PACIFIC JOURNAL OF MATHEMATICS
Vol. 85, No. 1, 1979

SYMMETRIC SHIFT REGISTERS

JAN SØRENG

We will study symmetric shift registers over the field $GF(2) = \{0, 1\}$. The symmetric shift register $\theta_S: \{0, 1\}^n \to \{0, 1\}^n$ corresponding to a symmetric polynomial $S(x_2, \cdots, x_n)$ is defined by

$$\theta_S(a_1, \cdots, a_n) = (a_2, \cdots, a_{n+1}) \text{ where } a_{n+1} = a_1 + S(a_2, \cdots, a_n) .$$

p is a period of $A \in \{0, 1\}^n$ with respect to θ_S if $\theta_S^p(A) = A$. If p is the least period of A, then $A \to \theta_S(A) \to \cdots \to \theta_S^p(A) = A$ is the cycle corresponding to A. This is the first of two papers where we will determine in a constructive way (for each S):

1. **The minimal period for each $A \in \{0, 1\}^n$.**
2. **The possible minimal periods.**
3. **The number of cycles corresponding to each minimal period.**

Kjeldsen [1] and the author ([2], [3]) have earlier proved some partial results about these symmetric shift registers. In this paper we will define a block structure for each $A \in \{0, 1\}^n$ and study how this block structure alter by applying θ_S. This will be the basis for the forthcoming paper. Moreover, as an easy application we will for each A find a period (not necessarily the least). This application demonstrates how the block structure can be used. By refining the proof of this application we will determine the minimal periods in the next paper.

Now we give a summary of the paper. In §2 we introduce some notation and mention how the problems are reduced to the case $S = E_k + \cdots + E_{k+p}$ where E_i is defined by $E_i(a_2, \cdots, a_n) = 1$ if and only if $a_2 + \cdots + a_n = i$.

In §3 we define the block structure for each $A \in \{0, 1\}^n$ and formulate Theorem 3.2 which determines periods. In §4 we prove that A is uniquely determined by its block structure. Moreover, we study how this block structure change by applying θ_S. We also prove Theorem 3.2 by finding a p such that the block structure of respectively A and $\theta_S^p(A)$ are equal. In the end of §4 we mention how the lemmas will be used in the forthcoming paper. In §5 we prove some of the lemmas in §4.

The author is grateful to Kjell Kjeldsen who inspired him to study symmetric shift registers.

2. Preliminaries.

First we introduce some notations: a, b, c, d

denote the integers $\in \{0, 1\}$. $e, f, g, \cdots$ denotes the integers $\geqq 0$. We denote finite sequences of the integers 0 and 1 by capital letters (also the empty sequence). The letter B will always denote a block (Definition 3.1).

For $s \in \{0, 1, \cdots\}$ we define $s(A) = A \cdots A$ where A appears s times.

We let $1_t = 1 \cdots 1$(resp. $O_t = 0 \cdots 0$) denote a string of t consecutive 1's(resp. 0's).

We denote $\bar{a} = (a_1, \cdots, a_n) \in \{0, 1\}^n$ also by $\bar{a} = a_1 \cdots a_n$. The weight $w(\bar{a})$ of a vector $\bar{a} = (a_1, \cdots, a_n)$ is defined by $w(\bar{a}) = \sum_{i=1}^{n} a_i$.

Suppose $A = a_1 \cdots a_n$ and $C = a_i \cdots a_j$ is a piece of A. We define the left (resp. the right) position of C by $l(C) = i$(resp. $r(C) = j$).

Moreover, we refer to the index of notation. Next we formulate Lemma 2.1 and Theorem 2.2 in [2]. These results reduce the problem to the case $S = E_k + \cdots + E_{k+p}$. Let S_p be the homogeneous symmetric polynomial of degree p in the variables $x_2, \cdots, x_n$. Then we have ([2, Lemma 2.1])

$$S_p = \sum_{k=0}^{n-1} \binom{k}{p} (\mathrm{mod}\ 2) E_k$$

where $\binom{k}{p}$ denotes the binomial coefficient. We define intervals in the set of the integers Z in the usual way by

$$[q, t] = \{i: i \in Z \quad \text{and} \quad q \leqq i \leqq t\} .$$

Let S be the symmetric polynomial in the variables $x_2, \cdots, x_n$ 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 $i \in \{1, \cdots, f-1\}$. Then we have by [2, Theorem 2.2]:

If $w(\bar{a}) \in [q_i, t_i + 1]$ for some i, the periods of $\bar{a}$ with respect to respectively the difference equation $x_{n+1} = x_1 + S(x_2, \cdots, x_n)$ and $x_{n+1} = x_1 + (E_{q_i} + \cdots + E_{t_i})(x_2, \cdots, x_n)$ are equal.

Otherwise, the periods of $\bar{a}$ with respect to the difference equation $x_{n+1} = x_1 + S(x_2, \cdots, x_n)$ and $x_{n+1} = x_1$ are equal.

Theorem 3.2 solve the case $S = E_k + \cdots + E_{k+p}$. For each symmetric S we can therefore determine a period for each $A \in \{0, 1\}^n$.

3. The main definition and a theorem.

The main concept in this paper is the blocks of $A \in \{0, 1\}^n$. We define the blocks with respect to p in A by an inductive procedure. Roughly, the blocks are defined as follows:

(1) For $1 \leqq i \leqq p$, i consecutive 1's is an i-block.

(2) More than p consecutive 1's constitute a $(p+1)$-block. This is the correct definition if the distances between the blocks are "sufficiently" large. Here is an example with $p = 4$

$$A = 0\underbrace{11}_{\text{2-block}}0000\underbrace{111}_{\text{3-block}}0000\underbrace{11111}_{\text{5-block}}0000000\underbrace{11111}_{\text{5-block}}11$$

The general definition is more complicated. The main difficulty is that the blocks can contain subblocks.

An example will illustrate this point: We let $\theta = \theta_S$ where $S = E_3 + E_4$, and

$$A = 00011110\overset{*}{0}01000$$

By direct calculation or by using Lemma 4.3 in [2] we can prove

$$\begin{aligned}
\theta^{n+2}(A) &= 000\underline{11110}\overset{*}{0}10000\\
\theta^{2(n+2)}(A) &= 0001\underline{1111}\overset{*}{0}100000\\
\theta^{3(n+2)}(A) &= 00011\underline{110}\overset{*}{1}100000\\
\theta^{4(n+2)}(A) &= 000\underline{11011}\overset{*}{1}00000\\
\theta^{5(n+2)}(A) &= 000\overset{*}{1}\underline{0111}100000\\
\theta^{6(n+2)}(A) &= 00\overset{*}{1}\underline{00111}100000\\
\theta^{7(n+2)}(A) &= 0\overset{*}{1}\underline{0001111}00000\\
\theta^{8(n+2)}(A) &= \overset{*}{1}\underline{0000111}100000\\
\theta^{8(n+2)+2}(A) &= 000\underline{11110000}\overset{*}{0}01\\
&\vdots\\
\theta^{11(n+2)+2}(A) &= 000\underline{11110}00\overset{*}{0}1000
\end{aligned}$$

We have underlined the 2-blocks in our example and put a * above the 1-blocks where the blocks are defined as in Def. 3.1. The example also gives an indication of how we can determine the period of A by studying the movement of the blocks. We need more nota tion. If $A = a_1 \cdots a_n$ and $i \leqq j$, we define

$$f_i^A(j) = (\text{the number of 1's in } a_i \cdots a_j) - (\text{the number of 0's in } a_i \cdots a_j)\,. \tag{3.1}$$

If $C = a_s \cdots a_t$, then we define

$$f^A(C) = f_s^A(t)\,. \tag{3.2}$$

Moreover, we let f_C^A denote $f_{l(C)}^A$. When there is no room for misinterpretation, we write $f = f^A$.

(3.3) $t \in D$ means $t \in [l(D), r(D)]$.

(3.4) $C < D$ means that C is contained in D and $C \neq D$.

Now we will define the blocks. That a block B_i is on level i will mean that the block is contained in a chain of blocks

(3.5) $B_1 > B_2 \cdots > B_{i-1} > B_i$ where B_j is on level j.

We divide the definition of the blocks into two parts by first defining 1-structures and 0-structures of A. A 1-structure (0-structure) is a generalization of q consecutive 1's (respectively 0's) which is succeeded by q 0's (respectively 1's). $a \wedge b$ denotes the minimum of a and b.

DEFINITION 3.1, part 1. Suppose $A = a_1 \cdots a_n \in \{0, 1\}^n$.

(a) Suppose $a_r = 1$. Let s be the maximal integer such $D = a_r \cdots a_s$ satisfies

(1) $0 < f(a_r \cdots a_i) \leqq f(a_r \cdots a_s)$ for $i \in \{r, \cdots, s\}$

and

(2) If $r \leqq i \leqq j \leqq s$, then $f(a_i \cdots a_j) > -(p+1)$.

By definition D is a 1-structure with respect to p.

(b) Suppose $a_r = 0$. Let s be the maximal integer such that $D = a_r \cdots a_s$ satisfies

$$0 > f(a_r \cdots a_i) \geqq f(a_r \cdots a_s) \quad \text{for} \quad i \in \{r, \cdots, s\}.$$

By definition D is a 0-structure.

DEFINITION 3.1, part 2. (a) Suppose $A = a_1 \cdots a_n \in \{0, 1\}^n$. We define the blocks in A with respect to p by induction with respect to the level of the blocks in the following way: (The 1-structures are defined with respect to p.)

Level 1. We decompose A in the following way $A = 0_{i_1} B_1 0_{i_2} \cdots B_m 0_{i_{m+1}}$ where B_j is a 1-structure. By definition $B_1, \cdots, B_m$ are the blocks in A on level 1.

Level 2. Suppose B is a block on level 1. We decompose B in the following way

(3.6) $B = 1_{i_1} B_1 1_{i_2} B_2 \cdots B_m 1_{i_{m+1}}$ where B_j is a 0-structure.

By definition $B_1, \cdots, B_m$ are the blocks in A on level 2 which are contained in B.

Level 3. Suppose B is a block on level 2. We decompose B in the following way

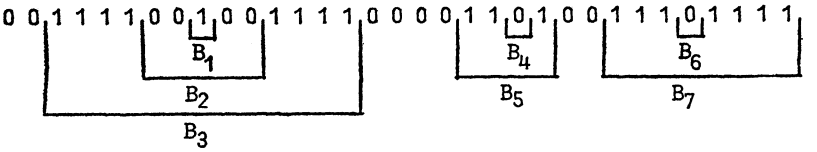
(3.7) $\quad B = 0_{i_1}B_1 0_{i_2}B_2 \cdots B_m 0_{i_{m+1}}$ where B_j is a 1-structure .

By definition $B_1, \cdots, B_m$ are the blocks in A on level 3 which are contained in B.

We continue in this way. If $i \in \{3, 5, 7, \cdots\}$ and B is a block on level i, we decompose B as in (3.6). If $i \in \{4, 6, 8, \cdots\}$ and B is a block on level i, we decompose B as in (3.7).

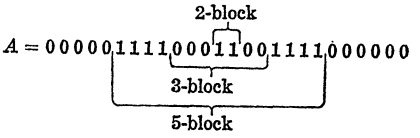
(b) Let B be a block in A on level i. Then we define level$(B)=i$, type$(B)=|f(B)|\wedge(p+1)$ and $m(B)=|f(B)|$. Moreover, if type$(B)=q$ we say that B is a q-block or that B is a block of type q.

Here is an example with $p = 3$.



type(B_1) = type(B_4)=type(B_6)=1, type(B_5)=2, type(B_2)=3, type(B_3)= type(B_7)=4, level(B_3) = level(B_5) = level(B_7) = 1, level(B_2) = level(B_4)= level(B_6) = 2 and level(B_1) = 3.

We observe that the decomposition in (3.5) is unique and that type(B_j) > type(B_{j+1}) for $j = 1, \cdots, i-1$. Here is an example with $p = 4$



The main part of our proofs is how the blocks move by applying $\theta_{E_k+\cdots+E_{k+p}}$. We will get that the movement of a j-block, where $j < p+1$, can be characterized by an equation (j).

We associate p equations to A as follows:

Let γ_j = the number of j-blocks in A with respect to $p(j = 1, \cdots, p+1)$. Let

$$\alpha_j = n + j - \sum_{i=1}^{p+1} 2 \min\{i, j\} \cdot \gamma_i \, .$$

We define the equations (1)—(p) as follows:

(p): $\quad \alpha_p X_p = Y \, .$

$$
\begin{aligned}
&(\text{p}-1): \quad \alpha_{p-1}X_{p-1} = 2Y + 2\gamma_p X_p \,. \\
&(\text{p}-2): \quad \alpha_{p-2}X_{p-2} = 3Y + 2\gamma_{p-1}X_{p-1} + 4\gamma_p X_p \,. \\
&(\text{p}-3): \quad \alpha_{p-3}X_{p-3} = 4Y + 2\gamma_{p-2}X_{p-2} + 4\gamma_{p-1}X_{p-1} + 6\gamma_p X_p \,. \\
&\qquad\qquad\qquad\qquad \vdots \\
&(1): \qquad \alpha_1 X_1 = pY + (2\gamma_2 X_2 + \cdots + 2(p-1)\gamma_p X_p) \,.
\end{aligned}
$$

If $\gamma_i = 0$, we replace equation (i) by $X_i = 0$. In this way we obtain a system of p equations associated with A and with respect to p, i.e. for $j \in \{1, \cdots, p\}$ the equation (j) is defined by

$$
\begin{aligned}
&\alpha_j X_j = (p + 1 - j)Y + \sum_{i=j+1}^{p} 2\gamma_i(i-j)X_i \qquad \text{if} \quad \gamma_j \neq 0 \,. \\
&X_j = 0 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \text{if} \quad \gamma_j = 0 \,.
\end{aligned}
$$

Suppose k, p and n satisfies $0 < k \leqq k + p < n$. We define as in the introduction $\theta(x_1, \cdots, x_n) = \theta_{E_k+\cdots+E_{k+p}}(x_1, \cdots, x_n) = (x_2, \cdots, x_{n+1})$ where

$$
x_{n+1} = x_1 + (E_k + \cdots + E_{k+p})(x_2, \cdots, x_n) \,.
$$

We say that PER is a period for $A \in \{0, 1\}^n$ with respect to θ if $\theta^{PER}(A) = A$.

THEOREM 3.2. *We determine the periods with respect to* $\theta = \theta_{E_k+\cdots+E_{k+p}}$ *in this way:*

Let $A \in \{0, 1\}^n$ *and* $w(A) = k + p + 1$. *Suppose* A *contains* γ_i *i-blocks with respect to* p *for* $i = 1, \cdots, p + 1$.

(a) *Suppose* $\gamma_{p+1} \neq 0$ *and* $\gamma_i \neq 0$ *for an integer* $i < p + 1$. *Suppose* $Y, X_1, \cdots, X_p$ *are positive integers satisfying the system of equations associated with* A *and with respect to* p. *Then*

$$
PER = (n + p + 1)Y + \sum_{i=1}^{p} 2 \cdot i \cdot \gamma_i \cdot X_i
$$

is a period for A.

(b) *If there exists only one* j *such that* $\gamma_j \neq 0$, *then* $PER = n + j$ *is period for* A.

We prove this theorem in §§4 and 5. If $w(A) = \sup_i w(\theta^i(A))$, we can always suppose $w(A) = k + p + 1$ and $\gamma_{p+1} \neq 0$ by Lemma 5.6 (b) and (a) respectively.

By putting $Y = \alpha_1 \cdots \alpha_p$ we get a solution of the system of the equations in Theorem 3.2. Moreover, it is very easy to see that a least solution exists: Suppose $Y, X_1, \cdots, X_p$ and $Y^*, X_1^*, \cdots, X_p^*$ are two solutions and that $Y \leqq Y^*$. By equation (p) we observe that

$X_p \leqq X_p^*$, by equation (p—1) we then get $X_{p-1} \leqq X_{p-1}^*$ and etc. The least solution can be obtained in this way: $X_p^p = 1$ and $Y^p = \alpha_p$ is the least solution of equation (p). Let r be the least integer r such that $t = (2Y^p + 2\gamma_p X_p^p) \cdot r/\alpha_{p-1}$ is an integer. Put $Y^{p-1} = r \cdot Y^p$, $X_p^{p-1} = r \cdot X_p^p$ and $X_{p-1}^{p-1} = t$. Then X_{p-1}^{p-1}, X_p^{p-1} and Y^{n-1} is the least solution of the equations (p) and (p—1). By continuing in this way we will finally obtain the least solution $Y^1, X_1^1, \cdots, X_p^1$ of all the equations.

4. **The properties of the block structure.** In this section we will introduce a lot of lemmas about the block structure and prove Theorem 3.2.

The Lemmas 4.4, 4.6, 4.7, 4.8, 4.10, 4.11, 4.12 and 4.13 are proved it the next section.

First we define a measure d which measures how much to the left a block is in $A \in \{0, 1\}^n$. We do the convention that B always denotes a block. $s \wedge t$ denotes the minimum of s and t. For $1 \leqq s \leqq t \leqq n$ and $A = a_1 \cdots a_n \in \{0, 1\}^n$ we define

$$d_q(A, s, t) = d_q(a_s \cdots a_t) = t - s + 1 - \sum \{q \wedge \text{type}(B^*): s \leqq l(B^*) \leqq t\} - \sum \{q \wedge \text{type}(B^*): s \leqq r(B^*) \leqq t\} .$$

If B is a block such that $\text{type}(B) = q$ and $l(B) > 1$, then we define

$$d(B) = d_q(a_1 \cdots a_{l(B)-1}) .$$

We observe that $d_q(B)$ and $d(B)$ are different by definition. Moreover, if $l(B) = 1$, then we define $d(B) = 0$. This measure is very important.

The next two lemmas describe some of the properties of the block structure. For example, Lemma 4.1 gives for one thing that each $A \in \{0, 1\}^n$ is uniquely determined by its block structure.

LEMMA 4.1. (a) *Suppose* $w(A) = k + p + 1$ *and* A *contains* γ_i *i-blocks* ($i = 1, \cdots, p + 1$).

$$(1) \quad \begin{cases} \text{There exists } m \geqq 0 \text{ such that } m + \sum_{i=1}^{p+1} i \cdot \gamma_i = k + p + 1 \\ \text{and } m + 2 \cdot \sum_{i=1}^{p+1} i \cdot \gamma_i \leqq n + p + 1 . \end{cases}$$

Suppose $B_1^i, \cdots, B_{\gamma_i}^i$ *are the i-blocks in A numbered from left to right. We put* $t_j^i = d(B_j^i)(i = 1, \cdots, p + 1; j = 1, \cdots, \gamma_i)$ *and* $t_j^{p+2} = m(B_j^{p+1}) - (p + 1)$ *where* $m(B) = |f(B)|$ *as in Definition* 3.1. *Then we have*

$$(2)\quad \begin{cases} 0 \leqq t_1^i \leqq \cdots \leqq t_{\gamma_i}^i \leqq \alpha_i & \text{for } i = 1, \cdots, p\ . \\ 0 \leqq t_j^{p+1},\ 0 \leqq t_j^{p+2} & \text{for } j = 1, \cdots, \gamma_{p+1}\ . \\ t_j^{p+1} + t_j^{p+2} \leqq t_{j+1}^{p+1} & \text{for } j = 1, \cdots, \gamma_{p+1} - 1 \text{ and} \\ t_{\gamma_{p+1}}^{p+1} + t_{\gamma_{p+1}}^{p+2} \leqq \alpha_{p+1}\ . & \\ t_1^{p+2} + \cdots + t_{\gamma_{p+1}}^{p+2} = m\ . & \end{cases}$$

(b) *Suppose* m, γ_i *and* t_i^j *satisfy* (1) *and* (2) *in* (a). *Then there exists one and only one* $A \in \{0, 1\}^n$ *such that* $w(A) = k + p + 1$ *and all blocks in* A *can be numbered by* (*from left to right*) $B_j^i (i = 1, \cdots, p + 1;\ j = 1, \cdots, \gamma_i)$ *such that type*$(B_j^i) = i$, $t_j^i = d(B_j^i) (i = 1, \cdots, p + 1;\ j = 1, \cdots, \gamma_i)$ *and* $t_j^{p+2} = m(B_j^{p+1}) - (p + 1)$ *for* $j = 1, \cdots, \gamma_{p+1}$.

(c) *By definition* m, γ_i *and* t_i^j *satisfy* (2)′ *if and only if* m, γ_i *and* t_i^j *satisfy* (2), $t_1^i > 0$ *for* $i = 1, \cdots, p$ *and* $t_{\gamma_{p+1}}^{p+1} + t_{\gamma_{p+1}}^{p+2} = \alpha_{p+1}$.

If $w(A) = k + p + 1$, A *ends with a* $(p + 1)$*-block and starts with* 0 *or a* $(p + 1)$*-block, then* m, γ_i *and* t_i^j *in* (a) *satisfy* (1) *and* (2)′.

If m, γ_i *and* t_i^j *satisfy* (1) *and* (2)′, *the corresponding* $A \in \{0, 1\}^n$ *in* (b) *ends with a* $(p + 1)$*-block and starts with* 0 *or a* $(p + 1)$*-block.*

Proof of (a) *and* (b). We suppose first that A ends with a $(p + 1)$-block denoted by B_{END}. We call a piece $0_i1_i = B_i1_i$(respectively $1_i0_i = B_i0_i$) of A, such that $B_i = 0_i$(resp. $B_i = 1_i$) is an i-block in A, an i-component of A. We decompose A in this way:

$$A = K_1(A) \longrightarrow K_2(A) \longrightarrow \cdots \longrightarrow K_{p+1}(A)$$

where $K_{i+1}(A)$ is constructed by removing all the i-components in $K_i(A)$. $K_i(A)$ will only contain blocks of type $\geqq i$. To each q-block B there corresponds a chain of q-blocks

$$B = K_1(B) \longrightarrow \cdots \longrightarrow K_q(B)$$

where $K_{i+1}(B)$ is constructed by removing all the i-components in $K_i(B)$. By the definitions of $m(B)$ and $d(B)$ we get easily $m(K_i(B)) = m(B)$, type$(K_i(B))$ = type(B) and $d(K_i(B)) = d(B)$.

By the decomposition method we get

$$\text{the length of } K_{p+1}(A) = n - 2\sum_{i=1}^{p} i \cdot \gamma_i\ .$$

$$\text{the number of 1's in } K_{p+1}(A) = k + p + 1 - \sum_{i=1}^{p} i \cdot \gamma_i\ .$$

We put $m = t_1^{p+2} + \cdots + t_{\gamma_{p+1}}^{p+2}$. Since $K_{p+1}(A)$ only contains $(p + 1)$-blocks we observe

the length of $K_{p+1}(A) = l(K_{p+1}(B_{END})) - 1 + m(B_{END})$.

The number of 1's in $K_{p+1}(A) = m + (p+1)\gamma_{p+1}$. By combining these equations we get

$$n - 2\sum_{i=1}^{p} i\cdot\gamma_i = l(K_{p+1}(B_{END})) - 1 + m(B_{END}) . \tag{4.1}$$

$$k + p + 1 - \sum_{i=1}^{p} i\cdot\gamma_i = (p+1)\gamma_{p+1} + m .$$

Now we will prove (1). The last equality implies $m + \sum_{i=1}^{p+1} i\cdot\gamma_i = k + p + 1$. We observe that

$$\begin{aligned} &l(K_{p+1}(B_{END})) - 1 \\ &\quad \geqq \sum \{m(K_{p+1}(B)) + (p+1) \colon \text{type}(B) = p+1 \text{ and } B \neq B_{END}\} \\ &\quad = m + (p+1)(2\gamma_{p+1} - 1) - m(B_{END}) . \end{aligned}$$

Hence, by (4.1)

$$n - 2\sum_{i=1}^{p} i\cdot\gamma_i = l(K_{p+1}(B_{END})) - 1 + m(B_{END}) \geqq m + (p+1)(2\gamma_{p+1} - 1)$$

and (1) follows. Now we do some observations. Suppose C is an i-component which we remove from $K_i(A)$. There are three possibilities:

1. If $K_i(A) = C\cdots$, then $C = 1_i0_i$.
2. If $K_i(A) = \cdots C$, then $C = 0_i1_i$.
3. Suppose $K_i(A) = \cdots C \cdots$. If there is a 1 in position $l(C) - 1$, then $C = 0_i1_i$; otherwise $C = 1_i0_i$. Moreover, $l(C) - 1$ is not among the first i positions in a block and not either among the i positions which succeed a block of type $> i$.

Moreover, we observe

$$\begin{aligned} \alpha_i &= n + i - 2\cdot\sum_{j=1}^{i} j\cdot\gamma_j - 2i\cdot(\text{the number of blocks in } K_{i+1}(A)) \\ &= \left(n - 2\cdot\sum_{j=1}^{i} j\cdot\gamma_j\right) - i\cdot(2\cdot\text{the number of blocks in } K_{i+1}(A) - 1) . \end{aligned}$$

Hence,

$$\alpha_i = \text{the length of } K_{i+1}(A) - i\cdot(2\cdot\text{the number of blocks in } K_{i+1}(A) - 1) . \tag{4.2}$$

By using these observations we will now construct $K_i(A)$ from $K_{i+1}(A)$. We must put each i-block in between the right positions in $K_{i+1}(A)$. We pass over the first i-positions in each block and the

i-positions which succeed each block in $K_{i+1}(A)$. We number the remaining positions from left to right by $1, \cdots, \alpha_i$ (the number of enumerated positions is α_i by (4.2)). Suppose B is an i-block in A such that $0 \leqq d(B) \leqq \alpha_i$. We consider the following 3 possibilities:

1. If $d(B) = 0$, we put 1_i0_i in the front of $K_{i+1}(A)$. Then $K_i(B) = 1_i$.

2. Suppose $0 < d(B) < \alpha_i$. Suppose position r in $K_{i+1}(A)$ is numbered by $d(B)$. If there is a 1 (resp. 0) in position r, we put 0_i1_i(resp. 1_i0_i) in between the positions r and $r+1$ in $K_{i+1}(A)$. Then $K_i(B) = 0_i$(resp. $K_i(B) = 1_i$).

3. If $d(B) = \alpha_i$, we put 0_i1_i in the end of $K_{i+1}(A)$. Then $K_i(B) = 0_i$. (The last position in $K_{i+1}(A)$ is always numbered by α_i.)

If there are several i-blocks B such that $d(B) = q$, we put the i-components corresponding to these blocks in between the same positions.

Now we prove that this construction method is correct. Suppose we are in Case 2 (we treat Cases 1 and 3 analogously). We observe that position r is numbered by

$$\begin{aligned} r - i \cdot &(\text{the number of end positions of blocks } \in \{1, \cdots, r\}) \\ &= d_i(K_{i+1}(A), 1, r) . \end{aligned}$$

Wherever we put the other i-blocks into $K_{i+1}(A)$ we get $d(K_i(B)) = d_i(K_{i+1}(A), 1, r)$. Hence,

$$d(K_i(B)) = \text{the integer which position } r \text{ is numbered by} = d(B) .$$

We observe that $0 \leqq d(B) \leqq \alpha_i$ for all i-blocks. If $d(B) < 0$ or $d(B) > \alpha_i$, there is not any appropriate place where we can put $K_i(B)$ into $K_{i+1}(A)$.

We will now prove (2). $0 \leqq t_1^i \leqq \cdots \leqq t_{\gamma_i}^i \leqq \alpha_i$ follows easily. By definition $m = t_1^{p+2} + \cdots + t_{\gamma_{p+1}}^{p+2}$. The remaining claims in (2) follows by studying $K_{p+1}(A)$. We let $l(C)$ denote the left position of C relatively $K_{p+1}(A)$. Let

$$s = l(K_{p+1}(B_j^{p+1})) \quad \text{and} \quad t = l(K_{p+1}(B_{j+1}^{p+1})) - 1 .$$

Then we observe that

$$d_{p+1}(K_{p+1}(A), s, t) \geqq m(K_{p+1}(B_j^{p+1})) - (p+1) = t_j^{p+2} .$$

Hence,

$$t_{j+1}^{p+1} = d(K_{p+1}(B_{j+1}^{p+1})) = d(K_{p+1}(B_j^{p+1})) + d(K_{p+1}(A), s, t) \geqq t_j^{p+1} + t_j^{p+2} .$$

Moreover,

$$\begin{aligned}\alpha_{p+1} &= \text{the length of } K_{p+1}(A) - (p+1)(2\gamma_{p+1}-1)\\ &= [l(K_{p+1}(B_{END})) - 1] + m(B_{END}) - (p+1)(2\gamma_{p+1}-1)\\ &= d(B_{END}) + [m(B_{END}) - (p+1)] = t_{\gamma_{p+1}}^{p+1} + t_{\gamma_{p+1}}^{p+2}\end{aligned}$$

and (2) is proved.

(b) follows by constructing A step by step: $K_{p+1}(A) \to \cdots K_2(A) \to K_1(A) = A$ as in the proof of (a). The uniqueness follows from the construction method.

Finally we suppose that A does not end with a $(p+1)$-block. We define $A^* = A0_{p+1}1_{p+1}$. By using the lemma on A^* it is easily seen that the lemma is true for A. For example, we prove $d(B) \leqq \alpha_i$ in the following way:

If A does not end with a 1-block, then $K_2(A^*)$ obviously ends with $0_{p+1}1_{p+1}$. Next we suppose A ends with s 1-blocks. Then A^* has the form

$$A^* = \cdots 001010 \cdots 1010_{p+1}1_{p+1} = \cdots \overset{*}{0}0s(10)0_p1_{p+1}\,.$$

In the construction of $K_2(A^*)$ $s(10)$ is removed. Moreover, the 0 marked by a * is maybe removed. In any way $K_2(A^*)$ will end with $0_{p+1}1_{p+1}$. In the same way we prove that $K_{i+1}(A^*)$ always ends with $0_{p+1}1_{p+1}$. Moreover, the number of positions in $0_{p+1}1_{p+1}$ which we enumerate is at least $2\cdot(p+1-i)$ when we construct $K_i(A^*)$. Hence, if type$(B) = i$, then

$$d(B) \leqq \alpha_i^* - 2(p+1-i) = \alpha_i$$

where α_i^* is "α_i relatively A^*".

Proof of (c). Suppose A ends with a $(p+1)$-block and starts with 0 or a (p + 1)-block. We observe: If $d(B) = 0$ for some B with type$(B) < p+1$, then A must start with some block of type $< p+1$. Hence, $d(B) > 0$ for type$(B) < p+1$. $t_{\gamma_{p+1}}^{p+1} + t_{\gamma_{p+1}}^{p+2} = \alpha_{p+1}$ is proved in the proof of (a) and (b). Hence, the first claim follows by using (a). The second claim in (c) follows analogously.

To illustrate the proof we study the example in §3 with $p = 3$:

$$A = 00111100100111100001101001111011111$$

contains 3 1-blocks (6, 14, 17), 1 2-block (9), 1 3-block (3) and 2 4-blocks (2, 3) where the distances of the blocks are in the round brackets.

We now construct $A = K_1(A) \to K_2(A) \to K_3(A) \to K_4(A)$. We underline the i-components in $K_i(A)$. We also number some of the positions in $K_i(A)$ as in the second part of the proof: We put a *

above the positions which we do not number. The remaining positions in $K_{i+1}(A)$ are numbered from 1, $\cdots$, α_i. We put the correct numbers above those positions corresponding to the i-blocks in A. If the components are put into $K_{i+1}(A)$ as in the proof, we observe that we get $K_i(A)$.

$$K_1(A) = 00111100100111100001101001110111$$
$$K_2(A) = \overset{*}{0}0111\overset{*}{1}0\overset{*6}{0}0111\overset{*}{1}0000\overset{*14*}{1}10\overset{*\ 17}{0}111111$$
$$K_3(A) = \overset{**}{0}0111\overset{**}{1}0\overset{**}{0}0111\overset{**}{1}0000\overset{9**}{1}11111$$
$$K_4(A) = \overset{***3}{0}0111\overset{***}{1}0000\overset{***}{1}11111$$

LEMMA 4.2. *Suppose* $A \in \{0, 1\}^n$, $w(A) = k + p + 1$ *and* $A = DE$. *We suppose that* D *has the form*

$$D = 0_{i_1}B_1C_1 \cdots 0_{i_r}B_rC_r0_{i_{r+1}}$$

where (for $1 \leqq i \leqq r$*)*B_i *is a block of type* $\leqq p$ *and* $0 > f_{C_i}(t) \geqq f(C_i) = -f(B_i)$ *for* $t \in C_i$.

Let $q \in \{1, \cdots, p + 1\}$. *We suppose* E *starts with a* 0 *or a block of type* $> q$. *Then for all block* B *such that type* $(B) = q$, *we get*:

$$d(B) \leqq d_q(D) \text{ for } B < D \text{ and } d(B) > d_q(D) \text{ for } B < E\,.$$

(In this lemma we admit $D = \varnothing$ or $E = \varnothing$.)

Proof. We only sketch the proof since no new ideas are involved. We decompose D and E as in the previous proof:

$$D = K_1(D) \longrightarrow \cdots \longrightarrow K_{p+1}(D)\,.$$
$$E = K_1(E) \longrightarrow \cdots \longrightarrow K_{p+1}(E)\,.$$

Since E starts with 0 or a block of type $> q$, it follows from the construction process that $d_E(B) > 0$ for $B < E$($d_E(B)$ is the distance of B relatively E). By induction it is easily proved that the number of positions in $K_{q+1}(D)$, which we enumerate, is $d_q(D)$. From these two claims the lemma follows.

The Lemmas 4.6-4.14 describe how the block structure change by applying θ. All these lemmas are proved in §5 and they are all a consequence of Lemma 5.1. Lemma 5.1 is the key lemma in this paper.

First we prove a lemma which shows how $\theta_{E_k+\cdots E_{k+p}}$ works. We need a definition:

If $a = 1$, then $a' = 0$. If $a = 0$, then $a' = 1$.

If $C = a_i \cdots a_j$, then $C' = a_i' \cdots a_j'$.

LEMMA 4.3. *Let* $A = a_1 \cdots a_n$ *and* $k \leqq w(A) \leqq k + p + 1$.

(a) *If* $k \leqq w(A) - f_1(t) \leqq k + p + 1$ *for* $t \leqq s$, *then* $\theta^s(A) = a_{s+1} \cdots a_n a_1' \cdots a_s'$.

(b) *If* $w(A) = k + p + 1$ *and* $a_1 \cdots a_s = 0_s$, *then* $\theta^s(A) = a_{s+1} \cdots a_n a_1 \cdots a_s$.

(c) *If* $w(A) = k$ *and* $a_1 \cdots a_s = 1_s$, *then* $\theta^s(A) = a_{s+1} \cdots a_n a_1 \cdots a_s$.

Proof. (b) and (c) are easily shown.

(a) We prove by induction with respect to t that

$$w(\theta^t(A)) = w(A) - f_1(t) \quad \text{and} \quad \theta^t(A) = a_{t+1} \cdots a_n a_1' \cdots a_t' .$$

We divide the basis step into 3 cases.

Case 1. $w(A) = k + p + 1$.

$k + p + 1 - f_1(1) = w(A) - f_1(1) \leqq k + p + 1$ implies $f_1(1) > 0$. Hence, $a_1 = 1$ and $w(a_2, \cdots, a_n) = k + p$. We get

$$a_{n+1} = a_1 + (E_k + \cdots + E_{k+p})(a_2, \cdots, a_n) = 1 + 1 = 0 = a_1' .$$

Case 2. $w(A) = k$.

$k \leqq w(A) - f_1(1) = k - f_1(1)$ implies $f_1(1) < 0$. Hence, $a_1 = 0$ and $w(a_2, \cdots, a_n) = k$. We get

$$a_{n+1} = a_1 + (E_k + \cdots + E_{k+p})(a_2, \cdots, a_n) = 0 + 1 = 1 = a_1' .$$

Case 3. $k < w(A) < k + p + 1$.

We get immediately $w(a_2, \cdots, a_n) \in \{k, \cdots, k + p\}$.

In all the cases $w(\theta(A)) = w(A) - f_1(1)$. The induction step is proved analogously.

When we prove Theorem 3.2(a) we reduce the problem by the following lemma:

LEMMA 4.4. *We suppose* $w(A) = k + p + 1$ *and* A *contains a* $(p + 1)$*-block. Then there exists an* i *such that* $\theta^i(A)$ *satisfies:*

(0) *The number of* j*-blocks in* A *and* $\theta^i(A)$ *is equal for* $j = 1, \cdots, p + 1$.

(1) $\theta^i(A)$ *ends with a* $(p + 1)$*-block.*

(2) $w(\theta^i(A)) = k + p + 1$.

(3) $\theta^i(A)$ *starts with* 0 *or a* $(p + 1)$*-block.*

(4) $\Sigma\{m(B)\colon \text{type}(B) = p+1 \text{ and } B \text{ block in } A\} = \Sigma\{m(B)\colon \text{type}(B) = p+1 \text{ and } B \text{ block in } \theta^i(A)\}$.

In the rest of §4, except Lemma 4.12, we therefore suppose that

$$\text{(4.3)} \qquad \begin{cases} A \text{ ends with a } (p+1)\text{-block.} \\ w(A) = k + p + 1\ . \\ A \text{ starts with 0 or a } (p+1)\text{-block.} \end{cases}$$

We denote the last $(p+1)$-block in A with B_{END}.

Now we will study how the blocks move and change by applying θ^n. We need more notation. We divide each $(p+1)$-block B into two parts $H(B)$ and $K(B)$ as follows

(4.4) $B = H(B)K(B)$ where $f_B(t) \leqq p+1$ for $t \in H(B)$ and $f_B(l(K(B))) = p+2$ or $K(B) = \varnothing$.

If type $(B) < p+1$, we put $H(B) = B$ and $K(B) = \varnothing$. Furthermore we associate to certain blocks B a tail as in the next definition.

DEFINITION 4.5. (a) We decompose A (by induction) such that

$$A = 0_{i_1}B_1T_10_{i_2} \cdots B_mT_m0_{i_{m+1}}B_{END}$$

where B_i is a block on level 1 and T_i is maximal with respect to (1) and (2):

(1) $0 > f_{T_i}(t) \geqq -\text{type}(B_i)$ for $t \in T_i$.

(2) $f(T_i) = -\text{type}(B_i)$.

We call T_i the tail of B_i.

(b) Suppose B is a $(p+1)$-block. We decompose $K(B)$ (by induction) such that

$$K(B) = 1_{i_1}B_1T_11_{i_2} \cdots 1_{i_m}B_mT_m1_{i_{m+1}}$$

where B_i is a block on level 2 and T_i is maximal with respect to (1) and (2):

(1) $0 < f_{T_i}(t) \leqq \text{type}(B_i)$.

(2) $f(T_i) = \text{type}(B_i)$.

We call T_i the tail of B_i.

Suppose B is a block in A. If $l(B) \in T$ where T is a tail, it is easy to see that B is contained in T. Furthermore, if $l(B) \in H(B_*)$ where B_* is a block, B is contained in $H(B_*)$. If B is a block we define as before

(4.5) $m(B) = |f(B)| = |(\text{the number of 1's in } B) - (\text{the number of 0's in } B)|$.

The next lemma gives us a bijective correspondence between the blocks in A and

$$\hat{A} = \theta^n(A)1_{p+1} \in \{0, 1\}^{n+p+1} . \tag{4.6}$$

LEMMA 4.6. *There is a bijective correspondence* $B \to \hat{B}$: {*the blocks in* A} $\to$ {*the blocks in* $\hat{A}$} *such that* $m(B) = m(\hat{B})$, $\text{type}(B) = \text{type}(\hat{B})$ *and:*

If B *has a tail* T, *then* $l(\hat{B}) = l(B) +$ (*the number of positions in* $H(B)$). $r(\hat{B}) = r(B) +$ (*the number of positions in* T). *Furthermore,*

$$l(\hat{B}_{END}) = l(B_{END}) + (\textit{the number of positions in } H(B_{END})) .$$
$$r(\hat{B}_{END}) = n + p + 1 .$$

Otherwise, $l(\hat{B}) = l(B)$ *and* $r(\hat{B}) = r(B)$.

LEMMA 4.7. *There exists an integer* $s > 0$ *such that* $\theta^{n+s}(A)$ *satisfies* (4.3).

Let s_A *be the least integer with this property. Then* $p + 1 \leqq s_A \leqq n$. *Besides every block in* $\hat{A}$ *is either contained in* $\hat{a}_1 \cdots \hat{a}_{s_A}$ *or* $\hat{a}_{s_A+1} \ldots \hat{a}_{n+p+1}$ *where* $\hat{A} = \hat{a}_1 \cdots \hat{a}_{n+p+1}$.

We define

$$\varphi(A) = \theta^{n+s_A}(A) . \tag{4.7}$$

(4.8) If B corresponds to a block $\hat{B}$ in $\hat{a}_1 \cdots \hat{a}_{s_A}$, we say that B and $\hat{B}$ circles around by φ.

The next lemma describe the block structure of $\varphi(A)$. In the proof of Theorem 3.2 we study $\varphi(A), \varphi^2(A), \cdots$. We will find a q such that the block structure of A is equal to the block structure of $\varphi^q(A)$. This will imply that $A = \varphi^q(A)$.

LEMMA 4.8. *There is a bijective correspondence* $\hat{B} \to \varphi(B)$: {*The blocks in* $\hat{A}$} $\to$ {*the blocks in* $\varphi(A)$} *such that* $\text{type}(\varphi(B)) = \text{type}(B)$, $m(\varphi(B)) = m(B)$ *and:*

If $\hat{B}$ *circles around by* φ, $l(\varphi(B)) = l(\hat{B}) - s_A + n$ *and* $r(\varphi(B)) = r(\hat{B}) - s_A + n$. *If* $\hat{B}$ *does not circle around and* $B \neq B_{END}$, *then* $l(\varphi(B)) = l(\hat{B}) - s_A$ *and* $r(\varphi(B)) = r(\hat{B}) - s_A$. $l(\varphi(B_{END})) = l(\hat{B}_{END}) - s_A$ *and* $r(\varphi(B_{END})) = n$.

The next lemmas describe how $d(B)$ change by applying the shift register. To formulate these lemmas we need the following definition.

Condition 4.9. Suppose $B \to B^*$ is a bijective correspondence between the blocks in A and A^*. Suppose $B_1^q, \cdots, B_{\gamma_q}^q$ are the q-blocks in A numbered from left to right.

By definition $B \to B^*$ satisfies Condition 4.9 if there exist integers r_q, $x_q (q = 1, \cdots, p+1)$ such that

(1) The order of the q-blocks in A^* from left to right is $B_{r_q+1}^{q*}, \cdots, B_{\gamma_q}^{q*}, B_1^{q*}, \cdots, B_{r_q}^{q*}$.

(2) For $j = 1, \cdots, r_q$ we have $d(B_j^{q*}) = d(B_j^q) + \alpha_q - x_q$.
For $j = r_q + 1, \cdots, \gamma_q$ we have $d(B_j^{q*}) = d(B_j^q) - x_q$.

(3) $m(B_j^{p+1}) = m((B_j^{p+1})^*)$ for $j = 1, \cdots, \gamma_{p+1}$.

LEMMA 4.10. *If B is a block in A, then $d(\hat{B}) = d(B) + \text{type}(B)$ ($\hat{B}$ is as in Lemma* 4.6).

Now we consider $B \to \varphi(B)$ which is defined in Lemmas 4.6 and 4.8. $\hat{A} = \hat{a}_1 \cdots \hat{a}_{n+p+1}$ and s_A are defined in (4.6) and Lemma 4.7. We define

(4.9) $x_q(A) = p + 1 - q + \Sigma\{2(\text{type}(B_*) - q)$: $\hat{B}_* < \hat{a}_1 \cdots \hat{a}_{s_A}$ and $\text{type}(B_*) > q\}$. $(x_q(A) = d_q(\hat{a}_1 \cdots \hat{a}_{s_A}) - q)$.

This last equality is proved in Lemma 5.5.

LEMMA 4.11. (a) *$B \to \varphi(B)$ satisfies Condition* 4.9 *with $r_q =$ the number of q-blocks in $\hat{a}_1 \cdots \hat{a}_{s_A}$ and $x_q = x_q(A)$ as in* (4.9). *Specially, we have $r_{p+1} = x_{p+1} = 0$.*

(b) *If* $\text{type}(B) = q < p+1$, *we have* $\hat{B} < \hat{a}_1 \cdots \hat{a}_{s_A} \Leftrightarrow d(B) \leqq x_q$.

(c) *Suppose* $\text{type}(B) = q < p+1$.
If $d(B) \leqq x_q(A)$, then $d(\varphi(B)) = d(B) + \alpha_q - x_q(A)$.
If $d(B) > x_q(A)$, then $d(\varphi(B)) = d(B) - x_q(A)$.

(d) $x_q(A) = p + 1 - q + \sum_{i=q+1}^{p} 2 \cdot (i-q) \cdot r_i$ *and* $0 < x_q(A) \leqq \alpha_q$ $(q = 1, \cdots, p)$.

(e) $\varphi(A) = \theta^t(A)$ *where* $t = n + p + 1 + \sum_{i=1}^{p} 2 \cdot i \cdot r_i \leqq 2n$ *and t is the minimal integer such that $\theta^t(B)$ satisfies* (4.3).

LEMMA 4.12. *We suppose that $w(A) = w(\theta^i(A)) = k + p + 1$. Then there exists a bijective correspondence $B \to \theta^i(B)$ between the blocks in respectively A and $\theta^i(A)$, satisfying Condition* 4.9.

(4.10) We define $\varphi_{\min}(A) = \theta^i(A)$where $i > 0$ is the least integer $i > 0$ such than $\theta^i(A)$ satisfies (4.3).

If A contains only 1 $(p+1)$-block, $\varphi_{\min}(A) = \varphi(A)$. The next lemma takes care of the other case.

LEMMA 4.13. *Suppose* $A = a_1 \cdots a_n$ *contains more than* $1(p+1)$*-block and* B *is the first* $(p+1)$*-block in* A.

(a) $\varphi_{\min}(A) = \theta^{\delta}(A)$ *where* $\delta < n$.

(b) *A block in* A *is contained in* $a_1 \cdots a_\delta$ *or* $a_{\delta+1} \cdots a_n$.

(c) $a_1 \cdots a_\delta = \cdots BT$ *where* B *is the first* $(p+1)$*-block in* A *and* T *is the tail of* B.

(d) *There is a bijective correspondence* $B \to \varphi_{\min}(B)$ *between the blocks in respectively* A *and* $\varphi_{\min}(A)$, *satisfying Condition* 4.9 *with* $r_q =$ *the number of* q*-blocks in* $a_1 \cdots a_\delta$ *and* $x_q = d_q(a_1 \cdots a_\delta)$.

(e) *If* $\text{type}(B_*) = q < p+1$, *then* $B_* < a_1 \cdots a_\delta \Leftrightarrow d(B_*) \leqq x_q$.

(f) $x_q = d(B) + m(B) - (p+1) + \sum_{i=q+1}^{p+1} 2 \cdot (i-q) \cdot r_i$ *and* $0 < x_q < \alpha_q$ $(q = 1, \cdots, p)$.

(g) $\varphi_{\min}(A) = \theta^{t}(A)$ *where* $t = d(B) + m(B) - (p+1) + \sum_{i=1}^{p+1} 2 \cdot i \cdot r_i$.

Now we will prove Theorem 3.2. We define

$$L_i^s(A) = x_i(A) + \cdots + x_i(\varphi^{s-1}(A)) \,. \tag{4.11}$$

We need the following lemma.

LEMMA 4.14. *Suppose* B *is a block in* A *such that* $\text{type}(B) = j < p+1$. *Let* s *be a positive integer. Suppose* $t \geqq 0$ *is the least integer such that* $d(B) + t\alpha_j - L_j^s(A) \geqq 1$. *Then*

$$d(\varphi^s(B)) = d(B) + t\alpha_j - L_j^s(A) \,.$$

Moreover, B *circles around* t *times by* φ^s (i.e., *there exist* t *different integers* s^1 *such that* $0 \leqq s^1 < s$ *and* $\varphi^{s^1}(B)$ *circles around by* φ).

Proof. We prove this by induction with respect to s.

Suppose the lemma is true for $(s-1)$ and that t' is the least integer such that

$$d(B) + t'\alpha_j - L_j^{s-1}(A) \geqq 1 \,. \tag{4.12}$$

Then,

$$d(\varphi^{s-1}(B)) = d(B) + t'\alpha_j - L_j^{s-1}(A) \,. \tag{4.13}$$

Moreover, we suppose $d(\varphi^{s-1}(B)) \leqq x_j(\varphi^{s-1}(A))$ (if $d(\varphi^{s-1}(B)) > x_j(\varphi^{s-1}(A))$ the proof is analogous). By Lemma 4.11(c)

$$d(\varphi(\varphi^{s-1}(B))) = d(\varphi^{s-1}(B)) + \alpha_j - x_j(\varphi^{s-1}(A)) \,. \tag{4.14}$$

(4.13) and (4.14) imply

$$d(\varphi^s(B)) = d(B) + (t'+1)\alpha_j - L_j^s(A) \,.$$

By (4.13) we get

$$d(B) + t'\alpha_j - L_j^s(A) = d(\varphi^{s-1}(A)) - x_j(\varphi^{t-1}(A)) \leqq 0 .$$

By (4.12) and Lemma 4.1 we get

$$d(B) + (t' + 1)\alpha_j - L_j^s(A) \geqq 1 + \alpha_j - x_j(\varphi^{s-1}(A)) \geqq 1$$

since $r_j(\cdot) \leqq \alpha_j$ by Lemma 4.11(d). Hence, $(t' + 1)$ is the least integer such that $d(B) + t\alpha_j - L_j^s(A) \geqq 1$. Hence, the lemma is true for s.

Moreover, we need two observations:

(4.15) $x_{p+1}(A) = 0$. Hence $d(B) = d(\varphi(B))$ and $m(B) = m(\varphi(B))$ when type$(B) = p + 1$.

(4.16) Suppose $1 \leqq j \leqq p$. If $L_j^s(A) = t\alpha_j$, then for each j-block B we have $d(\varphi^s(B)) = d(B)$ and B circles around t times by φ. (This is an easy consequence of Lemma 4.14.)

The proof of Theorem 3.2. (b) is trivial. By Lemma 4.4 we suppose that A satisfies (4.3). By (4.15) $d(\varphi^Y(B)) = d(B)$ and $m(\varphi^Y(B)) = m(B)$ when type$(B) = p + 1$. $\varphi^Y(A) = A$ follows from Lemma 4.1(b) and the following claim: $d(B) = d(\varphi^Y(B))$ for every j-block, and every j-block circles aroud X_j times by $\varphi^Y (j = 1, \cdots, p)$. This claim follows from (4.16) if we can prove that $L_j^Y(A) = X_j\alpha_j$ for $j = 1, \cdots, p$. We prove the last statement by induction with respect to j starting with $j = p$.

By Lemma 4.11(d) $x_p(\varphi^i(A)) = 1$, hence $L_p^Y(A) = Y = \alpha_p X_p$. Suppose $L_f^Y(A) = X_f\alpha_f$ for $f = p, p-1, \cdots, j+1$. We get $x_j(\varphi^i(A)) = p+1-j - \Sigma\{2(\text{type}(B) - j)\colon \varphi^i(B)$ circles around, type$(B) > j\}$.

When $q > j$ each q-block B circles around X_q times by φ^Y (this follows from the induction hypothesis and (4.16)). Hence,

$$L_j^Y(A) = x_j(A) + \cdots x_j(\varphi^{Y-1}(A)) = Y(p + 1 - j) + \sum_{q=j+1}^{p} X_q \cdot \gamma_q \cdot 2(q - j)$$
$$= \alpha_j \cdot X_j .$$

Finally we compute φ^Y. By Lemma 4.11(e) φ^Y is equal to θ applied

$$\sum_{q=0}^{Y-1} (n + p + 1 + \Sigma\{2 \text{ type}(B)\colon \varphi^q(B) \text{ circles around by } \varphi\})$$
$$= Y(n + p + 1) + 2\cdot\gamma_1\cdot X_1 + 4\gamma_2\cdot X_2 + \cdots + 2p\cdot\gamma_p\cdot X_p \text{ times} .$$

Finally we mention how the lemmas will be used in the forthcoming paper. If $w(A) = \sup_i w(\theta^i(A))$, Lemma 4.12 will imply that all $\theta^i(A)$ such that $w(\theta^i(A)) = w(A)$ have the "same type" of block structure as A. When we determine the minimal periods, we will use

$\varphi_{\min.}$ instead of φ. Lemmas 4.11, 4.13 and 4.14 will be used in the study of $\varphi_{\min}$. The minimal period of A will be determined by its block structure. When we determine the possible minimal periods we will use Lemma 4.1 which characterize the possible block structures. We will also need this lemma when we determine the number of cycles corresponding to each minimal period.

5. **The proofs.** In this section we prove the Lemmas 4.4, 4.6, 4.7, 4.8, 4.10, 4.11, 4.12, and 4.13. The key lemma is Lemma 5.1. We need more notation. We define

(5.1) If $K(B) = 1_{i_1}B_1T_1 \cdots 1_{i_m}B_mT_m1_{i_{m+1}}$ is as in Definition 4.5, then $\widetilde{K(B)} = 1_{i_1}B_1'T_1' \cdots 1_{i_m}B_m'T_m'1_{i_{m+1}}$.

Moreover, we say that A satisfies Condition (5.2) if

(5.2) $w(A) = k + p + 1$, and A starts with a 0 or has the form $A = B \cdots B_*$ where $\text{type}(B) \geqq \text{type}(B_*)$.

(5.3) $\delta(A)$ is the least index such that $\theta^{\delta(A)}(A)$ satisfies (5.2) (if it exists).

LEMMA 5.1. *Suppose* $A = H(B)K(B)D$ *satisfies* (5.2). *Let* $h =$ *the number of positions in* $H(B)K(B)$.

(a) (1) $\theta^h(A) = DH(B)'\widetilde{K(B)}$.

(2) $w(\theta^h(A)) = k + p + 1 - \text{type}(B)$.

(3) $w(\theta^t(A)) \geqq k + p + 1 - \text{type}(B)$ *for* $1 \leqq t \leqq h$.

We define $A^h = \theta^h(A)1_{\text{type}(B)} = DH(B)'\widetilde{K(B)}1_{\text{type}(B)} \in \{0, 1\}^{n+type(B)}$.

(b) *There exists a bijective correspondence* $B_* \to B_*^h$: {*the blocks in* A}$\to$ {*the blocks in* A^h} *satisfying* $\text{type}(B_*) = \text{type}(B_*^h)$, $m(B_*) = m(B_*^h)$ *and*:

(1) *If* $B_* < H(B)$, *then* $B_*^h = B_*'$.

(2) *Suppose* $B_* < K(B)$. *If* B_* *has a tail* $T(B_*)$, *then* $B_*^h = T(B_*)'$. *Otherwise* $B_*^h = B_*'$.

(3) *If* $B_* < D$, *then* $B_*^h = B_*$.

(4) $B^h = \widetilde{K(B)}1_{\text{type}(B)}$.

(c) (1) $\delta = \delta(\theta^h(A))$ *exists and* $\text{type}(B) \leqq \delta < l(\widetilde{K(B)})$. *We decompose* $A^h = D_1D_2\widetilde{K(B)}1_{\text{type}(B)}$ *where* $r(D_1) = \delta$.

(2) *Every block in* A^h *is contained in* D_1 *or* $D_2\widetilde{K(B)}1_{type(B)}$.

(3) $\theta^{h+\delta}(A) = D_2\widetilde{K(B)}D_1'$.

(4) $w(\theta^{h+t}(A)) \geqq k + p + 1 - \text{type}(B)$ *for* $1 \leqq t \leqq \delta$. *We denote* D_1 *by* $T(B)$, i.e., $\theta^{h+\delta}(A) = D_2\widetilde{K(B)}T(B)'$.

(d) *There exists a bijective correspondence* $B_*^h \to B_*^{h+\delta}$: {*the blocks in* A^h} $\to$ {*the blocks in* $\theta^{h+\delta}(A)$} *satisfying* $\text{type}(B_*^{h+\delta}) = \text{type}(B_*)$,

$m(B_*^{h+\delta}) = m(B_*)$ *and*:

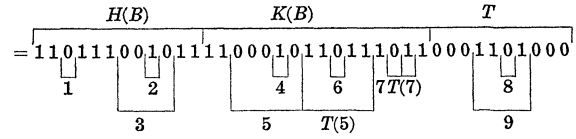
(1) *If* $B_*^h < D_2\widetilde{K(B)}$, *then* $B_*^{h+\delta} = B_*^h$.

(2) *If* $B_*^h < D_1$, *then* $B_*^{h+\delta} = B_*^{h'}$.

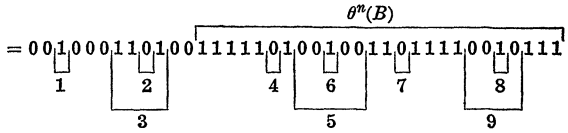
(3) $B^{h+\delta} = \widetilde{K(B)}D_1'$.

We observe that the definition of $T(B)$ in Lemma 5.1 corresponds to the definition of the tail of B in Definition 4.5: Suppose $A = 0_{i_1}B_1T_1 \cdots B_mT_m0_{i_{m+1}}B_{END}$ is as in Definition 4.5. If we apply Lemma 5.1 on $\theta^{i_1}(A) = B_1T_1 \cdots$ we get $T_1 = T(B_1)$. Analogously we get $T_i = T(B_i)$ for $i = 2, \cdots, m$.

We will now illustrate the proof by an example. The clumsy formulation of the lemma is necessary to treat all cases. However, if we suppose $A = BT$ where T is the tail of B, the lemma is easier to understand. In this case h and δ in Lemma 5.1 are given by $h =$ the length of B, and $\delta =$ the length of T. We therefore study the following example with $p = 3$: $A = H(B)K(B)T$



$\theta^{h+\delta}(A) = \theta^n(A) = H(B)'\widetilde{K(B)}T''$



The blocks in A, except B itself, are nummerated from 1 to 9. The corresponding blocks in $\theta^n(A)$ are also nummerated from 1 to 9. Moreover, we have denoted the tail of the blocks No. 5 and 7 by $T(5)$ and $T(7)$ respectively. We observe that the blocks of $\theta^n(A)$ are obtained from the blocks of A in the following way:

1. $B \to \widetilde{K(B)}T'$.
2. We remove a level from the blocks in $H(B)$.
3. We add a level to the blocks in T.
4. The block No. $5 \to T(5)'$, and the block No. $7 \to T(7)'$.
5. We remove a level from the blocks contained in the blocks No. 5 or 7.
6. We add a level to the blocks contained in $T(5)$ or $T(7)$.

Proof of Lemma 5.1.

Proof of (a). We put $z = r(H(B))$. We get from Lemma 4.3(a)

that $\theta^z(A) = K(B)DH(B)'$.

If $K(B) \neq \emptyset$, then $w(\theta^z(A)) = k$ and by using Lemma 4.3(a) and 4.3(c) several times we get $\theta^h(A) = DH(B)'\widetilde{K(B)}$ and $w(\theta^h(A)) = k$. (2) and (3) are easily shown.

Proof of (b-3). We only need to prove this for blocks on level 1. Let $B_* < D$ be a block on level 1 in A. We must prove that B_* is succeded by a D_* in A^h satisfying:

$$\begin{aligned} &0 > f_{D*}(t) \text{ for } t \in D_* \\ &r(D_*) = n + \text{type}(B) \text{ or } f(D_*) = -\min\{f(B_*), p+1\} = -\text{type}(B_*) . \end{aligned} \tag{5.4}$$

If $D = D_1B_*D_*D_2$ where D_* satisfies (5.4), there is nothing to prove. Otherwise $D = D_1B_*C_*$ where C_* satisfies: $0 > f_{C*}(t)$ for $t \in C_*$. Suppose first $C_* \neq \emptyset$. If $\text{type}(B) = p + 1$, we get

$$f(C_*H(B)') < -(p+1) \quad \text{and} \quad f_{C*}(t) < 0 \quad \text{for} \quad t \in C_*H(B)' .$$

If $\text{type}(B) < p + 1$, then $A^h = D_1B_*C_*H(B)'1_{\text{type}(B)}$ and

$$f_{C*}(t) < 0 \quad \text{for} \quad t \in C_*H(B)'1_{\text{type}(B)} .$$

If $C_* = \emptyset$, we have by (5.2) that $\text{type}(B_*) \leqq \text{type}(B)$. Hence, B_* is suceeded by $H(B)'$ and $f(H(B)') \leqq \text{type}(B_*)$. In all these cases we get easily a D_* satisfying (5.4).

The proof of $(b-1)$ is the main part of the proof.

Proof of (b—1). Because of (b—3) the first 1 in $H(B)'$ will start a block on level 1. Suppose $H(B) = 1_{i_1}B_1 1_{i_2}B_2 \cdots B_m 1_{i_{m+1}}$ where $B_1, \cdots, B_m$ are the blocks on level 2 in $H(B)$. We get

$$H(B)' = 0_{i_1}B_1'0_{i_2}B_2' \cdots B_m'0_{i_{m+1}} .$$

Since $f_{H(B)}(t) \leqq f(H(B))$ for $t \in H(B)$, there exists C_1 such that $H(B) = \cdots B_1C_1 \cdots$ and

$$0 < f_{C_1}(t) \leqq f(C_1) = \text{type}(B_1) \quad \text{for} \quad t \in C_1 .$$

We get

$$\begin{aligned} &H(B)' = \cdots B_1'C_1' \cdots \\ &0 < f_{B_1'}(t) \leqq f(B_1') = \text{type}(B_1) \quad \text{for} \quad t \in B_1' \\ &0 > f_{C_1'}(t) \geqq f(C_1') = -\text{type}(B_1) \quad \text{for} \quad t \in C_1' . \end{aligned}$$

By definition B_1' is a block in A^h satisfying $\text{type}(B_1') = \text{type}(B_1)$ and $\text{level}(B_1') = 1 = \text{level}(B_1) - 1$. We treat $B_2, \cdots, B_m$ analogously.

By the same argument we prove (by induction with respect to level (B_*)) that (b—1) is true for all $B_* < H(B)$.

Proof of (b − 4). $K(\widetilde{B})1_{\text{type}(B)}$ starts with a 1. Hence by (b—1) there starts a block on level 1 in position $l(K(\widetilde{B})1_{\text{type}(B)})$. If $K(B) = \varnothing$, there is nothing to prove. Otherwise, we prove easily that

$$f_{K(B)}(t) > 0 \quad \text{for} \quad t \in K(\widetilde{B})1_{p+1} \quad \text{and} \quad f(K(\widetilde{B})1_{p+1}) > p + 1 .$$

Moreover, there is no C contained in $K(\widetilde{B})1_{p+1}$ satisfying $f_C(t) < 0$ for $t \in C$ and $(f(C) = -(p + 1)$ or $r(C) = n + p + 1)$. Hence, $B^h = K(\widetilde{B})1_{p+1}$ is a $(p + 1)$-block. Furthermore,

$$f(B^h) = f(K(\widetilde{B})) + p + 1 = f(K(B)) + f(H(B)) = f(B) .$$

Proof of (b—2). $K(B) = 1_{i_1}B_1T_1 1_{i_2} \cdots B_mT_m 1_{i_{m+1}}$ where B_i $(i = 1, \cdots, m)$ are the blocks in $K(B)$ which has a tail T_i. We get

$$K(\widetilde{B}) = 1_{i_1}B_1'T_1'1_{i_2} \cdots B_m'T_m'1_{i_{m+1}} .$$

We treat only B_1T_1. $B_2T_2, \cdots, B_mT_m$ are treated analogously. As in (b—1) we get: For all $B_* < B_1$, B_*' is a block in A^h such that type (B_*') = type(B_*) and level(B_*') = level$(B_*) - 1$.

Next we show that $B_1^h = T_1'$. T_1' satisfies

$$0 > f_{T_1'}(t) \geqq f(T_1') = -\text{type}(B_1) \quad \text{for} \quad t \in T_1' . \tag{5.5}$$

Obviously $B^h = K(\widetilde{B})1_{p+1}$ has the form $B^h = \cdots T_1'C_1 \cdots$ where C_1 satisfies

$$0 < f_{C_1}(t) \leqq f(C_1) = \text{type}(B_1) .$$

Hence $B_1^h = T_1'$ is a block of type(B_1) such that level(B_1^h) = level(B_1).

At last we prove as in (b − 1) that: For all $B_* < T_1$, B_*' is a block in A^h such that type(B_*') = type(B_*) and level(B_*') = level$(B_*) + 1$.

Proof of (c). We have $\theta^h(A) = DH(B)'K(\widetilde{B})$. We prove that $\theta^h(A)$ has the form $\theta^h(A) = D_1D_2K(\widetilde{B})$ where

$$0 > f_{D_1}(t) \geqq f(D_1) = -\text{type}(B) \text{ for } t \in D_1 . \tag{5.6}$$

Since B is a block in $A = H(B)K(B)D$ we have two possibilities. If $f_D(t) < 0$ for $t \in D$, we get $f_D(t) < 0$ for $t \in DH(B)'$ and $f(DH(B)') < -\text{type}(B)$. Otherwise, $D = D_1D_3$ where D_1 satisfies (5.6).

We choose D_1 maximal with respect to (5.6). We put $\delta = r(D_1)$. By (5.6) every block starting in D_1 is contained in D_1. Hence, (2)

is true. (3) and (4) follow from Lemma 4.3. However, we are not able to prove (1) without using (d). Hence, we proved (d) first.

Proof of (d). If $B_*^h < D_2$ is a block on level 1 in A^h, we show that $\theta^{h+\delta}(A)$ has the form $\theta^{h+\delta}(A) = \cdots B_*^h D_* \cdots$ where D_* satisfies

$$\begin{aligned} &f_{D_*}(t) < 0 \quad \text{for} \quad t \in D_* \,. \\ &r(D_*) = n \quad \text{or} \quad f(D_*) \leqq -\text{type}(B_*^h) \,. \end{aligned} \tag{5.7}$$

If $D_2 = \cdots B_*^h D_* \cdots$ where D_* satisfies (5.7), there is nothing to prove. Otherwise $A^h = B_*^h C_*$ where $f_{C_*}(t) < 0$ for $t \in C_*$. In this case $\text{type}(B) < (p+1)$ and $K(B) = \varnothing$. We obviously have $C_* = C_1 1_{\text{type}(B)}$ where $f(C_1) < -\text{type}(B)$. $D_* = C_1 T(B)'$ will satisfy $f_{D_*}(t) < 0$ for $t \in D_*$ and $r(D_*) = n$. Hence, (d—1) is true for $B_*^h < D_2$.

Next we prove (d—3). If $K\widetilde{(B)} = \varnothing$, $B^{h+\delta} = T(B)'$ satisfies the lemma. Otherwise, $K\widetilde{(B)} \neq \varnothing$ and $\text{type}(B) = p+1$. We get

$$f(K\widetilde{(B)}T(B)') > p+1 \quad \text{and} \quad f_{K\widetilde{(B)}}(t) > 0 \text{ for } t \in K\widetilde{(B)}T(B)' \,.$$

Suppose there exists a $C < A^{h+\delta}$ such that

$$\begin{aligned} &l(C) \in K\widetilde{(B)}T(B)' \\ &f(C) \leqq f_C(t) < 0 \quad \text{for} \quad t \in C \\ &r(C) = n \quad \text{or} \quad f(C) = -(p+1) \,. \end{aligned}$$

We see easily that $C < K\widetilde{(B)}$. This is a contradiction since $B^h = K\widetilde{(B)}1_{p+1}$ is a $(p+1)$-block. We therefore get that $B^{h+\delta} = K\widetilde{(B)}T(B)'$ is a $(p+1)$-block. Hence, we have proved (d—3).

We prove trivially that (d—1) is true for $B_*^h < K\widetilde{(B)}$. Finally we show (d—2) in the same way as (b—1).

The proof of (c-1). We suppose $D_2 \neq \varnothing$ (if $D_2 = \varnothing$, then the proof is analogous and much easier). By the maximality of D_1 with respect to (5.6) we get that D_2 starts with 0 or a block of type $\geqq$ type(B). By (d—1) $\theta^{h+\delta}(A) = D_2 \cdots$ starts with 0 or a block of type $\geqq$ type(B). Moreover, if D_1 satisfies (5.6) and is not maximal with respect to (5.6), then D_2 starts with a block of type $<$ type(B). By (d—1) $\theta^{h+\delta}(A)$ will start with a block of type $<$ type(B). Hence, δ is the least index satisfying (5.2).

LEMMA 5.2. *Suppose* $w(A) = k+p+1$ *and* $A = B_1C_1DB$ *where* $\text{type}(B_1) < \text{type}(B)$ *and*

$$0 > f_{C_1}(t) \geqq f(C_1) = -f(B_1) \quad \textit{for} \quad t \in C_1 \,.$$

Let $h = r(C_1)$. *Then we have* $\theta^h(A) = DBB_1'C_1'$ *and* $w(\theta^h(A)) = k + p + 1$. *Furthermore,*

$$w(\theta^t(A)) \geqq k + p + 1 - \text{type}(B_1) \quad \textit{for} \quad t \in \{1, \cdots, h\} .$$

There exists a bijective correspondence $B_* \to B_*^h$: {*the blocks in* A} $\to$ {*the blocks in* A^h} *such that* $\text{type}(B_*^h) = \text{type}(B_*)$, $m(B_*^h) = m(B_*)$ *and*

(1) *If* $B_* < D$, *then* $B_*^h = B_*$.
(2) *If* $B_* < B_1C_1$, *then* $B_*^h = B_*'$.
(3) $B^h = BB_1'C_1'$.
(4) *If* $B_* < B$, *then* $B_*^h = B_*$.

Proof. We observe that $f(BB_1'C_1') = f(B)$ and $f_B(t) > 0$ for $t \in BB_1'C_1'$. Hence (3) is proved. (1) and (4) are trivial. (2) is proved in the same way as Lemma 5.1(b-1).

Proof of Lemma 4.4. The lemma follows easily by using Lemmas 5.1 and 5.2 several times.

Proof of Lemma 4.6, 4.7 *and* 4.8. Suppose $A = 0_{i_1}B_1T_10_{i_2}B_2T_2 \cdots B_mT_m0_{i_{m+1}}B_{END}$ where $B_i = H(B_i)K(B_i)$ and T_i is the tail of B_i. We prove Lemma 4.6 by using Lemma 5.1(b) and (d) respectively $m + 1$ and m times. We also use Lemma 4.3(b) $m + 1$ times. Then Lemma 4.7 follows from 5.1(c) ($s_A = \delta(\theta^n(A))$), and Lemma 4.8 follows from 5.1(d).

LEMMA 5.3. *Suppose* $C < A$, $f(C) = 0$, C *starts with a block and*

$$0 < |f_C(t)| \leqq p + 1 \quad \textit{for} \quad t \in C \quad \textit{and} \quad t \neq r(C) .$$

Then the length of $C = \Delta(C)$ *where* $\Delta(C) = \sum_{i=1}^{p+1} 2 \cdot i \cdot$(*the number of* i*-blocks* $B < C$).

Proof. The proof is by induction with respect to $j =$ the number of blocks contained in C. If $j = 1$, then $C = 1_q0_q$ or 0_q1_q and the claim is true. Suppose the claim is true for $1, \cdots, j$. Suppose that C contains $j + 1$ blocks. $C = BE$ where B is a block. Suppose level(B) is odd. (If level(B) is even the proof is analogous.) Then

$$B = 1_{i_1}C_11_{i_2} \cdots C_q1_{i_{q+1}} \quad \text{and} \quad E = 0_{j_1}D_10_{j_2} \cdots D_r0_{j_{r+1}}$$

where D_j and C_i satisfy the hypothesis of the lemma and

$$i_1 + \cdots + i_{q+1} = j_1 + \cdots + j_{r+1} = \text{type}B .$$

By the induction hypothesis, the lemma is true for C_i and D_j, and we get the length of $BE = \Delta(BE)$.

LEMMA 5.4. *Suppose* $A = H(B)K(B)D = a_1 \cdots a_n$, type$(B) = q$, $A^h = a_1^h a_2^h \cdots$, $B_* \to B_*^h$ *and* $B_*^h \to B_*^{h+\delta}$ *are as in Lemma* 5.1.

(a) $B_* \to B_*^h$ *satisfies Condition* 4.9 *with* $r_j =$ *the number of* j*-blocks in* $a_1 \cdots a_h$ *and* $x_j = d_j(a_1 \cdots a_h)$.

(b) $B_*^h \to B_*^{h+\delta}$ *satisfies Condition* 4.9 *with* $r_j =$ *the number of* j*-blocks in* $a_1^h \cdots a_\delta^h$ *and* $x_j = d_j(a_1^h \cdots a_\delta^h)$.

(c) *Suppose* type$(B_*) = j <$ type$(B) = q$. *Then* $B_*^h < a_1^h \cdots a_\delta^h$ *if and only if* $d(B_*^h) \leqq d_j(a_1^h \cdots a_\delta^h)$.

Proof. We suppose that $K(B)$ is as in (5.1). Hence,

$$A = H(B)K(B)D = H(B)1_{i_1}B_1T_1 \cdots 1_{i_m}B_mT_m1_{i_{m+1}}D\,.$$
$$A^h = DH(B)'\widetilde{K(B)}1_q = DH(B)'1_{i_1}B_1'T_1' \cdots 1_{i_m}B_m'T_m'1_{i_{m+1}}1_q\,.$$

(If $q < p + 1$, then $K(B) = \varnothing$.) By Lemma 5.1(b) we get $B^h = \widetilde{K(B)}1_q$ and $B_i^h = T_i'$ for $i = 1, \cdots, m$. The other blocks get displaced h positions modulo n.

We observe that

$$d_j(D) = d_j(A) - d_j(H(B)K(B)) \quad \text{and} \quad \alpha_j = d_j(A) + j\,. \tag{5.8}$$

First we consider B^h. $H(B)$ has the form $H(B) = 1_{i_1}C_11_{i_2} \cdots C_m1_{i_{m+1}}$ where C_i satisfies Lemma 5.3, and $i_1 + \cdots + i_{m+1} = q$. By Lemma 5.3 $d_q(H(B)') = q$. Hence,

$$\begin{aligned} d(B^h) &= d_q(D) + d_q(H(B)') = d_q(D) + q = \alpha_q - d_q(H(B)K(B)) \\ &= d(B) + \alpha_q - d_q(a_1 \cdots a_h) \end{aligned}$$

by (5.8) and since $d(B) = 0$ and $a_1 \cdots a_h = H(B)K(B)$.

Next we suppose $B_* < H(B)$, type $(B_*) = s$ and $A = EB_* \cdots$. Then $A^h = DE'B_*^h \cdots$.

There is a bijective correspondence between {the end positions of blocks in E}\{$l(B)$} and {the end positions of blocks in E'}. Hence, $d_s(E') = d_s(E) + s = d(B_*) + s$. Hence, by (5.8)

$$\begin{aligned} d(B_*^h) &= d_s(D) + d_s(E') = d_s(D) + s + d(B_*) = d(B_*) + \alpha_s - d_s(H(B)K(B)) \\ &= d(B_*) + \alpha_s - d_s(a_1 \cdots a_h). \end{aligned}$$

All the other cases are treated in the same way.

(b) is proved as (a), and (c) follows from Lemma 4.2.

Proof of Lemma 4.10. We treat only the case type$(B) = q$ and B has a tail. Then by Lemma 4.6

$$A = EH(B)K(B) \cdots, \quad \hat{A} = \tilde{E}H(B)'\hat{B} \cdots$$

and there exists a bijective correspondence between

$$\{\text{the end positions of blocks in } E\}$$

and

$$\{\text{the end positions of blocks in } \tilde{E}\}\ .$$

Therefore $d_q(E) = d_q(\tilde{E})$. As in the previous proof $d_q(H(B)') = q$. We get $d(\hat{B}) = d_q(\tilde{E}) + d_q(H(B)') = d_q(E) + q = d(B) + q$. All the other cases are treated in the same way.

LEMMA 5.5. *Suppose A satisfies* (4.3). *Suppose r_j = the number of j-blocks in $\hat{a}_1 \cdots \hat{a}_{s_A}$, where $\hat{A} = \hat{a}_1 \cdots \hat{a}_{n+p+1}$ and s_A are defined in* (4.6) *and Lemma* 4.7.

(a) $s_A = p + 1 + \sum_{i=1}^{p} 2 \cdot i \cdot r_i$.

(b) $d_j(\hat{a}_1 \cdots \hat{a}_{s_A}) = p + 1 + \sum_{i=j+1}^{p} 2 \cdot (i - j) \cdot r_i = x_j(A) + j$ *where* $x_j(A)$ *is defined in* (4.9).

Proof. $s_A = \delta(\theta^n(A)) = \delta(\hat{a}_1 \cdots \hat{a}_n)$. By (5.6) in the proof of Lemma 5.1 we get

$$0 > f(\hat{a}_1 \cdots \hat{a}_t) \geqq -f(\hat{a}_1 \cdots \hat{a}_{s_A}) = -(p + 1) \quad \text{for} \quad 1 \leqq t \leqq s_A\ .$$

Hence, $\hat{a}_1 \cdots \hat{a}_{s_A}$ is equal to

$$0_{i_1} C_1 0_{i_2} \cdots C_m 0_{i_{m+1}}$$

where C_i satisfies Lemma 5.3 and $i_1 + \cdots + i_{m+1} = p + 1$.

(b) By definition

$$d_j(\hat{a}_1 \cdots \hat{a}_{s_A}) = s_A - \sum_{i=1}^{j} 2 \cdot i \cdot r_i - j \cdot \sum_{i=j+1}^{p} 2 \cdot r_i\ ,$$

and (b) follows from (a).

Proof of Lemma 4.11. From Lemma 5.4(b) we get that $\hat{B} \to \varphi(B)$ satisfies Condition 4.9 with $\delta = s_A$ and

$$r_j = \text{the number of } j\text{-blocks in } \hat{a}_1 \cdots \hat{a}_\delta\ .$$
$$x_j = d_j(\hat{a}_1 \cdots \hat{a}_\delta) = x_j(A) + j \ \text{(Lemma 5.5)}\ .$$

Moreover, if $\text{type}(B) = j$ we get by Lemma 5.4(c)

$$\hat{B} < \hat{a}_1 \cdots \hat{a}_\delta \Longleftrightarrow d(\hat{B}) \leqq d_j(\hat{a}_1 \cdots \hat{a}_\delta)\ .$$

Since $d(\hat{B}) = d(B) + \text{type}(B)$, Lemma 4.11(a) and (b) are true. By combining (a) and (b) we get (c) easily.

The first parts of (d) and (e) follows from Lemma 5.5. Moreover $x_q(A) \leqq \alpha_q$ $(q = 1, \cdots, p)$ is proved as follows: Let B_{END} be the last block in A. If $B \neq B_{\text{END}}$ is a block in $a_1 \cdots a_n$, then $\hat{B} < \hat{a}_1 \cdots \hat{a}_n$.

But $r(\hat{B}_{\text{END}}) = n + p + 1$ and $1(\hat{B}_{\text{END}}) = n + 1$ if $K(B) = \varnothing$. Hence,

$$d_q(\hat{a}_1 \cdots \hat{a}_n) \leqq d_p(a_1 \cdots a_n) + 2q$$

and by Lemma 5.5(b) and (5.8) we get

$$x_p(A) = d_p(\hat{a}_1 \cdots \hat{a}_{s_A}) - q \leqq d_q(\hat{a}_1 \cdots \hat{a}_n) - (q \leqq d_q(a_1 \cdots a_n) + q = \alpha_q .$$

That t is the least integer such that $\theta^t(A)$ satisfies (4.3) follows from the proof of Lemma 5.1.

Proof of Lemma 4.12. Let i be the least i such that $w(\theta^i(A)) = k + p + 1$. We divide the proof into 3 cases.

(1) If A starts with 0, then $i = 1$.

(2) Suppose A satisfies Lemma 5.1. Then $B \to B^h$ will satisfy Condition 4.9 by Lemma 5.4(a). We do a little modification of Lemma 5.1 (c) and (d): We use δ' instead of δ, where δ' is the least integer $\delta' > 0$ such that $w(\theta^{h+\delta'}(A)) = k + p + 1$. (In the proof of Lemma 5.1 we choose D_1 minimal with respect to (5.6) and put $\delta' = r(D_1)$.)

As in Lemma 5.4(b) $B^h \to B^{h+\delta'}$ will satisfy Condition 4.9. Hence, $B \to \theta^{h+\delta'}(B)$ will satisfy Condition 4.9.

(3) Suppose A is as in Lemma 5.2. Then $i = h$. As before it is easy to see that $B \to \theta^h(B) = B^h$ satisfies Condition 4.9.

Proof of Lemma 4.13. (a), (b) and (c) follows from Lemma 5.1. The proof of (d) and (e) are modifications of the proof of the Lemma 5.4.

(f) We prove that

$$\text{(5.9)} \quad \text{the length of } a_1 \cdots a_\delta = m(B) - (p + 1) + d(B) + \sum_{i=1}^{p+1} 2 \cdot i \cdot r_i .$$

Suppose $a_1 \cdots a_\delta = DBT$. D has the form

$$D = 0_{i_1} C_1 0_{i_2} \cdots C_m 0_{i_{m+1}}$$

where C_i satisfies Lemma 5.3 and $i_1 + \cdots + i_{m+1} = d(B)$. Hence,

$$\text{the length of } D = d(B) + \sum \{2 \cdot \text{type}(B^*) \colon B^* < D\} .$$

We prove analogously,

$$\text{the length of } B = m(B) + \sum \{2 \cdot \text{type}(B^*) \colon B^* < B\} .$$
$$\text{the length of } T = (p + 1) + \sum \{2 \cdot \text{type}(B^*) \colon B^* < T\} .$$

(5.9) follows from these equalities since $\text{type}(B) = p + 1$ and $r_{p+1} = 1$. (f) follows from (5.9) by using the definition of $x_q = d_q(a_1 \cdots a_\delta)$. Moreover, (5.9) implies (g). ($x_q \leqq \alpha_q$ is proved as follows: It is not difficult to prove $d_q(a_{\delta+1} \cdots a_n) \geqq p+1-2q$. (For example if $a_{\delta+1} \cdots a_n =$

1_{p+1} where 1_{p+1} is a $(p+1)$-block, then $d_q(a_{\delta+1}\cdots a_n)=p+1-2q)$. Hence,

$$\begin{aligned} x_q &= d_q(a_1\cdots a^s) = d_q(a_1\cdots a_n) - d_q(a_{\delta+1}\cdots a_n) \\ &\leqq (\alpha_q - q) - (p+1-2q) = \alpha_q - (p+1-q) < \alpha_q) \,. \end{aligned}$$

Now we prove two lemmas which we will use in the next paper.

LEMMA 5.6. (a) *We suppose* $A \in \{0,1\}^n$ *and* $w(A) = k+p+1$. *We determine the block structure of* A *with respect to* p. *If* $j = \sup\{\text{type}(B)$: B *block in* $A\}$, *then* $w(\theta_S^i(A)) \geqq k+p+1-j$ *and* $\theta_S^i(A) = \theta_{S'}^i(A)$ *for every* i, *where* $S = E_k + \cdots + E_{k+p}$, $S' = E_{k'} + \cdots + E_{k'+p'}$, $p' = j-1$ *and* $k' = k+p+1-j$.

(b) *We suppose* $A \in \{0,1\}^n$, $S = E_k + \cdots + E_{k+p}$ *and* $w(A) = \sup w(\theta_S^i(A)) = k+p'+1$. *Then* $\theta_S^i(A) = \theta_{S'}^i(A)$ *for every* i, *where* $S' = E_k + \cdots + E_{k+p'}$.

(c) *We suppose* $A = a_1\cdots a_n \in \{0,1\}^n$ *and* $w(A) = k+p+1$. *Moreover, we suppose* $1 \leqq z \leqq p+1$ *and* $A = B$ *is a* z*-block or*

$$\begin{cases} A = B_1T_1B_2T_2\cdots B_{f-1}T_{f-1}B_f \text{ where } \text{type}(B_i) = z \text{ and} \\ T_i = a_r\cdots a_s \text{ satisfies} \\ 0 > f(a_r\cdots a_j) \geqq -z = f(T_i) \text{ for } j = r,\cdots,s (i = 1,\cdots,f-1)\,. \end{cases}$$

Then for $p' > p$ *we have* $\theta_{S'}^i(A) = \theta_S^i(A)$ *for every* i, *where* $S' = E_k + \cdots + E_{k+p'}$ *and* $S = E_k + \cdots + E_{k+p}$.

Proof. (b) Suppose $p' < p$. Suppose $\theta_S^i(A) = c_1\cdots c_n$. If $w(c_2\cdots c_n) = k+p'+1$, then $c_1 = 0$. Hence $\theta_S^{i+1}(A) = c_2\cdots c_nc_1'$ and $w(\theta_S^{i+1}(A)) = k+p'+2$ which is a contradiction. Hence, we have proved $w(c_2\cdots c_n) \leqq k+p'$. Hence, $S(c_2\cdots c_n) = S'(c_2\cdots c_n)$.

(a) $w(\theta_S^i(A)) \geqq k+p+1-j$ follows from Lemma 5.1(a-3) and (c-4). Then $\theta_S^i(A) = \theta_{S'}^i(A)$ follows as in the proof of (b).

(c) We suppose $A = B = H(B)K(B)$ as in Lemma 5.1. (The other case is treated analoguously.) We let h and δ be as in Lemma 5.1. We observe $h = n$ and $\delta =$ the length of $H(B)$: By Lemma 5.1 $\theta_S^n(A) = H(B)'\widetilde{K(B)}$. Moreover, $\theta_S^{n+\delta}(A) = \widetilde{K(B)}H(B)$ is a $(p+1)$-block. Moreover, it is not difficult to prove (for example by Lemma 4.3) that

$$w(\theta_S^i(A)) < k+p+1 \text{ or } \theta_S^i(A) \text{ starts with } 1$$

for $i = 1,\cdots,h+\delta$. Hence, $\theta_S^i(A) = \theta_{S'}^i(A)$ for $i = 1,\cdots,h+\delta$. This is proved analogously for $i > h+\delta$.

LEMMA 5.7. *Suppose* $A \in \{0,1\}^n$ *and* $w(A) = k+p+1$ *and* $S = E_k + \cdots + E_{k+p}$. *Suppose* $A = BTD$ *where* B *is a block and* $T = a_r\cdots a_s$ *satisfies*

$$0 > f(a_r \cdots a_j) \geqq -\text{type}(B) = f(T) \text{ for } j = r, \cdots, s .$$

Then $w(\theta_S^z(A)) = k + p + 1$ *where* $z =$ *the length of* BT.

Proof. The Lemma follows from Lemma 4.3.

Index of Notations

$s(A)$	Section 2	B_{END}	(4.3)
0_t, 1_t	Section 2	$H(B)$, $K(B)$	(4.4)
$w(\cdot)$	Section 2	The tail	Definition 4.5
$l(\cdot)$, $r(\cdot)$	Section 2	$m(B)$	(4.5)
$f(\cdot)$	(3.1), (3.2)	$\hat{B}$, $\hat{A}$	(4.6), Lemma 4.6
$t \in D$	(3.3)	s_A	Lemma 4.7
$C < D$	(3.4)	$\varphi(A)$, $\varphi(B)$	(4.7), Lemma 4.8
type(B), level(B)	Definition 3.1	circles around	(4.8)
θ	Section 3	$x_q(A)$	(4.9)
α_j, γ_j	Section 3	$\varphi_{\min}$	(4.10)
$d_q(\cdot)$, $d_q(A, s, t)$	Section 4	$L_i^s(A)$	(4.11)
$d(B)$	Section 4	$\widetilde{K(B)}$	(5.1)
$s \wedge t$	Section 4	$\delta(A)$	(5.3)
a', C'	Section 4		

References

1. 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.
2. J. Søreng, *The periods of the sequences generated by some symmetric shift registers*, J. Combinatorial Theory, Series A., **21** (1976), 165–187.
3. ———, *The periods of the sequences generated by some symmetric shift registers*—Part 2, Preprint.

Received December 14, 1977 and in revised form September 19, 1978.

University of Oslo
P. O. Po. Box 1053-Blindern
Oslo 3, Norway