be chosen minimal.

Because of Lemma 3.2 we can suppose that A satisfies Cond. 3.1.

We consider $A, \varphi(A), \varphi^2(A), \ldots$. There clearly exist integers $s_1 < s_2$ such that $\varphi^{s_1}(A) = \varphi^{s_2}(A)$. Putting $s = s_2 - s_1$, we get $\varphi^s(A) = A$.

We suppose A contains the blocks $E_1, \ldots, E_x$, numbered from left to right, that is $r(A,E_i) < r(A,E_{i+1})$ for $i = 1,\ldots,x-1$.

Consider $A = \varphi^s(A) = \varphi^{2s}(A) = \ldots$. Because of the finiteness there exist $p < q$ such that

$$r(\varphi^{ps}(A),\varphi^{ps}(E_i)) = r(\varphi^{qs}(A),\varphi^{qs}(E_i)) \quad \text{for} \quad i=1,\ldots,x .$$

Putting $t = qs-ps$, we get

$$r(\varphi^t(A),\varphi^t(E_i)) = r(A,E_i) \quad \text{for} \quad i=1,\ldots,x .$$

This means that every 1-block (2-block) circles exactly the same number of times around by applying φ^t . Let b (a) be the number of times every 1-block (2-block) circles around by applying φ^t . By Lemma 3.10 the 3-block do not circle around at all. Therefore we get that every 1-block, 2-block and 3-block moves respectively nb, na and 0 places by applying φ^t.

Using Lemma 3.10 we get by applying φ^t:

Each 1-blocks B_1 moves (the number of places)

$\sum_{i=0}^{t-1}(2+k(\varphi^i(A))$ (the main rule)

$+ b\gamma_3$ (B_1 meets every 3-block b times)

$+ b\gamma_3$ (B_1 jumps out of every 3-block b times)

$+ 2(b-a)\gamma_2$ (B_1 meets every 2-block $(b-a)$ times)

$- b$ (B_1 moves -1 place every time B_1 circles around).

Hence,

$$(3.1) \qquad nb = 2t + \sum_{i=0}^{t-1} k(\varphi^i(A)) + 2b\gamma_3 + 2(b-a)\gamma_2 - b .$$

Each 2-block B_2 moves (the number of places)

$\sum_{i=0}^{t-1}(1+k(\varphi^i(A))$ (the main rule)

$+ 2a\gamma_3$ (B_2 meets every 3-block a times)

$+ 2a\gamma_3$ (B_2 jumps out of every 3-block a times)

$- 2(b-a)\gamma_2$ (B_2 meets every 1-block $(b-a)$ times)

$- 2a$ (B_2 moves -2 places every time B_2 circles around).

Hence,

(3.2) $$na = t + \sum_{i=0}^{t-1} k(\varphi^i(A)) + 4a\gamma_3 - 2(b-a)\gamma_1 - 2a \ .$$

Each 3-block B_3 moves (the number of places)

$\sum_{i=0}^{t-1} k(\varphi^i(A))$ (the main rule)

$-2b\gamma_1$ (B_3 meets every 1-block b times)

$-4a\gamma_2$ (B_3 meets every 2-block a times) .

Hence,

$$0 = \sum_{i=0}^{t-1} k(\varphi^i(A)) - 2b\gamma_1 - 4a\gamma_2 \ .$$

Hence,

(3.3) $$\sum_{i=0}^{t-1} k(\varphi^i(A)) = 2b\gamma_1 + 4a\gamma_2 \ .$$

(This follows also from the definition of $k(\varphi^i(A))$, which implies that $k(\varphi^i(A)) = 2y_1 + 4y_2$ where y_j = the number of j-blocks in $\varphi^i(A)$ circling around by applying φ .)

(3.1) and (3.3) imply

$$nb = 2t + 2b\gamma_1 + 4a\gamma_2 + 2b\gamma_3 + 2b\gamma_2 - 2a\gamma_2 - b \ .$$

Hence

(3.4) $$2t = b(n+1 - 2\gamma_1 - 2\gamma_2 - 2\gamma_3) - 2a\gamma_2 \ .$$

(3.2) and 3.3) imply

$$na = t + 2b\gamma_1 + 4a\gamma_2 + 4a\gamma_3 - 2b\gamma_1 + 2a\gamma_1 - 2a \ .$$

Hence

(3.5) $\quad t = a(n+2 - 2\gamma_1 - 4\gamma_2 - 4\gamma_3)$.

(3.4) and (3.5) imply (2.3):

$$b(n+1 - 2\gamma_1 - 2\gamma_2 - 2\gamma_3) = a(2n+4 - 4\gamma_1 - 6\gamma_2 - 8\gamma_3) .$$

$\varphi(\varphi^i(A)) = \theta^{n+3+k(\varphi^i(A))}(\varphi^i(A))$. Hence φ^t is equal to θ applied

$$\sum_{i=0}^{t-1}(n+3+k(\varphi^i(A))) = t(n+3) + \sum_{i=0}^{t-1} k(\varphi^i(A)) \quad \text{times.}$$

(3.3) and (3.5) imply that φ^t is equal to θ applied

$$t(n+3) + 2b\gamma_1 + 4a\gamma_2 = a(n+2-2\gamma_1-4\gamma_2-4\gamma_3)(n+3) + 2b\gamma_1 + 2a\gamma_2 \text{ times}$$

which is a period for A . The proof of the first part is complete.

The main concept of the second part of the proof is the defintions of distances between blocks. We calculate modulo n . We write card $\mathfrak{M}$ to denote the number of elements in $\mathfrak{M}$ where $\mathfrak{M}$ is a set.

Definition 3.13.

Suppose B and C are two blocks in $A = a_1 \dots a_n$. If B is to the left of C , we define

$$\mathfrak{M}(B,C) = \mathfrak{M} = \{a_{r(c)+1},\dots,a_n\} \cup \{a_1,\dots,a_{r(B)-1}\} \text{ and}$$

$$z(B,C) = z = 1 \text{ , else}$$

$$\mathfrak{M}(B,C) = \mathfrak{M} = \{a_{r(C)+1},\dots,a_{r(B)-1}\} \text{ and } z(B,C) = z = 0 .$$

If $a_i \in \mathfrak{M}$, we say that a_i is between B and C .

If B is a 1-block we define

$$\chi(B,C) = \chi = 2\cdot(\text{the number of 1-blocks between } B \text{ and } C)$$
$$+ 2\cdot(\text{the number of 2-blocks between } B \text{ and } C)$$
$$+ (\text{the number of endpoints } a_i \text{ between } B \text{ and } C, \text{ of 3-blocks}) - z \,.$$

If B is a 2-block or 3-block we define

$$\chi(B,C) = \chi = 2\cdot(\text{the number of 1-blocks between } B \text{ and } C)$$
$$+ 4\cdot(\text{the number of 2-blocks between } B \text{ and } C)$$
$$+ 2\cdot(\text{the number of endpoints } a_i \text{ between } B \text{ and } C, \text{ of 3-blocks}) - 2z$$

We define $d(B,C) = \operatorname{card} \mathfrak{m} - \chi$.

Before proving the second part of Thm. 2.3 we need 5 lemmas concerning distances between blocks.

Lemma 3.14.

Suppose A satisfies Cond. 3.1. and contains γ_i i-blocks for $i=1,2,3$. Suppose further that B_i and C_i are i-blocks in A, and $\hat{B}_3$ is the last 3-block in A.

a) If B_1 and B_2 meet by applying φ, we have $d(B_1,B_2) = 1$ and $d(\varphi(B_1),\varphi(B_2)) = n+1 - 2\gamma_1-2\gamma_2-2\gamma_3$, otherwise

$$d(\varphi(B_1),\varphi(B_2)) = d(B_1,B_2) - 1 + z$$

where $z=1$ if B_2 jumps out of a 3-block or meet a 3-block $\neq \hat{B}_3$ by applying φ .

b) B_2 and B_3 meet by applying φ if and only if $d(B_2,B_3) = 4$. In this case

$$d(\varphi(B_2),\varphi(B_3)) = n+5 - 2\gamma_1-4\gamma_2-4\gamma_3 \,,$$

otherwise

$$d(\varphi(B_2),\varphi(B_3)) = d(B_2,B_3) - 1 \ .$$

c) $d(\varphi(B_1),\varphi(C_1)) = d(B_1,C_1)$.

d) $d(\varphi(B_2),\varphi(C_2)) = d(B_2,C_2)$.

e) $d(\varphi(B_3),\varphi(C_3)) = d(B_3,C_3)$.

Lemma 3.15.

We suppose A satisfies Cond. 3.1, and B_i is an i-block for $i=1,2$. If t is a multiple of $n+2 - 2\gamma_1-4\gamma_2-4\gamma_3$ and $d(\varphi^t(B_1),\varphi^t(B_2)) = d(B_1,B_2)$, then $\varphi^t(A) = A$.

Lemma 3.16.

We suppose A satisfies Cond. 3.1, and B_i is an i-block in A for $i=1,2$. Moreover, we suppose that r and s are multiples of $n+2 - 2\gamma_1-4\gamma_2-4\gamma_3$.

If B_1 and B_2 meet $< c$ times by applying φ^t on $\varphi^r(A)$, then B_1 and B_2 meet $\leqq c$ times by applying φ^t on $\varphi^s(A)$.

Lemma 3.17.

Suppose A satisfies the hyphotesis of Thm. 2.3, and let $s= n+2 - 4\gamma_1-4\gamma_2-2\gamma_3$. Moreover, B_i is an i-block for $i=2,3$.

Then B_2 meets B_3 once, and jumps out of B_3 once, by applying φ^s on A .

Lemma 3.18.

We suppose A satisfies Cond. 3.1, and that each 1-block B_1 meets each 2-block c times, and each 2-block B_2 meets each 3-block B_3 a times by applying φ^s . We also suppose

$\varphi^s(A) = A$.

Then each 1-block B_1 circles around $c+a$ times by applying φ^s .

Part 2 of the proof of Thm. 2.4:

We suppose A satisfies Cond. 3.1, and that a,b are the minimal numbers which satisfies (2.3).

From the first part of the proof where exist integers a',b' which satisfies (2.3), and if $t = a'(n+2-2\gamma_1-4\gamma_2-4\gamma_3)$ (See (3.5)), then $\varphi^t(A) = A$. Moreover, each 1-block meets each 2-block in A $c' = b' - a'$ times by applying φ^t .

There exists a $q > 0$ such that $a' = aq$ and $b' = bq$. We define

$$t_i = ai(n+2 - 2\gamma_1-4\gamma_2-4\gamma_2) \quad \text{for } i=1,\dots,q .$$

Hence,

(3.6) $\varphi^{tq}(A) = A$.

(3.7) Each 1-block meets each 2-block $qc = qb - qa$ times by applying φ^{tq} on A .

We prove

(3.8) Each 1-block meets each 2-block $c=b-a$ times by applying φ^{t_1} on A .

Suppose (3.8) is not true. By (3.7) there exist a 1-block B_1, a 2-block B_2 and $i,j \in \{0,\dots,q-1\}$ such that $\varphi^{ti}(B_1)$ meets $\varphi^{ti}(B_2) < c$ times by applying φ^{t_1} , and $\varphi^{tj}(B_1)$ meets $\varphi^{tj}(B_2) > c$ times by applying φ^{t_1} . Lemma

3.16 with $t = t_1$ gives a contradiction.

Next we show that $d(B_1,B_2) = d(\varphi^{t_1}(B_1),\varphi^{t_1}(B_2))$ where B_i is an i-block. Lemma 3.17 implies

(3.9) Each 2-block meets each 3-block a times and jumps out of each 3-block a times by applying φ^{t_1} on A.

Let $\Omega = \{0,\dots,t_1-1\}$. Then (3.9) and Lemma 3.14.a) imply

(3.10) There exist $(\gamma_3-1)a+\gamma_3 a$ numbers $i \in \Omega$ such that $d(\varphi^{i+1}(B_1),\varphi^{i+1}(B_2)) = d(\varphi^{i}(B_1),\varphi^{i}(B_2))$.

(3.8) and Lemma 3.14a) imply

(3.11) There exist $c=b-a$ numbers $i \in \Omega$ such that $d(\varphi^{i}(B_1),\varphi^{i}(B_2)) = 1$ and $d(\varphi^{i+1}(B_1),\varphi^{i+1}(B_2)) = n+1-2\gamma_1-2\gamma_2-2\gamma_3$. In this case $\varphi^{i}(B_1)$ meets $\varphi^{i}(B_2)$ by applying φ.

(3.10), (3.11) and Lemma 3.14a) imply

(3.12) There exist $t_1-c-2\gamma_3 a+a$ numbers $i \in \Omega$ such that $d(\varphi^{i+1}(B_1),\varphi^{i+1}(B_2)) = d(\varphi^{i}(B_1),\varphi^{i}(B_2))-1$.

By (3.11) $d(\varphi^{i}(B_1),\varphi^{i}(B_2))$ changes first from $d(B_1,B_2)$ to 1, then $(c-1)$ times from $n+1-2\gamma_1-2\gamma_2-2\gamma_3$ to 1, and finally from $n+1-2\gamma-2\gamma_2-2\gamma_3$ to $d(\varphi^{t_1}(B_1),\varphi^{t_1}(B_2))$.
Hence by (3.12)

$$\begin{aligned} t_1-c-2\gamma_3 a+a = {} & (d(B_1,B_2)-1)+(c-1)(n+1-2\gamma_1-2\gamma_2-2\gamma_3-1) \\ & + (n+1-2\gamma_1-2\gamma_2-2\gamma_3-d(\varphi^{t_1}(B_2),\varphi^{t_1}(B_2))) . \end{aligned}$$

Since $t_1 = a(n+2-2\gamma_1-4\gamma_2-4\gamma_3)$ and $c=b-a$, we get

$$d(B_1,B_2)-d(\varphi^{t_1}(B_1),\varphi^{t_1}(B_2)) = a(n+3-2\gamma_1-4\gamma_2-6\gamma_3)-(b-a)$$
$$-(b-a)(n-2\gamma_1-2\gamma_2-2\gamma_3)$$
$$= a(2n+4-4\gamma_1-6\gamma_2-8\gamma_3) - b(n+1-2\gamma_1-2\gamma_2-2\gamma_3) = 0$$

by (2.3). Hence,

$$d(B_1,B_2) = d(\varphi^{t_1}(B_1),\varphi^{t_2}(B_2)) \; . \tag{3.13}$$

(3.13) and Lemma 3.15 imply that $A = \varphi^{t_1}(A)$. By Lemma 3.18 each 1-block circles around $b=a+c$ times by applying φ^{t_1} . Besides, each 2-block circles around a times by applying φ^{t_1} . Hence,

$$\sum_{i=0}^{t_1-1} k(\varphi^i(A)) = 2b\gamma_1+4a\gamma_2$$

As in the end of the first part of the proof we get that $a(n+2-2\gamma_1-4\gamma_2-4\gamma_3)(n+3)+2b\gamma_1+4a\gamma_2$ is a period. The proof is complete.

Proof of Cor. 2.5.:

In the case that A contains only two different types of blocks, the proof is easy by using Thm. 2.4.

Suppose A contains 3 different types of blocks, therefore $n \geq 9$. We suppose that a,b are the minimal positive integers which satisfy (2.3). We have

$$a \leq n+1 - 2\gamma_1-2\gamma_2-2\gamma_3 \leq n-5$$

and

$$b \leq 2n+4 - 4\gamma_1-6\gamma_2-8\gamma_3 \leq 2n-14 \; .$$

The period p in Thm. 2.3 satisfies

$$p = a(n+2-2\gamma_1-4\gamma_2-4\gamma_3)(n+3) + 4a\gamma_2 + 2b\gamma_1$$
$$\leq (n-5)(n-8)(n+3) + 4(n-5)\tfrac{n}{4} + 2(2n-14)\tfrac{n}{2}$$
$$= n^3-7n^2-18n+120 < n^3 \quad \text{since} \quad n \geq 9 .$$

We have used the fact that $\gamma_1 \leq \frac{n}{2}$ and $\gamma_2 \leq \frac{n}{4}$.

Proof of Cor. 2.6:

We suppose A satisfies Cond. 3.1. Then $\varphi^i(A)$ satisfies Cond. 3.1. for all i .

It is easy to see that $\theta(\varphi^i(A)),\ldots,\theta^{n+3+k(\varphi_i(A))-1}(A)$ do not satisfy Cond. 3.1. Therefore the minimal period p satisfies $\theta^p = \varphi^q$ for some q; that is, $\theta^p(A) = \varphi^q(A) = A$ for some q .

We suppose the 1-block and the 2-block circles respectively b and a times around by applying φ^q on A . Then it is easy to see that the 1-block meets the 2-block $c = b-a$ times by applying φ^q on A . As in the first part of the proof of Thm. 2.3 we see that p is as in the theorem.

4. The general situation.

In this section we will indicate by an example how to treat the general situation $E_k + \ldots + E_{k+p}$ for $p > 2$.

We suppose $p=3$. As in the case $p=2$ we must define the concepts: i-block (for $i=1,2,3,4$) , θ , φ , $k(A)$, meet, jump out, circle around, and "Cond. 3.1." Specially, $\varphi(A)=\theta^{n+4+k(A)}(A)$

We suppose $A \in \{0,1\}^n$ satisfies "Cond. 3.1", and contains 1 i-block B_i for $i=1,2,3,4$. Then we can show the following:

As a main rule B_1 moves $3+k(A)$ places by applying φ . B_1 moves in addition:

2 places if B_1 meets B_2 ,
1 place if B_1 meets B_3 or B_4 ,
1 place if B_1 jumps out of B_3 or B_4 ,
-1 place if B_1 circles around .

As a main rule B_2 moves $2+k(A)$ places by applying φ . B_2 moves in addition:

-2 places if B_1 meets B_2 ,
2 places if B_2 meets or jumps out of B_3 ,
2 places if B_2 meets or jumps out of B_4 ,
-2 places if B_2 circles around.

As a main rule B_3 moves $1+k(A)$ places by applying φ . B_3 moves in addition:

-2 places if B_1 meets B_3 ,
-4 places if B_2 meets B_3 ,
3 places if B_3 meets or jumps out of B_4 ,
-3 places if B_3 circles around.

As a main rule B_4 moves $k(A)$ places by applying φ . B_4 moves in addition:

-2 places if B_1 meets B_4 ,
-4 places if B_2 meets B_4 ,
-6 places if B_3 meets B_4 .

We suppose next that $A = \varphi^s(A)$, and that the 1-block, 2-block and 3-block respectively circles around a, b and c times. Let $K = \sum_{i=0}^{s-1} k(\varphi^i(A))$. By applying φ^s to A , B_1 moves the following number of places:

$3s+K$	(the main rule)
$-a$	(B_1 circles around a times)
$+2(a-b)$	(B_1 meets B_2 $(a-b)$ times)
$+2(a-c)$	(B_1 meets and jumps out of B_3 $2(a-c)$ times)
$+2a$	(B_1 meets and jumps out of B_4 $2a$ times).

Hence

(4.1) $na = 3s+K-a + 2(a-b) + 2(a-c) + 2a$.

In the same way, by studying B_2, B_3 and B_4 we get the equations:

(4.2) $nb = 2s+K - 2b - 2(a-b) + 4(b-c) + 4b$.

(4.3) $nc = s+K - 3c - 2(a-c) - 4(b-c) + 6c$.

(4.4) $0 = K - 2a - 4b - 6c$.

From (4.4) we see that $K = 2a + 4b + 6c$. Putting this into (4.1), (4.2) and (4.3), we get

(4.5) $3s = a(n-7) - 2b - 4c$.

(4.6) $2s = b(n-12) - 2c$.

(4.7) $s = c(n-15)$.

Hence,

(4.8) $a(n-7) - 2b - 4c = 3c(n-15)$.

(4.9) $b(n-12) - 2c = 2c(n-15)$.

As in the end of the first part of the proof of Thm. 2.3

we can show that φ^s is equal to θ applied

$$(4.10) \quad p = s(n+4) + K = c(n-15)(n+4) + 2a + 4b + 6c$$

times (We use (4.4) and (4.7)). p is therefore a period for A .

Let us check the above result on the following example: $n=19$, $k=7$ and $A = 0001011001110001111$. Calculations show that the period of A is $p = 748$.

Putting $n=19$ into (4.8) and (4.9) we then get

$$(4.11) \quad 12a - 2b - 4c = 12c ,$$

$$(4.12) \quad 7b - 2c = 8c .$$

The smallest integers satisfying (4.11) and (4.12) are $a=11$, $b=10$, $c=7$. We put these into (4.10), and again obtain $p = 7 \cdot 4 \cdot 23 + 2 \cdot 11 + 4 \cdot 10 + 6 \cdot 7 = 748$ as a period.

5. Proofs of Lemmas from Section 3.

Throughout this section, k,n and θ are as in Thm. 2.3.

Definition 5.1.

If $a=1$, then $a'=0$. If $a=0$, then $a'=1$. Moreover, for every $C = c_1 \dots c_t \in \{0,1\}^t$, we define $C' = c_1' \dots c_t'$.

Lemma 5.2.

If $A = a_1 \dots a_n$, then $\theta(A) = a_2 \dots a_n a_1'$ whenever $w(a_2 \dots a_n) \in \{k,k+1,k+2\}$, $\theta(A) = a_2 \dots a_n a_1$ otherwise.

The proof is obvious.

Definition 5.3.

Suppose $A = a_1 \dots a_n$ and $C = a_s \dots a_r$.

If C is outside all the 3-blocks in A and $C=10$ or $11t(01)00$ for some $t \geq 0$, C is an H-block in A .

If C is inside a 3-block in A and $C=01$ or $00t(10)11$ for some $t \geq 0$, C is a K-block in A .

Lemma 5.4.

Suppose $A \in \{0,1\}^n$ and $w(A) = k+3$.

a) If $A=10C$, then $\theta^2(A) = C01$.

b) If $A = 11t(01)00C$, then $\theta^{4+2t}(A) = C00t(10)11$.

c) Suppose

$$B_3 = 11s_o(01)1C_1 \dots C_p 1s_1 C_{p+1} 1s_2 \dots C_{p+q} 1s_{q+1} ,$$

$$G = 00f(10)0D_1 \dots D_r \text{ and } A = B_3 G E ,$$

where $s_1 > 0$, each C_i is a K-block, each D_i is an H-block and $s_i, f \geq 0$. Furthermore, let

$$\tilde{B}_3 = 00s_o(10)0C_1' \dots C_p' 1s_1 C'_{p+1} 1s_2 \dots C'_{p+q} 1s_{q+1}$$

$$\tilde{G} = 11f(01)1D_1' \dots D_r' = G'$$

$$y = r(A,B_3) \text{ and } z = r(A,G) .$$

Then we have

$$\theta^y(A) = GE\tilde{B}_3 , \ \theta^z(A) = E\tilde{B}_3\tilde{G} , \ w(\theta^y(A)) = k \text{ and}$$

$$w(\theta^z(A)) = k+3 .$$

Proof.

a) and b) follows from Lemma 5.2.

c) Let $n_i = r(A,C_i)$ and $m_i = r(A,D_i)$. We use Lemma 5.2 many times. The vectors in the following equations have weight k .

$$\begin{aligned}
\theta^{3+2s_o}(A) &= C_1 \ldots E00s_o(10)0 \\
\theta^{n_1}(A) &= C_2 \ldots E00s_o(10)0C_1' \\
&\ \ \vdots \\
\theta^{n_p}(A) &= 1s_1 \ldots E00s_o(10)0C_1' \ldots C_p' \\
\theta^{n_p+s_1}(A) &= C_{p+1} \ldots E00s_o(10)0C_1' \ldots C_p'1s_1 \\
\theta^{n_{p+1}}(A) &= 1s_2 \ldots E00s_o(10)0C_1' \ldots C_p'1s_1C_{p+1}' \\
&\ \ \vdots \\
\theta^{n_{p+q}}(A) &= 1s_{q+1} \ldots E00s_o(10)0C_1'1s_1C_{p+1}' \ldots C'_{p+q} \\
\theta^{y}(A) &= 00f(10)0D_1 \ldots D_rE\tilde{B}_3 = GE\tilde{B}_3 \ .
\end{aligned}$$

The vectors in the following equations have weight $k+3$.

$$\begin{aligned}
\theta^{y+3+2f}(A) &= D_1 \ldots D_rE\tilde{B}_3 11f(01)1 \\
\theta^{m_1}(A) &= D_2 \ldots D_rE\tilde{B}_3 11f(01)1D_1' \\
&\ \ \vdots \\
\theta^{z}(A) = \theta^{m_r}(A) &= E\tilde{B}_3 11f(01)1D_1' \ldots D_r' = E\tilde{B}_3\tilde{G} \ .
\end{aligned}$$

Proof of Lemma 3.2:

(5.1) If $A = D01$ and $w(A) = k+3$, then $\theta^{-2}(A) = 10D$.

(5.2) If $A = D00s(10)11$ and $w(A) = k+3$ where $s \geq 0$, then $\theta^{-(4+2s)}(A) = 11s(01)00D$.

Suppose A satisfies 1) and 2) in Def. 3.1, and $A = CD$ where C ends with a 3-block and D does not contain any 3-block. We define $p_1 = n-r(A,C)$. Then $A_1 = \theta^{-p_1}(A)$ ends with a 3-block. (5.1) and (5.2) implies that $w(A_1) = k+3$. Therefore A_1 satisfies 1), 2) and 4) in Cond. 3.1.

Suppose $A_1 = C_1 \ldots C_p E B_3$ where $C_i = 10$ or $C_i = 11s(01)00, B_3$ is a 3-block and E starts with 0 or a 3-block. Let $p_2 = r(A,C_p)$. $\theta^{p_2}(A_1) = EB_3C_1' \ldots C_p'$. Then $B_3C_1' \ldots C_p'$ becomes a 3-block in $\theta^{p_2}(A_1)$. Therefore $\theta^{p_2}(A_1)$ satisfies Cond. 3.1.

<u>Proof.of Lemma 3.6</u>:

We observe that A has the form

$$A = 0s_1Q_10s_2Q_20s_3 \ldots\ldots 0s_pQ_p$$

where $s_i \geq 0$, and Q_i has one of the following forms for $i < p$

(5.3) $Q_i = 10$ where Q_i is outside all the 3-blocks in A , and the 1-block in Q_1 does not meet any block by applying θ^{n+2} on A .

(5.4) $Q_i = 11t(01)00$ where $t \geq 0$, Q_i is outside all the 3-blocks in A , and the blocks in Q_i do not meet any 3-block in A by applying θ^{n+2} on A .

(5.5) $Q_i = B_3G$ where B_3 and G are as in Lemma 5.4. c) .

Furthermore,

(5.6) If Q_1 is of the form (5.3) or (5.4), then $s_1 > 0$. If Q_i is of the form (5.5) and $0 \le i < p$, then Q_{i+1} is of the form (5.5) or $s_{i+1} > 0$. $Q_p = B_3$ where B_3 is as in Lemma 5.4. c).

By Lemma 5.4

$\theta^n(A) = 0_{s_1}\tilde{Q}_1 0_{s_2}\tilde{Q}_2 0_{s_3} \dots 0_{s_p}\tilde{Q}_p$ where $\tilde{Q}_i$ is defined as follows:

Case 1: If Q_i is as in (5.3), then $\tilde{Q}_i = 01$.

Case 2: If Q_i is as in (5.4), then $\tilde{Q}_i = 00t(10)11$.

Case 3: If $Q_i = B_3G$ is as in (5.5), then $\tilde{Q}_i = \tilde{B}_3\tilde{G}$ as in Lemma 5.4. c).

Case 4: If $i=p$, $\tilde{Q}_p = \tilde{B}_3$ is as in Lemma 5.4. c) (see (5.6)).

Furthermore, Lemma 5.4. c) implies $w(\theta^n(A)) = k$. Since A starts with $01, 11$ or 00, $\theta^n(A)$ starts with 00. Hence $\theta^{n+2}(A)$ is of the form

(5.7) $\theta^{n+2}(A) = C\tilde{Q}_p 11$ and $w(\theta^{n+2}(A)) = k+2$.

Next, we prove

(5.8) A 3-block in $A^* = \theta^{n+2}(A)1$ is contained in $\tilde{Q}_p 1$ or $\tilde{Q}_i$ where Q_i is as in (5.5).

Let Q_i be as in (5.5). By (5.6), $A = HQ_i 0t(10)M$ or $A = Q_i K$ where K starts with a 3-block. In both cases $\tilde{Q}_i$ is followed by $00t(10)0$ for some $t \ge 0$. If Q_i is as in (5.3) or (5.4), no 3-block in A^* can start at any position in $\tilde{Q}_i$. We conclude that (5.8) is true.

Case 1: We denote the 1-block in $Q_i = 10$ by B_1 . The number 1 in $\tilde{Q}_i = 01$ is in position $r(A,B_1)+1$ in $\theta^n(A)$, and is preceded and followed by 0 . Therefore, there is a 1-block B_1^* in position $r(A,B_1)-1$ in $A^* = \theta^{n+2}(A)1$. This is in accordance with a) since B_1 do not meet any block by applying θ^{n+2} on A .

Case 2: We denote the 2-block in Q_i by B_2 and the 1-blocks by $B_1^1,\dots,B_1^t$, such that $Q_i = B_2 0 B_1^1 0 \dots 0 B_1^t 00$. Since $\tilde{Q}_i = 00t(10)11$ is followed by 00 , there are 1-block in the positions $r(A,B_1^1)-1,\dots,r(A,B_1^t)-1$ and a 2-block in the position $r(A,B_2) + 2t+2$ in $\theta^n(A)$. Therefore, there are 1-blocks in the positions $r(A,B_1^1)-3,\dots,r(A,B_1^t)-3$ in $A^* = \theta^{n+2}(A)1$. This is in accordance with a) since the 1-blocks meet B_2 by applying θ^{n+2} . Furthermore, there is a 2-block in the position $r(A,B_2)+2t$. This is in accordance with b), since B_2 meet t 1-blocks by applying θ^{n+2} on A .

Case 3: $Q_i = B_3 G$ and $\tilde{Q}_i = \tilde{B}_3\tilde{G}$ where

$$B_3 = 11 s_0(01) 1 C_1 \dots C_p 1^{s_1} C_{p+1} 1^{s_2} \dots C_{p+q} 1^{s_{q+1}}$$

$$G = 00f(10)0D_1 \dots D_r$$

$$\tilde{B}_3 = 00 s_0(10) 0 C_1' \dots C_p' 1^{s_1} C'_{p+1} 1^{s_2} \dots C'_{p+q} 1^{s_{q+1}}$$

$$\tilde{G} = 11\, f(01) 1 D_1' \dots D_r'$$

where $s_1 > 0$, C_i is a K-block, D_i is an H-block and $s_i, f \geq 0$.

We divide Case 3 into 9 subcases.

<u>Case 3a</u>: Suppose $1 \leq i \leq p$. Suppose $C_i = 01 = B_1 1$ where B_1 is a 1-block which jumps out of B_3. Then $C_i' = 10, C_i'$ is preceded by a 0 and is outside all the 3-blocks in $\theta^n(A)$. Therefore there is a 1-block in $\theta^n(A)$ in position $r(A,B_1)$, hence a 1-block in A^* in **position** $r(A,B_1) - 2$.

<u>Case 3b</u>: Suppose $1 \leq i \leq p$ and $C_i = 00t(10)11$. $C_i' = 11t(01)00$ is outside all the 3-blocks in $\theta^n(A)$. As in Case 3a, the blocks in C_i do not move by applying θ^n. Therefore if B is a block in C_i, there is a block B^* of the same type in A^* such that $r(A^*,B^*) = r(A,B) - 2$. Since the block B jumps out of the 3-block B_3 by applying θ^{n+2}, this is in accordance with Lemma 3.6 a) and b).

<u>Case 3c</u>: The 1-blocks in $s_o(01)$ move as the 1-block in Case 3a.

<u>Case 3d</u>: We define B^*_3 and F by

$$B^*_3 = 1_{s_1} C'_{p+1} 1_{s_2} \ldots 1_{s_{q+1}} 11f(01)1D'_1 \ldots D'_r = 11F ,$$

hence $\tilde{Q}_i = 00s_o(10)0C_1' \ldots C'_p B^*_3$. First we prove that B^*_3 starts with $11t(01)1$ for some $t \geq 0$. If $s_1 \geq 2$, $C'_{p+1} = 11t(01)00$ or $C'_{p+1} \ldots 1s_{q+1}$ is the empty set, the claim is trivially true. Therefore, we suppose $s_1 = 1$ and $C'_{p+1} = 10$. If we move from the left to the right in F, we reach two consecutive 1's before we reach two consecutive 0's. Hence, B^*_3 starts with $11t(01)1$ for **some** $t \geq 0$. Next we observe that B^*_3 does not contain any piece of the form $00s(10)0$. By (5.8) B^*_3 is a 3-block in A^*. We now observe that:

$$m(B_3) = 3 + s_1 + \dots + s_{q+1} = m(B^*_3) ,$$

$$r(A^*,B^*_3) = r(A,B) + 3 + 2\beta_1 + 4\beta_2 - 2$$

where β_i = the number of i-blocks in $11f(01)1D'_1 \dots D'_r$ = the number of i-blocks which meet B_3 by applying θ^{n+2} ,

$$l(A^*,B^*_3) = l(A,B) + 3 + 2\beta_1 + 4\beta_2 - 2$$

where β_i = the number of i-blocks in $00s_o(10)0C'_1 \dots C'_p$ = the number of i-blocks which jump out of B_3 by applying θ^{n+2} .

Case 3e: Suppose $p < i \leq p+q$ and $C_i = 01 = B_1 0$ where B_1 is a 1-block in A contained in B_3 . Then $C_i^! = 10$, $C_i^!$ is followed by a 1 and $C_i^!$ is contained in B^*_3 . The 0 in $C_i^!$ is a 1-block in A^* . Hence, there is a 1-block in A^* in the position $r(A,B_1) - 1$. This is in accordance with the lemma since B_1 does not meet or jump out of any block by applying θ^{n+2} .

Case 3f: Suppose $p < i \leq p+q$ and $C_i = 00t(10)11 = B_2 1B_1^1 1B_1^2 \dots 1B_1^t 11$ where B_2 is a 2-block and B_1^i are 1-blocks. $C_i^! = 11t(01)00 = 11B_1^1{}^*1B_1^2{}^* \dots 1B_1^t{}^*1B^*_2$ where $B_1^i{}^*$ are 1-blocks and B^*_2 is a 2-block in A^* . $r(A^*,B_1^i{}^*) = r(A,B_1) -3$ and $r(A^*,B^*_2) = r(A,B_2) + 2t$. This is in accordance with the lemma, since B_1^i meets a 2-block and B_2 meets t 1-blocks by applying θ^{n+2} .

Case 3g: Suppose $D_i = 10 = B_1 0$ where B_1 is a 1-block which meets B_3 by applying θ^{n+2} . $D'_i = 01 = B^*_1 1$ is contained in B^*_3 , and B^*_1 is a 1-block in A . $r(A^*,B^*_1) = r(A,B_1) -2$.

Case 3h: The 1-blocks in $f(10)$ move as the 1-block in case 3g.

Case 3i: Suppose $D_i = 11t(01)00 = B_2 0 B_1^1 0 B_1^2 \dots 0 B_1^t 00$ where B_2 is a 2-block and B_1^i are 1-blocks in A.
$D_i' = 00t(10)11 = B^*_2 1 B_1^1{}^* 1 B_1^2{}^* \dots 1 B_1^t{}^* 11$ where $B_1^i{}^*$ are 1-blocks and B^*_2 is a 2-block in A^*. $r(A^*, B^i_{1*}) = r(A, B_1^i) - 2$ and $r(A^*, B^*_2) = r(A, B_2) - 2$. This is in accordance with the lemma, since B_1^i and B_2 meet B_3 by applying θ^{n+2}.

Case 4: This case is treated like Case 3a ,..., Case 3f. Specially, there is a 3-block B^*_3 in A^* such that $r(A^*, B^*_3) = n+1$.

The proof of Lemma 3.6 a), b), c) and d) is now complete.

Suppose Q_1 is of the form (5.5). Then $\tilde{Q}_1$ starts with $00s_o(10)0$ and e) is satisfied.

Next, suppose Q_1 is of the form (5.3) or (5.4). By (5.6) $s_1 > 0$. A is of the form $0s_1 C_1 \dots C_e D$ where D starts with 0 or a 3-block, and $C_i = 10$ or $C_i = 11t(01)00$ for some $t \geq 0$. $\theta^n(A) = 0s_1 C_1' \dots C_e' \tilde{D}$ where $\tilde{D}$ starts with $00s(10)0$ for some $s \geq 0$, and e) is satisfied.

The proof of Lemma 3.6 is complete.

Proof of Lemma 3.10. We denote the last 3-block in A by B_3. We let $A^* = \theta^{n+2}(A)1 = s(10)0C_1 \dots C_p D$ be as in Lemma 3.6.e). Besides, we denote A^* by $A^* = a^*_1 \dots a^*_{n+1}$ and put $r = r(A^*, C_p)$. Then

$$\varphi(A) = \theta^{n+3+k(A)}(A) = a^*_{r+1} \dots a^*_n s(01)1C_1' \dots C_p' =$$

$a^*{}_{r+1} \ldots a^*{}_n a^*{}_1{}' \ldots a^*{}_r{}'$.

We suppose $\hat{B}^*{}_3 = a^*{}_s \ldots a^*{}_{n+1}$. From (5.7) in the proof of Lemma 3.6 we get that $a^*{}_{n-1} = a^*{}_n = 1$. Therefore,

$\hat{B}_3^{**} = a^*{}_s \ldots a^*{}_n s(01)1C_1' \ldots C_p' = a^*{}_s \ldots a^*{}_n a^*{}_1{}' \ldots a^*{}_r{}'$

is a 3-block in $\varphi(A)$.

Since (the number of 1's in $s(01)1C_1' \ldots C_p'$) - (the number of 0's in $s(01)1C_1' \ldots C_p'$) = 1 , $m(\hat{B}_3^*) = m(\hat{B}_3^{**})$. We observe that $k(A) = r-1 = 2\beta_1 + 4\beta_2$ where β_i = the number of i-blocks which meet $\hat{B}_3$ by applying φ. Hence,

$$r(\hat{B}_3^{**}) = n = r(\hat{B}_3) - (k(A) - 2\beta_1 - 4\beta_2) .$$

Next let B_i be an i-block in A which corresponds to a block B_i^* in $a_1^* \ldots a_r^*$. We prove that B_i corresponds to an i-block in $\varphi(A)$ such that $r(B_i^{**}) = n + r(B_i^*) - (k(A)+1)$. If $B_1^* = a_j^* = 1$, then $B_1^{**} = a_j^{*\prime} = 0$ is a 1-block in $\varphi(A)$ and

$$(5.9) \qquad r(B_1^{**}) = n-r+j = n+j-(k(A)+1) = n+r(B_1^*)-(k(A)+1) .$$

Analogously, there exists a 2-block B_2^{**} in $\varphi(A)$ such that

$$(5.10) \qquad r(B_2^{**}) = n+r(B_2^*) - (k(A)+1) .$$

By Lemma 3.6.a) and (5.9) (y,z are defined in Lemma 3.6.a))

$$(5.11) \qquad r(B_1^{**}) = n+r(B_1) - ([k(A)+2]+y+2z+1-1) .$$

We add and subtract 1 to indicate that B_1 both circles around and meets $\hat{B}_3$ by applying φ . (5.11) is in accordance with

Lemma 3.10.a). By Lemma 3.6.b) and (5.10) (y,z are defined in Lemma 3.6.b))

$$(5.12) \qquad r(B_2^{**}) = n+r(B_2) - ([k(A)+1]+2y-2z+2-2) \ .$$

We add and subtract 2 to indicate that B_2 both circles around and meets $\hat{B}_3$ by applying φ . (5.12) is in accordance with Lemma 3.10.b).

Suppose B_i is an i-block in A different from $\hat{B}_3$, which does not circle around by applying φ , and corresponds to B_i^* in A^* . Since $\varphi(A) = \theta^{(n+2)+(1+k(A))}(A)$, there exists an i-block B_i^{**} in $\varphi(A)$ such that

$$(5.13) \qquad r(B_i^{**}) = r(B_i^*) - k(A)-1 \ , \ l(B_i^{**}) = l(B_i^*)-k(A)-1 \ \text{ and }$$
$$m(B_3^{**}) = m(B_3^*) \ .$$

By (5.13) and Lemma 3.6 the Lemma is true for B_i .

Finally, $l(\hat{B}_3^{**}) = l(\hat{B}_3^*) - k(A)-1$. Therefore, by Lemma 3.6 we get that d) in the Lemma is true for $B_3 = \hat{B}_3$.

The proof of Lemma 3.12 follows easily from the proof of Lemma 3.10.

Lemma 5.5.

Suppose B and C are blocks in $A = a_1 \ldots a_n$ and specially that B is a 2-block. Furthermore, suppose $\hat{B}_3$ is the last 3-block in A . Let $\mathcal{M} = \mathcal{M}(B,C)$ be as in Def. 3.13. We then define

$$\mathcal{N} = \mathcal{N}(B,C) = \cup\{D \subset \mathcal{M} : \ D \text{ is an H-block or a K-block in } A\}$$

$\cup\{\{a_i,a_{i+1}\}\subset \mathcal{M} : a_i \in D$ is a left endpoint of a 3-block in $A\}$

$\cup\{\{a_i,a_{i+1}\}\subset \mathcal{M} : a_{i-1} \in D$ is a right endpoint of a 3-block $\neq \hat{B}_3$ in $A\}$.

If $C \neq \hat{B}_3$, then $d(B,C) = \operatorname{card}\mathcal{M} - \operatorname{card}\mathcal{N}$, while $C = \hat{B}_3$ implies $d(B,\hat{B}_3) = \operatorname{card}\mathcal{M} - \operatorname{card}\mathcal{N} + 2$. Besides, all the sets in the union in this lemma are disjoint.

Proof: By studying the definitions of blocks we observe that all the sets in the union in the lemma are disjoint. Hence,

card $\mathcal{N}$ = 2(the number of 1-blocks between B and C)
+ 4(the number of 2-blocks between B and C)
+ 2(the number of endpoint $a_i \neq a_n$, between B and C , of 3-blocks) .

If $C \neq \hat{B}_3$, then T = (the number of endpoints, between B and C , of 3-blocks)$-2z$ is equal to (the number of endpoints $a_i \neq a_n$, between B and C , of 3-blocks) , else T = (the number of endpoints $a_i \neq a_n$, between B and C , of 3-blocks) -2 , where z is as in Def. 3.13. Therefore, $\chi = \operatorname{card}\mathcal{N}$ if $C \neq \hat{B}_3$, and $\chi = \operatorname{card}\mathcal{N} - 2$ otherwise.

Proof of Lemma 3.14: In this proof, B_i and C_i denote i-blocks. Furthermore, "meet", "jump out" and "move" mean meet by applying φ etc.

a) Suppose $B_1^1, \ldots, B_1^t$ meet B_2 . By Def. 3.5 and 3.8 we can suppose

(5.14) $\quad r(B_1^i) = r(B_2)+2i$

and that B_1^i and $B2$ cannot meet any 3-block $\neq \hat{B}_3$. From Lemma 3.10, if B_1^i **meets** $\hat{B}_3$, then B_1^i moves 1 position in addition. Moreover, B_1^i also circles around, hence moves -1 position in addition. Analogously with B_2 . Lemma 3.10 implies

$$r(\varphi(B_1^i))=r(B_1^i)-(k(A)+2+2)=r(B_2)+2i-k(A)-4 \quad \text{and} \quad r(\varphi(B_2)) =r(B_2)-(k(A)+1-2t).$$

Hence,

(5.15) $\quad r(\varphi(B_1^i)) - r(\varphi(B_2)) = 2i-3-2t$

By (5.14) and (5.15) we get

$$d(B_1^i,B_2) = (r(B_1^i) - r(B_2)-1) - 2(i-1) = r(B_2)+2i-r(B_2)-1-2i+2 = 1 .$$

$$\operatorname{card}\mathfrak{M} (\varphi(B_1^i),\varphi(B_2)) = r(\varphi(B_1^i))-1+n-r(\varphi(B_2)) = n - 4+2i-2t .$$

$$d(\varphi(B_1^i),\varphi(B_2)) = n-4+2i-2t-2(\gamma_1-(t-i+1))-2(\gamma_2-1)-2\gamma_3+1=n+1-2\gamma_1-2\gamma_2-2\gamma_3.$$

This is in accordance with the first part of a).

Suppose B_1 and B_2 do not meet, and let $\mathfrak{M} = \mathfrak{M}(B_1,B_2), \chi=\chi(B_1,B_2), z=z(B_1,B_2), \mathfrak{M}_\varphi = \mathfrak{M}(\varphi(B_1),\varphi(B_2))$, $\chi_\varphi = \chi(\varphi(B_1),\varphi(B_2)), z_\varphi=z(\varphi(B_1),\varphi(B_2))$. We calculate $\operatorname{card}\mathfrak{M}_\varphi$ and χ_φ by the following prodedure: First, put $\operatorname{card}\mathfrak{M}_\varphi = \operatorname{card}\mathfrak{M}$ and $\chi_\varphi = \chi$. By Lemma 3.10 we must decrease $\operatorname{card}\mathfrak{M}_\varphi$ and χ_φ according to the following table:

		Decrease card($\mathfrak{M}_\varphi$) by	Decrease χ_φ by
	The main rule	1	0
	B_1 meets a 2-block	2	2
(5.16)	B_1 meets $\hat{B}_3$	0	0
	B_1 meets a 3-block $\neq \hat{B}_3$	1	1
	B_1 jumps out of a 3-block	1	1
	A 1-block meets B_2	2	2
(5.17)	B_2 meets $\hat{B}_3$	0	0
	B_2 meets a 3-block $\neq \hat{B}_3$	-2	-1
	B_2 jumps out of a 3-block	-2	-1

(5.16) follows in this way: If B_1 meets $\hat{B}_3$, both $\mathfrak{M}_\varphi$ and χ_φ decrease by 1. However, B_1 also circles around, hence $\mathfrak{M}_\varphi$ increases by 1 . Besides, χ_φ increases by 1 since $z = 1$ and $z_\varphi = 0$. (5.17) follows in the same way. Conclusion: card $\mathfrak{M}_\varphi - \chi_\varphi$ = card $\mathfrak{M} - \chi$ if B_2 meet a 3-block $\neq \hat{B}_3$ or jumps out of a 3-block, else

$$\text{card}\,\mathfrak{M}_\varphi - \chi_\varphi = (\text{card} \quad -\chi)-1 .$$

Hence, a) is proved.

b) Suppose $A = a_1 \ldots a_n$, $\mathfrak{M} = \mathfrak{M}(B_2,B_3)$ and $\mathfrak{N} = \mathfrak{N}(B_2,B_3)$ (see Lemma 5.5). In the following and asterisk below a_i means: $a_i \in \mathfrak{M}$ and $a_i \notin \mathfrak{N}$. We observe

(5.18) If $B_2 = a_i a_{i+1}$, then $a_i \in \mathfrak{M}$ and $a_i \notin \mathfrak{N}$.

First we suppose $B_3 \neq \hat{B}_3$, hence

(5.19) $A = DB_3\underset{**}{00}s(10)\underset{*}{0}C_1 \ldots C_pE$ where E starts with 0 or a 3-block and C_i are H-blocks.

If B_2 meets B_3 , then B_2 is contained in $C_1 \ldots C_p$. (5.18) and (5.19) imply by Lemma 5.5 that $d(B_2,B_3) = 4$.

If B_2 does not meet B_3 , we have two cases

(5.20) $\quad A = DB_3\underset{**}{00}s(10)\underset{*}{0}C_1\ldots C_p\underset{*}{0}F$ or $A = DB_3\underset{**}{00}s(10)\underset{*}{0}C_1\ldots C_p11t(01)\underset{*}{1}F$

Besides, B_2 is contained in F or D . (5.18) and (5.20) imply by Lemma 5.5 that $d(B_2,B_3) \geq 5$.

Finally we suppose $B_3 = \hat{B}_3$. Moreover, we suppose B_2^* and $\hat{B}_3^*$ in $A^* = \theta^{n+2}(A)1$ correspond to B_2 and $\hat{B}_3$. We now prove that

(5.21) $\quad d(B_2^*,\hat{B}_3^*) = d(B_2,B_3)$.

Suppose $\mathfrak{m} = \mathfrak{m}(B_2,\hat{B}_3), \chi = \chi(B_2,\hat{B}_3), \mathfrak{m}^* = \mathfrak{m}(B_2^*,\hat{B}_3^*)$ and $\chi^* = \chi(B_2^*,\hat{B}_3^*)$. We calculate card $\mathfrak{m}^*$ and χ^* by the following procedure: First put card $\mathfrak{m}^*$ = card $\mathfrak{m}$ and $\chi^* = \chi$. By Lemma 3.6 we must decrease card $\mathfrak{m}^*$ and χ^* according to the following table:

	Decrease card $\mathfrak{m}^*$ by	Decrease χ^* by
A 1-block meet B_2 by applying θ^{n+2}	-2	-2
B_2 meet a 3-block by applying θ^{n+2}	2	2
B_2 jumps out of a 3-block by applying θ^{n+2}	2	2

Hence, $d(B_2^*,\hat{B}_3^*) = \text{card}\,\mathfrak{m}^* - \chi^* = \text{card}\,\mathfrak{m} - \chi = d(B_2,\hat{B}_3)$.

Next we prove

(5.22) $\quad B_2^*$ in A^* circles around (this is equivalent to "B_2 meets $\hat{B}_3$") if and only if $d(B_2^*,\hat{B}_3^*) = 4$.

A^* has the following form as in Lemma 3.12.e.

(5.23) $\quad s(10)\underset{*}{0}C_1 \ldots C_pD$ where D starts with a 0 or a 3-block

and C_i are H-blocks. If B_2 meets $\hat{B}_3$, B_2^* is contained in $C_1 \ldots C_p$. Putting $\mathcal{N}^* = \mathcal{N}(B_2^*, \hat{B}_3^*)$ we get by (5.18), (5.23) and Lemma 5.5 that $\operatorname{card}\mathcal{M}^* - \operatorname{card}\mathcal{N}^* = 2$. If B_2 does not meet $\hat{B}_3$, we show as in the case $B_3 \neq \hat{B}_3$ that $\operatorname{card}\mathcal{M}^* - \operatorname{card}\mathcal{N}^* \geq 3$. By Lemma 5.5 $d(B_2^*, \hat{B}_3^*) = \operatorname{card}\mathcal{M}^* - \operatorname{card}\mathcal{N}^* + 2$ and the proof of (5.22) is complete.

Combining (5.21) and (5.22) we get: B_2 **meets** $\hat{B}_3$ if and only if $d(B_2, \hat{B}_3) = 4$.

Suppose B_2 **meets** $B_3 \neq \hat{B}_3$ (the case $B_3 = \hat{B}_3$ is treated in the same way), and that there are T_i i-blocks between B_2 and B_3. Moreover, we suppose $A = EB_3 00s(10)0C_1 \ldots C_iC_{i+1}F$ where C_j are H-blocks and $C_{i+1} = B_2t(01)00$. Observing that $\operatorname{card}(00s(10)0C_1 \ldots C_i) = 3 + 2T_1 + 4T_2$, we get

$$r(B_2) - r(B_3) = 5 + 2T_1 + 4T_2 .$$

Supposing there are s_i i-blocks which meet B_3 we get:

$$r(\varphi(B_2)) = r(B_2) - 1 - 2 - k(A) .$$
$$r(\varphi(B_3)) = r(B_3) + 2s_1 + 4s_2 - k(A) .$$
$$\begin{aligned}
\operatorname{card}\mathcal{M}(\varphi(B_2),\varphi(B_3)) &= [r(\varphi(B_2))-1] + n - r(\varphi(B_3)) \\
&= n-4-2s_1-4s_2+(r(B_2)-r(B_3)) \\
&= n+1+2(T_1-s_1)+4(T_2-s_2) .\\
\chi(\varphi(B_2),\varphi(B_3)) &= 2(\gamma_1-(s_1-T_1))+4(\gamma_2-(s_2-T_2))+2(2\gamma_3-1)-2 \\
&= 2\gamma_1+4\gamma_2+4\gamma_3-4-2(s_1-T_1)-4(s_2-T_2) .
\end{aligned}$$
$$d(\varphi(B_2),\varphi(B_3)) = \operatorname{card}\mathcal{M}(\varphi(B_2),\varphi(B_3)) - \chi(\varphi(B_2),\varphi(B_3)) = n+5-2\gamma_1-4\gamma_2-4\gamma_3 .$$

The last part of b), and the parts c), d) and e) are proved by using a procedure and a table as in the proof of a).

Definition 5.6

Suppose B and C are two blocks in $A = a_1 \dots a_n$. If B is to the left of C, we define

$$\overline{\mathcal{M}}(B,C) = \overline{\mathcal{M}} = \{a_{l(C)+1}, \dots, a_n\} \cup \{a_1, \dots, a_{l(B)-1}\} \quad \text{and} \quad z(B,C)=z=1,$$

else

$$\overline{\mathcal{M}}(B,C) = \overline{\mathcal{M}} = \{a_{l(C)+1}, \dots, a_{l(B)-1}\} \quad \text{and} \quad z(B,C) = z = 0 .$$

We define "between", $\overline{\chi}(B,C) = \overline{\chi}$ and $\overline{d}(B,C)$ as in Def. 3.13 by using $\overline{\mathcal{M}}$ instead of $\mathcal{M}$.

Lemma 5.7.

Suppose B_i is an i-block for $i = 2,3$. Then B_2 jumps out of B_3 if and only if $\overline{d}(B_2,B_3) = 2$. In this case

$$\overline{d}(\varphi(B_2),\varphi(B_3)) = n + 3 - 2\gamma_1 - 4\gamma_2 - 4\gamma_3 ,$$

otherwise

$$\overline{d}(\varphi(B_2),\varphi(B_3)) = \overline{d}(B_2,B_3) - 1 .$$

The proof of Lemma 5.7 is similar to the proof of Lemma 3.14.b). We only indicate the proof on an example: $n = 14$, $k = 3$ and

$$A = 0\,0\,0\,\overset{*}{1}\,0\,0\,0\,\underline{1\,1\,1\,\overline{0\,0}\,1\,1}$$

$$\varphi(A) = 0\,\overset{*}{1}\,0\,0\,0\,0\,0\,\overline{1\,1}\,0\,0\,\underline{1\,1\,1}$$

Denoting the i-blocks in A by B_i we observe that
$\mathrm{card}\,\overline{\mathcal{M}}(B_2,B_3) = 2$, $z(B_2,B_3) = 0$, $\overline{\chi}(B_2,B_3) = 0$,
$\mathrm{card}\,\overline{\mathcal{M}}(\varphi(B_2),\varphi(B_3)) = 9 = n-5$, $z(\varphi(B_2),\varphi(B_3)) = 1$,
$\overline{\chi}(\varphi(B_2),\varphi(B_3)) = 2\gamma_1 + 4(\gamma_2-1) + 2(2\gamma_3-1) -2 = 2+0+2-2 = 2$.
Hence, $\bar{d}(B_2,B_3) = 2$ and

$$\bar{d}(\varphi(B_2),\varphi(B_3)) = (n-5)-(2\gamma_1+4(\gamma_2-1)+2(2\gamma_3-1)-2) = n+3-2\gamma_1-4\gamma_2-4\gamma_3 .$$

Lemma 5.8

Suppose B_i is an i-block in A for $i = 2,3$, A satisfies Cond. 3.1 and let $s = n+2 - 2\gamma_1-4\gamma_2-4\gamma_2$. Then

$$d(B_2,B_3) = d(\varphi^s(B_2),\varphi^s(B_3)) \text{ and } \bar{d}(B_2,B_3) = \bar{d}(\varphi^s(B_2),\varphi^s(B_3)) .$$

Proof: We show first that

$$(5.25) \qquad 4 \leq d(B_2,B_3) \leq n+5-2\gamma_1-4\gamma_2-4\gamma_3 .$$

We choose p as the least integer such that $\varphi^{-p}(B_2)$ meets $\varphi^{-p}(B_3)$ by applying φ . By Lemma 3.14.b)

$d(\varphi^{-(p-1)}(B_2),\varphi^{-(p-1)}(B_3)) = n+5-2\gamma_1-4\gamma_2-4\gamma_3$. Hence,
$d(B_2,B_3) = (p-1)+(n+5-2\gamma_1-4\gamma_2-4\gamma_3) \leq n+5-2\gamma_1-4\gamma_2-4\gamma_3$.
$4 \leq d(B_2,B_3)$ is obvious. Putting $T = d(B_2,B_3)$ we get

$$d(\varphi^{T-4}(B_2),\varphi^{T-4}(B_3)) = 4 .$$
$$d(\varphi^{T-3}(B_2),\varphi^{T-3}(B_3)) = n+5-2\gamma_1-4\gamma_2-4\gamma_3 = s+3 .$$
$$d(\varphi^s(B_2),\varphi^s(B_3)) = (s+3) - (s-T+3) = T = d(B_2,B_3)$$

since $\varphi^s = \varphi^{(s-T+3)}\circ\varphi^{T-3}$. $\bar{d}(B_2,B_3) = \bar{d}(\varphi^s(B_2),\varphi^s(B_3))$ follows in the same way.

Definition 5.9.

"Between" is used in the same way as in Def. 3.13. Suppose B and C are blocks in A. Then

$y_i(B,C)$ = the number of i-blocks between B and C $(i=1,2)$,

$y_3(B,C)$ = the number of endpoints between B and C, of 3-blocks.

Moreover, we order the positions in A relatively to B in this way: $r(B) < r(B)+1 < \ldots < n < 1 < \ldots < r(B)-1$.

Lemma 5.10

Suppose A satisfies Cond. 3.1. Moreover, let B_i^* be an i-block for $i=1,2$ and $d(B_1^*,B_2^*) = d(\varphi^p(B_2^*),\varphi^p(B_2^*))$. Then $d(B_1,B_2^*) = d(\varphi^p(B_1),\varphi^p(B_2^*))$ for every 1-block B_1.

Proof: Suppose $r(B_2^*) < r(B_1^*) < r(B_1)$ relatively to B_2^*. Then $z(B_1,B_2^*) = z(B_1,B_1^*) + z(B_1^*,B_2^*)$, $\mathcal{M}(B_1,B_2^*) = \mathcal{M}(B_1^*,B_2^*)+\mathcal{M}(B_1,B_1^*) + 1$ and

$$\begin{aligned}\chi(B_1,B_2^*) &= 2(y_1(B_1^*,B_2^*)+y_1(B_1,B_1^*)+1)+2(y_2(B_1^*,B_2^*)+y_2(B_1,B_1^*)) \\ &\quad + (y_3(B_1^*,B_2^*)+y_3(B_1,B_1^*))+z(B_1,B_2^*) = \chi(B_1,B_2^*)+\chi(B_1,B_1^*)+2 .\end{aligned}$$

Hence,

$$(5.26) \qquad d(B_1,B_2^*) = d(B_1,B_1^*)+d(B_1^*,B_2^*)-1 .$$

By Lemma 3.14 c) $d(\varphi^p(B_1),\varphi^p(B_1^*)) = d(B_1,B_1^*)$. Since $r(B_2^*) < r(B_1^*) < r(B_1)$, $d(B_1^*,B_2^*) < d(B_1^*,B_1)$.
Hence, $d(\varphi^p(B_1^*),\varphi^p(B_2^*)) < d(\varphi^p(B_1^*),\varphi^p(B_1))$, which implies $\varphi^p(B_2^*) < \varphi^p(B_1^*) < \varphi^p(B_1)$ relatively to $\varphi^p(B_2^*)$. Similar to (5.26), we get $d(\varphi^p(B_1),\varphi^p(B_2^*))=d(\varphi^p(B_1),\varphi^p(B_1^*))+d(\varphi^p(B_1^*),\varphi^p(B_2^*))-1$

Hence, $d(B_1,B_2^*)=d(\varphi(B_1),\varphi(B_2^*))$.

If $r(B_2^*) < r(B_1) < r(B_1^*)$ relatively B_2^* , we show similar to (5.26) that

$$d(B_1^*,B_2^*) = d(B_1^*,B_1) + d(B_1,B_2^*)-1 ,$$
$$d(\varphi^p(B_1^*),\varphi^p(B_2^*)) = d(\varphi^p(B_1^*),\varphi^p(B_1)) + d(\varphi^p(B_1),\varphi^p(B_2^*))-1 .$$

This implies by Lemma 3.14. c) that $d(B_1,B_2^*) = d(\varphi^p(B_1),\varphi^p(B_2^*))$.

Lemma 5.11.

Suppose A satisfies Cond. 3.1, and B_i is an i-block for $i=1,2,3$. Then

$$d(B_2,B_3) + d(B_3,B_2) = (n-2)-[2\gamma_1+4(\gamma_2-1)+2(2\gamma_3-1)+2] ,$$
$$\bar{d}(B_2,B_3) + \bar{d}(B_3,B_2) = (n-2)-[2\gamma_1+4(\gamma_2-1)+2(2\gamma_3-1)+2] ,$$
$$d(B_1,B_2) + d(B_2,B_1) = (n-2)-[2(\gamma_1-1)+2(\gamma_2-1)+2\gamma_3+1] .$$

Proof: We observe that $\mathfrak{M}(B_2,B_3) + \mathfrak{M}(B_3,B_2) = n-2$ and $\chi(B_2,B_3) + \chi(B_3,B_2) = [2\gamma_1+4(\gamma_2-1)+2(2\gamma_3-1)+2]$. Hence, the first equality is true. The other equalities are proved in the same way.

Proof of Lemma 3.15. C_i denotes an arbitrary i-block. Lemmas 5.8, 5.11 and 3.13.d) imply

$$\begin{aligned}(5.27)\quad &\bar{d}(\varphi^t(C_3),\varphi^t(B_2)) = \bar{d}(C_3,B_2), d(\varphi^t(C_3),\varphi^t(B_2)) = d(C_3,B_2),\\ &d(\varphi^t(C_2),\varphi^t(B_2)) = d(C_2,B_2), d(\varphi^t(C_1),\varphi^t(B_2)) = d(C_1,B_2) .\end{aligned}$$

Let $A = DB_2E = a_1 \dots a_n$, $\varphi^t(A) = F\varphi^t(B_2)G = b_1\dots b_n$, $i = r(B_2)$ and $j = r(\varphi^t(B_2))$. We then get

$$B_2 \text{ is contained in } C_3 \Longleftrightarrow d(B_2,C_3) > \bar{d}(B_2,C_3)$$

$$(5.28) \quad \Longleftrightarrow d(\varphi^t(B_2),\varphi^t(C_3)) > \bar{d}(\varphi^t(B_2),\varphi^t(C_3)) \Longleftrightarrow \varphi^t(B_2) \text{ is contained in } \varphi^t(C_3) .$$

We suppose there exist a minimal integer q such that $a_{i+q} \neq b_{j+q}$. Without loss of generality we can suppose $a_{i+q} = 1$. Hence,

$$(5.29) \quad a_i = b_j ,\dots, a_{i+q-1} = b_{j+q-1} .$$

(5.27), (5.28) and (5.29) imply for $0 < q' \leq q$

$$l(C_3) = i+q' \Longrightarrow l(\varphi^t(C_3)) = j+q', r(C_3) = i+q'$$
$$(5.30) \quad \Longrightarrow r(\varphi^t(C_3)) = j+q', \; r(C_2) = i+q' \Longrightarrow r(\varphi^t(C_2)) =$$
$$j+q', r(C_1) = i+q' \Longrightarrow r(\varphi^t(C_1)) = j+q',$$

In particular, we have a_{i+q} is contained in a 3-block if and only if b_{j+q} contained in a 3-block. Thus (5.29) and (5.30) give a contradiction. For example, if $a_{i+q} = 1 = C_1$ is a 1-block, then $b_{j+q} = \varphi^t(C_1) = 0$ is a 1-block. This gives a contradiction since b_{j+q} is not contained in any 3-block. Without loss of generality we can suppose $i \geq j$. We have therefore proved that $a_i = b_j,\dots,a_n = b_{j+(n-i)}$. By (5.30) $n = r(\hat{B}_3) = r(\varphi^t(\hat{B}_3)) = j+n-i$. Hence, $j=i$ and $E = G$.

$D = F$ is proved in the same way by using $\bar{d}(B_2,C_3) = \bar{d}(\varphi^t(B_2),\varphi^t(C_3)), d(B_2,C_3) = d(\varphi^t(B_2),\varphi^t(C_3)), d(B_2,C_2) = d(\varphi^t(B_2),\varphi^t(C_2))$ and $d(B_2,C_1) = d(\varphi^t(B_2),\varphi^t(C_1))$.

<u>Proof of Lemma 3.16</u>: If $\varphi^r(A) = \varphi^s(A)$, the Lemma is tri-

vial. We suppose $\varphi^r(A) \neq \varphi^s(A)$. If there exists an i such that $d(\varphi^{r+i}(B_1),\varphi^{r+i}(B_2)) = d(\varphi^{s+i}(B_1,\varphi^{s+i}(B_2))$, we get by Lemma 3.15 that $\varphi^{r+i}(A) = \varphi^{s+i}(A)$. Hence, $\varphi^r(A) = \varphi^s(A)$ which is a contradiction. Therefore $d(\varphi^{r+i}(B_1),\varphi^{r+i}(B_2)) \neq d(\varphi^{s+i}(B_1),\varphi^{s+i}(B_2))$ for all i .
We observe by Lemma 3.14 a): If $\varphi^i(B_1)$ and $\varphi^i(B_2)$ do not meet by applying φ , $d(\varphi^i(B_1),\varphi^i(B_2))$ "decreases" by 0 or 1 . Hence:

(5.31) If $d(\varphi^{s+i}(B_1),\varphi^{s+i}(B_2)) > d(\varphi^{r+i}(B_1),\varphi^{r+i}(B_2))$, $\varphi^{r+i}(B_1)$ meets $\varphi^{r+i}(B_2)$ "before" $\varphi^{s+i}(B_1)$ meets $\varphi^{s+i}(B_2)$, else $\varphi^{s+i}(B_1)$ meets $\varphi^{s+i}(B_2)$ "before" $\varphi^{r+i}(B_1)$ meets $\varphi^{r+i}(B_2)$.

We suppose $t_1,\dots,t_q (q < c)$ are the integers such that $\varphi^{r+t_i}(B_1)$ meets $\varphi^{r+t_i}(B_2)$ by applying φ . We prove the following 3 claims by using (5.31):

(5.32) $\varphi^s(B_1)$ meets $\varphi^s(B_2)$ at most once by applying φ^{t_1+1} .

(5.33) $\varphi^{s+t_i+1}(B_1)$ meets $\varphi^{s+t_i+1}(B_2)$ once by applying $\varphi^{t_{i+1}-t_i}$.

(5.34) $\varphi^{s+t_q+1}(B_1)$ meets $\varphi^{s+t_q+1}(B_2)$ at most once by applying φ^{t-t_q-1} .

The Lemma now follows easily from (5.32), (5.33) and (5.34).

Proof of (5.32): If $d(\varphi^s(B_1),\varphi^s(B_2)) > d(\varphi^r(B_1),\varphi^r(B_2))$, then $\varphi^s(B_1)$ does not meet $\varphi^s(B_2)$ by applying φ^{t_1+1} . Otherwise, let y be the least integer such that $\varphi^s(B_1)$ meets $\varphi^s(B_2)$ by applying φ^y . Then

$d(\varphi^{s+y}(B_1),\varphi^{s+y}(B_2)) > d(\varphi^{r+y}(B_1),\varphi^{r+y}(B_2))$, and $\varphi^{r+y}(B_1)$ meets $\varphi^{r+y}(B_2)$ "before" $\varphi^{s+y}(B_1)$ meets $\varphi^{s+y}(B_2)$.

Proof of (5.33): Let y be the least integer such that $\varphi^{s+t_i+1}(B_1)$ meets $\varphi^{s+t_i+1}(B_2)$ by applying φ^y . Then $d(\varphi^{s+t_i+1+y}(B_1),\varphi^{s+t_i+1+y}(B_2)) > d(\varphi^{r+t_i+1+y}(B_1),\varphi^{r+t_i+1+y}(B_2))$, and $\varphi^{r+t_i+1+y}(B_1)$ meets $\varphi^{r+t_i+1+y}(B_2)$ "before" $\varphi^{s+t_i+1+y}(B_1)$ meets $\varphi^{s+t_i+1+y}(B_2)$.

The proof of (5.34) is analogous.

The proof of Lemma 3.17 follows from the proof of Lemma 5.8.

The proof of Lemma 3.18 is obvious since each 2-block meets each 3-block a times, each 1-block meets each 2-block c times and $A = \varphi^s(A)$.

INDEX OF NOTATION

REFERENCES

1. E.R. BERLEKAMP, "Algebraic Coding Theory", McGraw-Hill, New York, 1968.

2. K. KJELDSEN, On the cycle structure of a set of nonlinear shift registers with symmetric feedback functions, J. Combinatorial Theory, Ser. A. 20 (1976). 154-169.

3. J. SØRENG, The periods of the sequences generated by some symmetric shift registers, J. Combinatorial Theory, Ser. A. 21 (1976), 164-187.