ABSTRACT.

We determine the periods of the sequences generated by the difference equation

$$X_{n+1} = X_1 + S(x_2, \ldots, x_n)$$

where S is a symmetric polynomial, over the field $GF(2)$.

1. INTRODUCTION

In this paper we consider the difference equation $x_{n+1} = x_1+S(x_2,\ldots,x_n)$ where S is a symmetric polynomial, over the field $GF(2)$. $GF(2) = \{0,1\}$ is characterized by $1+1 = 0+0 = 0$ and $0+1 = 1$. We determine all the periods of the sequences generated by this difference equation.

The problem is equivalent to find the periods of the symmetric shift registers. The symmetric shift register θ_S corresponding to S is defined by

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

p is a period of $(a_1,\ldots,a_n)$ with respect to θ_S if $\theta_S^p(a_1,\ldots,a_n) = (a_1,\ldots,a_n)$.

In [1], [2] and [3] the periods were found for some symmetric polynomials. Besides, in [2] we reduced the problem to the case $S = E_k+\ldots+E_{k+p}$ where $p \geq 0$ and E_i is defined by

$E_i(a_2,\ldots,a_n) = 1$ if and only if $\sum_{j=2}^{n} a_j = i$, else $E_i(a_2,\ldots,a_n) = 0$.

In this paper we find the periods in this case. Hence by using Thm. 2.2 in [2] we find the periods for every symmetric polynomial. We use the ideas of [3] where the case $p = 2$ is treated in a very direct way.

We think that the method of the proofs and the lemmas may be are more important than the main result. These methods will give us a possibility to count the cycles of symmetric shift registers. By studing how the blockstructure is used in the proofs, it is possible to define invariants which characterize each cycle. In a forthcoming paper the author will do some work about this question.

2. PRELIMINARIES.

First we introduce some notations:

a, b, c, d denotes the integers $\in\{0,1\}$.

e, f, g, . denotes the integers ≥ 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 (Def. 3.1).

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

We let $1_t = 1\ldots1$ (resp. $0_t = 0\ldots0$) denote a string of t consecutive 1's (resp. 0's) .

We denote $\vec{a} = (a_1,\ldots,a_n)\in\{0,1\}^n$ also by $\vec{a} = a_1\ldots a_n$.

The weight $w(\vec{a})$ of a vector $\vec{a} = (a_1,\ldots,a_n)$ is defined by $w(\vec{a}) = \sum_{i=1}^{n} a_i$.

Suppose $A = a_1\ldots a_n$ and $C = a_i\ldots a_j$ 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 Thm. 2.2 in [2]. These results reduce the problem to the case $S = E_k+\ldots+E_{k+p}$. Let S_p be the homogeneous symmetric polynomial of degree p in the variables $x_2,\ldots,x_n$. 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 bionomial coefficient. We define intervals in the set of the integers Z in the usual way by

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

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

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

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

Thm. 3.2, which solve the case $S = E_k+\ldots+E_{k+p}$, will therefore give the complete solution of our problem.

3. THE MAIN RESULT

The main consept 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 $p = 4$

$$A = 0\underbrace{11}_{\text{2-block}}0000\underbrace{111}_{\text{3-block}}0000\underbrace{11111}_{\text{5-block}}0000000\underbrace{1111111}_{\text{5-block}}$$

The general definition is more complicated. The main difficulty is that the blocks can contain subblocks. We need more notation, If $A = a_1 \ldots a_n$ and $i \leqq j$, we define

(3.1) $f_i^A(j) =$ (the number of 1's in $a_i \ldots a_j$)-(the number of 0's in $a_i \ldots a_j$) .

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

(3.2) $f^A(C) = f_s^A(t)$.

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 $C \neq D$.

It is very easy to see that the following definition of blocks is well defined. That a block B_i is on level i will mean that the block is contained in a chain of blocks

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

Def. 3.1: Let $A = a_1 \ldots a_n \in \{0,1\}^n$. We define the blocks of A with respect to p in this way:

Level 1: We define the blocks on level 1 inductively. Suppose $m=0$ or $a_1 \ldots a_m$ ends with a block on level 1. If $a_{m+1} \ldots a_n$ contains a 1 , we define the next block B in this way:

Let j be the least $j>m$ such that $a_j = 1$. In position j there starts a C such that

$$0<f_C(t)<p+1 \quad \text{for} \quad t\in[l(C), r(C)-1]$$

and a), b) or c) is satisfied:

a) $f(C) = 0$.

b) $0<f(C)<p+1$ and $r(C) = n$.

c) $f(C) = p+1$.

In case a) and b) we decompose $C = BD$ such that

$$f_C(s) \leqq f(B) > f_C(t) \quad \text{for} \quad s\in B \quad \text{and} \quad t\in D .$$

B is by definition a $f(B)$-block.

In case c) we define a $(p+1)$-block B by the following conditions:

$l(B) = j$. Moreover, there does not exist a D satisfying $l(D)\in B$ and (3.6) :

(3.6) $0>f_D(t)$ for $t\in D$ and ($r(D) = n$ or $f(D) = -(p+1)$) .

$l(B) = n$ or there exists a D satisfying (3.6) and $l(D) = r(B)+1$.

Level q: We suppose the blocks on level $(q-1)$ are defined. Let B be a block on level $(q-1)$. If $(q-1)$ is odd, we decompose

B (uniquely) by induction in this way:

$B = 1_{i_1} B_1 1_{i_2} \ldots 1_{i_m} B_m 1_{i_{m+1}}$ such that for $i \in \{1,\ldots,m\}$

$$0 > f_{B_i}(t) \geq f(B_i) \quad \text{for} \quad t \in B_i$$

and there exists D_i satisfying (3.7):

$$(3.7) \quad \begin{cases} B = \ldots B_i D_i \ldots \\ 0 \neq f_{D_i}(t) \quad \text{for} \quad t \in D_i \ . \\ f(D_i) = -f(B_i) \ . \end{cases}$$

By definition B_i is a $(-f(B_i))$-block on level q .

If $(q-1)$ is even, we decompose B (uniquely) by induction in this way:

$B = 0_{i_1} B_1 0_{i_2} \ldots 0_{i_m} B_m 0_{i_{m+1}}$ such that for $i \in \{1,\ldots,m\}$

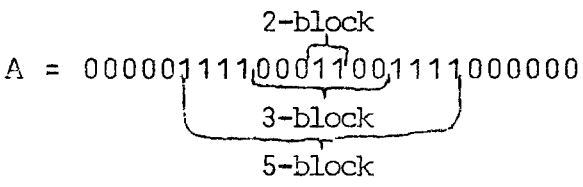
$$0 < f_{B_i}(t) \leq f(B_i) \quad \text{for} \quad t \in B_i$$

and there exists D_i satisfying (3.7).

By definition B_i is a $f(B_i)$-block on level q .

(3.8) If B is a q-block, we write $\text{type}(B) = q$. We denote the level of B by $\text{level}(B)$.

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



The main part of our proofs is how the blocks move by applying

$\theta_{E_k+\ldots+E_{k+p}}$. 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 $(j=1,\ldots,p+1)$. 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:

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

$$(p-1): \quad \alpha_{p-1}X_{p-1} = 2Y+2\gamma_p X_p .$$

$$(p-2): \quad \alpha_{p-2}X_{p-2} = 3Y+2\gamma_{p-1}X_{p-1}+4\gamma_p X_p .$$

$$(p-3): \quad \alpha_{p-3}X_{p-3} = 4Y+2\gamma_{p-2}X_{p-2}+4\gamma_{p-1}X_{p-1}+6\gamma_p X_p .$$

$$\vdots$$

$$(1) \quad \alpha_1 X_1 = pY+(2\gamma_2 X_2+\ldots+2(p-1)\gamma_p X_p) .$$

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 $j\in\{1,\ldots,p\}$ the equation (j) is defined by

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

$$X_j = 0 \qquad \text{If } \gamma_j = 0 .$$

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

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

We say that PER is a period for $A\in\{0,1\}^n$ with respect to (3.9) if $\theta^{PER}(A) = A$.

THEOREM 3.2: We determine the periods of the sequences generated by (3.9) 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 $i = 1,\ldots,p+1$.

a) Suppose $\gamma_{p+1} \neq 0$ and $\gamma_i \neq 0$ for an integer $i<p+1$. Suppose $Y,X_1,\ldots,X_p$ 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 a period for A .

We prove this theorem in Section 4 and 5.

If $w(A) = k+p+1$ and $q = \sup\{i:\gamma_i\neq 0\}<p+1$, it is an easy consequence of Lemma 5.1 and 5.2 that $w(A)\geq k+p+1-q$. Instead of $E_k+\ldots+E_{k+p}$ we can therefore use $S' = E_{(k+p+1-q)}+\ldots+E_{k+p} = E_{k'}+\ldots+E_{k'+p'}$ where $k' = k+p+1-q$ and $p' = q-1$. Moreover the blockstructure of A with respect to respectively p and

p' are equal. Specially $\gamma_{p'+1} \neq 0$. Hence we can use the theorem.

If $k<w(A)<k+p+1$ and $w(A) = \sup_i w(\theta^i(A))$, we can use $S' = E_k+\ldots+E_{w(A)-1} = E_k+\ldots+E_{k+p'}$ where $p' = w(A)-1-k$.

4. OUTLINES OF THE PROOF.

In this and the next section we will prove Thm. 3.2. The proofs of the Lemmas 4.2, 4.4, 4.5, 4.7, 4.8, 4.9, 4.11 and 4.13 are contained in Section 5. First we prove a Lemma which shows how $\theta = \theta_{E_k+\ldots+E_{k+p}}$ works. We need a definition:

(4.1) If $a = 1$, then $a' = 0$. If $a = 0$, then $a' = 1$.
If $C = a_i\ldots a_j$, then $C' = a_i'\ldots a_j'$.

Lemma 4.1: Let $A = a_1\ldots a_n$ and $k\leq w(A)\leq k+p+1$.

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

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

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

Proof: b) and c) are easily shown.

a) We prove by induction with respect to t that $w(\theta^t(A)) = w(A)-f_1(t)$ and $\theta^t(A) = a_{t+1}\ldots a_n a_1'\ldots a_t'$.

We divide the basis step into 3 cases.

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

$k+p+1-f_1(1) = w(A)-f_1(1) \leq k+p+1$ implies $f_1(1)>0$. Hence, $a_1 = 1$ and $w(a_2,\ldots,a_n) = k+p$. We get $a_{n+1} = a_1+(E_k+\ldots+E_{k+p})(a_2,\ldots,a_n) = 1+1 = 0 = a_1'$.

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

$k \leq w(A)-f_1(1) = k-f_1(1)$ implies $f_1(1)<0$. Hence, $a_1 = 0$ and $w(a_2,\ldots,a_n) = k$. We get $a_{n+1} = a_1+(E_k+\ldots+E_{k+p})(a_2,\ldots,a_n) = 0+1 = 1 = a_1'$.

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

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

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

Q.E.D.

Thm. 3.2 b) is easily shown. In the remaining part of this section we prove Thm. 3.2 a). First we reduce the problem.

Lemma 4.2: There exists i such that $\theta^i(A)$ satisfies

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

(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.

We therefore suppose that

$$(4.2)\quad \begin{cases} A \text{ ends with a } (p+1)\text{-block.} \\ w(A) = k+p+1 \ . \\ A \text{ starts with } 0 \text{ or a } (p+1)\text{-block.} \end{cases}$$

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

(4.3) $B = H(B)K(B)$ where $f_B(t) \leq p+1$ for $t \in H(B)$ and $f_B(1(K(B))) = p+2$ or $K(B) = \emptyset$.

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

Definition 4.3: a) We decompose A (by induction) such that

$$A = 0^{i_1} B_1 T_1 0^{i_2} \ldots B_m T_m 0^{i_{m+1}} B_{END}$$

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

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

(2) $f(T_i) = -type(B_i)$.

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

$$K(B) = 1_{i_1} B_1 T_1 1_{i_2} \ldots 1_{i_m} B_m T_m 1_{i_{m+1}}$$

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

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

(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 $1(B) \in T$ where T is a tail, it is easy to see that B is contained in T . Furthermore, if $1(B) \in H(B_*)$ where B_* is a block, B is contained in $H(B_*)$. If B is a block we define

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

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

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

Lemma 4.4: There is a bijektiv 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 $1(\hat{B}) = 1(B)+$(the number of positions in $H(B)$). $r(\hat{B}) = r(B)+$(the number of positions in T).

Furthermore,

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

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

We now construct a measure d which measures how much to the left in A a block is. We do the convention that B always denotes a block. If $type(B) = q$, then we define

$$(4.6) \quad \Delta_B = \sum_{l(B_*)<l(B)} \min\{q,type(B_*)\} + \sum_{r(B_*)<l(B)} \min\{q,type(B_*)\} .$$

$$(4.7) \quad d(B) = l(B)-\Delta_B .$$

Lemma 4.6 explains why d is a good measure. First we need a lemma and more notation:

$$(4.8) \quad \Delta(C) = \sum_{B_*<C} 2type(B_*) .$$

Lemma 4.5: Suppose $type(B) = q$.

a) the number of positons in $H(B) = q+\Delta(H(B))$.

b) If B has a tail, then $\Delta_{\hat{B}} = \Delta_B+\Delta(H(B))$.

Otherwise, $\Delta_{\hat{B}} = \Delta_B-q$.

Lemma 4.6: If B is a block in A , then $d(\hat{B}) = d(B) + type(B)$.

Proof: We use Lemma 4.4 and 4.5. We suppose first that

B has a tail:

$$d(\hat{B}) = l(\hat{B})-\Delta_{\hat{B}} = l(B)+(\text{the number of positions in } H(B))-\Delta_B-\Delta(H(B)) = d(B)+type(B) .$$

Otherwise,

$$d(\hat{B}) = l(\hat{B})-\Delta_{\hat{B}} = l(B)-\Delta_B+type(B) = d(B)+type(B) .$$

Q.E.D.

Lemma 4.7: There exists an integer $s>0$ such that $\theta^{n+s}(A)$ satisfies (4.2).

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

We define

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

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

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

Lemma 4.8: There is a bijektiv correspondence $\hat{B} \to \varphi(B)$: {The blocks in A} $\to$ {the bloeks in $\varphi(A)$} such that $type(\varphi(B)) = type(B)$, $m(\varphi(B)) = m(B)$ 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 $r(\varphi(B_{END})) = n$.

We now compute $d(\varphi(B))$. Then we need the following lemma.

Lemma 4.9:

a) $s_A = \Sigma 2\text{type}(B_*)+(p+1)$.
$\hat{B}_*$ circles around

b) Suppose $\text{type}(B) = q$. If $\hat{B}$ do not circle around, then

$$\Delta_{\varphi(B)} = \Delta_{\hat{B}}-\Sigma 2\min\{q, \text{type}(B_*)\}$$
$\hat{B}_*$ circles around

Otherwise,

$$\Delta_{\varphi(B)} = \Delta_{\hat{B}}-\Sigma 2\min\{q, \text{type}(B_*)\}+n-\alpha_q$$
$\hat{B}_*$ circles around

Lemma 4.10: Let B be a block in A such that $\text{type}(B) = q$. We define

$$X(B) = \Sigma 2(\text{type}(B_*)-\min\{q, \text{type}(B_*)\})+p+1-q.$$
B_* circles around

If $\hat{B}$ does not circle around, then

$$d(\varphi(B)) = d(B)-X(B) .$$

Otherwise, $d(\varphi(B)) = d(B)-X(B)+\alpha_q$.

Proof: Suppose $\hat{B}$ does not circle around. By lemma 4.8 and 4.9b) we get

$$d(\varphi(B)) = l(\hat{B})-s_A-\Delta_{\hat{B}}+\Sigma 2\min\{q, \text{type}(B_*)\}$$
$$B_* \text{ circles around}$$

and the conclusion follows from Lemma 4.6 and 4.9a). If $\hat{B}$ circles around the proof is analogous. Q.E.D.

The next Lemmas tell us how to calculate $d(\varphi^s(B))$.

Lemma 4.11: Suppose B is a block in A such that $\text{type}(B) = j<p+1$. Then

a) $2 \leq d(B) \leq \alpha_j+1$.

b) B circles around by $\varphi \Leftrightarrow d(B)-X(B) \leq 1$.

We define

$$(4.11) \quad L_s(B) = X(B)+\ldots+X(\varphi^{s-1}(B)) .$$

Lemma 4.12: Suppose B is a block in A such that $\text{type}(B) = j<p+1$. Let s be a positive integer.

Suppose $t \geq 0$ is the least integer such that $d(B)+t\alpha_j-L_s(B) \geq 2$. Then

$$d(\varphi^s(B)) = d(B)+t\alpha_j-L_s(B) .$$

Moreover, B circles around t times by φ^s (i.e. there exist t different integers s' such that $0 \leqq s' < s$ and $\varphi^{s'}(B)$ circles around by φ).

Proof: We prove the lemma by induction with respect to t . The case $t = 0$ is an easy consequence of Lemma 4.11b) and 4.10.

We suppose the lemma is true for t-1 . Suppose t is the least integer such that $d(B)+t\alpha_j-L_s(B) \geqq 2$. Let s' be the least integer such that $\varphi^{s'-1}(B)$ circles around by φ . By Lemma 4.10

$$d(\varphi^{s'}(B)) = d(B)+\alpha_j-L_{s'}(B) .$$

Hence,

$$\begin{aligned} & d(\varphi^{s'}(B))+(t-1)\alpha_j-L_{s-s'}(\varphi^{s'}(B)) \\ &= d(B)+t\alpha_j-(L_{s-s'}(\varphi^{s'}(B))+L_{s'}(B)) \\ &= d(B)+t\alpha_j-L_s(B) \geqq 2 . \end{aligned}$$

Hence by the induction hyphothesis

$$d(\varphi^s(B)) = d(\varphi^{s-s'}(\varphi^{s'}(B)) = d(B)+t\alpha_j-L_s(B) .$$

Q.E.D.

The next lemma gives that the blockstructure completely determines A .

Lemma 4.13: Suppose $d(B) = d(\varphi^s(B))$ for every block B in A , and B circles around X_q times by φ^s if

type(B) = q<p+1 . Then $A = \varphi^s(A)$.

Before the final step in our proof we need two observations.

(4.12) If type(B) = p+1 , then X(B) = 0 . Hence d(B) = d(φ(B)) .

(4.13) If type(B) = j≦p and $L_s(B) = t\alpha_j$, then $d(\varphi^s(B)) = d(B)$ and B circles around t times by φ^s .
(this is an easy consequence of Lemma 4.11a) and 4.12).

THE FINAL STEP OF THE PROOF:

By (4.12) $d(\varphi^Y(B)) = d(B)$ for every (p+1)-block. $\varphi^Y(A) = A$ follows from Lemma 4.13 and the following claim:

d(B) = $d(\varphi^Y(B))$ for every j-block, and every j-block circles around X_j times by φ^Y .

We prove this claim by induction with respect to j (the opposite way).

We prove the case j = p in the following way: If B is a p-block, X(B) = 1 . Hence

$$L_Y(B) = X(B)+\ldots+X(\varphi^{Y-1}(B)) = Y = \alpha_p X_p$$

and the claim follows from (4.13).

Suppose the claim is true for p,...,j+1 . Suppose B is a block such that type(B) = j . We observe that

$$X(\varphi^i(B)) = \Sigma 2(\text{type}(B_*)-\text{type}(B))+p+1-j \ .$$

$\varphi^i(B_*)$ circles around

$\text{type}(B_*)>\text{type}(B)$

By the induction hypothesis each block B_* satisfing $\text{type}(B_*) = i>\text{type}(B)$ circles around X_i times by φ^Y. Hence,

$$L_Y(B) = X(B)+\ldots+X(\varphi^{Y-1}(B))$$

$$= \Sigma X_{\text{type}B_*} 2(\text{type}(B_*)-\text{type}(B))+Y(p+1-j)$$

$$\text{type}(B_*)>\text{type}(B)$$

$$= \sum_{i=j+1}^{p} 2\gamma_i(i-j)X_i+Y(p+1-j) = \alpha_j X_j \ .$$

and the claim follows from (4.13).

Finally we compute φ^Y. By Lemma 4.9a) φ^Y is equal to θ applied

$$\sum_{q=0}^{y-1} (n+s_{\varphi^q(A)}) = \sum_{q=0}^{y-1} (n+p+1+ \Sigma 2\text{type}(B_*))$$

$\varphi^q(B)$ circles around

$$= Y(n+p+1)+2(X_1+\ldots+X_p) \text{ times.}$$

Q.E.D.

5. THE LEMMAS.

In this section we prove the Lemmas 4.2, 4.4, 4.5, 4.7, 4.8, 4.9, 4.11 and 4.13. The key lemma is Lemma 5.1. We need more notation. We define

(5.1) If $K(B) = 1_{i_1} B_1 T_1 \ldots 1_{i_m} B_m T_m 1_{i_{m+1}}$ is as in Def. 4.3, then $K\tilde{}(B) = 1_{i_1} B_1' T_1' \ldots 1_{i_m} B_m' T_m' 1_{i_{m+1}}$

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

(5.2) $w(A) = k+p+1$, and A does not have the form $A = B \ldots B_*$ where $type(B) < type(B_*)$.

(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) $\theta^h(A) = DH(B)'K\tilde{}(B)$

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

3) $w(\theta^t(A)) \geq k+p+1-type(B)$ for $1 \leq t \leq h$.

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

b) There exists a bijektiv correspondance $B_* \to B_*^h$: {the blocks in A}$\to${the blocks in A^h} satisfying $type(B_*) = type(B_*^h)$, $m(B_*) = m(B_*^h)$ 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) $B^h = K\tilde{}(B)1_{type(B)}$.

c) 1) $\delta = \delta(\theta^h(A))$ exists and $type(B) \leq \delta < 1(K(B))$.

We decompose $A^h = D_1 D_2 K(\mathcal{T}B)1_{type(B)}$ where $r(D_1) = \delta$.

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

3) $\theta^{h+\delta}(A) = D_2 K(\mathcal{T}B) D_1'$.

4) $w(\theta^{h+t}(A)) \geq k+p+1-type(B)$ for $1 \leq t \leq \delta$.

We denote D_1 by $T(B)$, i.e. $\theta^{h+\delta}(A) = D_2 K(\mathcal{T}B) T(B)'$. $T(B)$ is the tail of B as in Def. 4.3.

d) There exist a bijektiv correspondence $B_*^h \to B_*^{h+\delta}$: {the blocks in A^h} $\to$ {the blocks in $\theta^{h+\delta}(A)$} satisfying $type(B_*^{h+\delta}) = type(B_*)$, $m(B_*^{h+\delta}) = m(B_*)$ and:

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

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

3) $B^{h+\delta} = K(\mathcal{T}B) D_1'$:

Proof:

Proof of a): We put $z = l(H(B))$. We get from Lemma 4.1a) that $\theta^z(A) = K(B)DH(B)'$.

If $K(B) \neq \emptyset$, then $w(\theta^z(A)) = k$ and by using Lemma 4.1a) and 4.1c) several times we get $\theta^h(A) = DH(B)'K(\mathcal{T}B)$ and $w(\theta^h(A)) = k$. 2) and 3) are easily shown.

Proof of b-3): We need only 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 succeeded by a D_* in A^h satisfying:

(5.4) $0>f_{D_*}(t)$ for $t\in D_*$

$r(D_*) = n+type(B)$ or $f(D_*) = -min\{f(B_*),p+1\} = -type(B_*)$

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 $type(B) = p+1$, we get

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

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

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

If $C_* = \emptyset$, we have $type(B_*)<type(B)$. Hence B_* is suceeded by $H(B)'$ and $f(H(B)')<-type(B)$ 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 $H(B) = 1_{i_1}B_1 1_{i_2}B_2\ldots B_m 1_{i_{m+1}}$ where $B_1,\ldots,B_m$ are the blocks on level 2 in $H(B)$. We get

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

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

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

We get

$H(B)' = \ldots B_1' C_1' \ldots$

$0 < f_{B_1'}(t) \leq f(B_1') = \text{type}(B_1)$ for $t \in B_1'$

$0 > f_{C_1'}(t) \geq f(C_1') = -\text{type}(B_1)$ for $t \in C_1'$.

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 $B_2, \ldots, B_m$ analogously.

Next we prove by induction with respect to i for blocks $B_* < H(B)$:

(5.5) If $\text{level}(B_*) = i$, then B_*' is a block in A^h satisfying $\text{type}(B_*') = \text{type}(B_*)$ and $\text{level}(B_*') = \text{level}(B_*)-1$.

We have done the basistep $i = 2$. Suppose (5.5) is true for $(i-1)$ and $\text{level}(B_*) = i-1$. Suppose first that $(i-1)$ is even. Then

$$B_* = 0_{i_1} B_1 0_{i_2} B_2 \ldots B_m 0_{i_{m+1}}$$

where $B_1, \ldots, B_m$ are the blocks on level i in B_* . Moreover, B_* has the form $B_* = 0_{i_1} B_1 C_1 \ldots$ where C_1 satisfies

$0 > f_{C_1}(t) \geq f(C_1) = -f(B_1)$ for $t \in C_1$.

Hence,

$B_*' = 1_{i_1} B_1' C_1' \ldots$.

$0 < f_{C_1'}(t) \leq f(C_1') = -f(B_1')$ for $t \in C_1'$.

$0 > f_{B_1'}(t) \geq f(B_1') = -\text{type}(B_1)$ for $t \in B_1'$

Hence B_1' is a block in A^h satisfying (5.5). We treat $B_2,\ldots,B_m$ analogously. If (i-1) is odd, then B_* has the form $B_* = 1_{i_1} B_1 1_{i_2} \ldots B_m 1_{i_{m+1}}$ where $B_1,\ldots,B_m$ are the blocks on level i contained in B_*. The proof is analogous with the case "(i-1) is even".

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

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

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

$$f(B^h) = f(K(B))+p+1 = f(K(B))+f(H(B)) = f(B) .$$

Proof of b-2): $K(B) = 1_{i_1} B_1 T_1 1_{i_2} \ldots B_m T_m 1_{i_{m+1}}$ where B_i is the blocks in K(B) which has a tail T_i. We get

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

We treat only $B_1 T_1$. $B_2 T_2,\ldots,B_m T_m$ are treated analogously. As in b-3) 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

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

Obviously $B^h = K\tilde{(}B)1_{p+1}$ has the form $B^h = \ldots T_1' C_1 \ldots$ 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 $\text{type}(B_1)$ such that $\text{level}(B_1^h) = \text{level}(B_1)$.

At last we prove as in b-3) that: For all $B_*<T_1$, B_*' is a block in A^h such that $\text{type}(B_*') = \text{type}(B_*)$ and $\text{level}(B_*') = \text{level}(B_*)+1$.

Proof of c): We have $\theta^h(A) = DH(B)'K\tilde{(}B)$. We prove that $\theta^h(A)$ has the form $\theta^h(A) = D_1 D_2 K\tilde{(}B)$ 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, $D = D_1 D_2$ where D_1 satisfies (5.6).

We choose D_1 maximal with respect to (5.6). We put $\delta(\theta^h(A)) = r(D_1)$ and we get easily that 1) and 2) are true. 3) and 4) follows from Lemma 4.1.

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

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

If $D_2 = \ldots B_*^h D_* \ldots$ where D_* satisfies (5.7), there is nothing to prove. Otherwise $A^h = \ldots B_*^h C_*$ where $f_{C_*}(t)<0$ for $t\in C_*$. We obviously have $C_* = C_1 1_{type(B)}$ where $f(C_1)<-type(B)$. Put $D_* = C_1 T(B)'$ and we are done.

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

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

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

$$1(C)\in K\tilde{}(B)T(B)'$$
$$f(C)\leqq f_C(t)<0 \quad \text{for} \quad t\in C$$
$$r(C) = n \quad \text{or} \quad f(C) = -(p+1) .$$

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

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

Q.E.D.

Lemma 5.2: Suppose $w(A) = k+p+1$ and $A = B_1 C_1 DB$ where $type(B_1)<type(B)$ and

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

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

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

There exists a bijektiv correspondance $B_* \to B_*^h$: {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) $B^h = BB_1'C_1'$.

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) is trivial and 2) is proved in the same way as Lemma 5.1, b-1).

Q.E.D.

Proof of Lemma 4.2: The lemma follows easily by using Lemma 5.1 and 5.2 several times.

Q.E.D.

Proof of Lemma 4.4, 4.7 and 4.8: Suppose $A = 0_{i_1}B_1T_1 0_{i_2}B_2T_2 \dots B_mT_m 0_{i_{m+1}} B_{END}$ where $B_i = H(B_i)K(B_i)$ and T_i is the tail of B_i . We show Lemma 4.4 by using Lemma 5.1b) and d) respectively $m+1$ and m times. Then Lemma 4.7 follows from 5.1c) ($s_A = \delta(\theta^n(A))$) , and Lemma 4.8 follows from 5.1d).

Q.E.D.

Lemma 5.3: Suppose $C < A$, $f(C) = 0$, C starts with a block and

$0<|f_C(t)|\leq p+1$ for $t\in C$ and $t \neq r(C)$.

Then the length of $C = \Delta(C)$.

Proof: The proof is by induction with respect to j = the number of blocks contained in C . If $j = 1$, then $C = 1_q 0_q$ or $0_q 1_q$ and the claim is true. Suppose the claim is true for $1,\ldots,j$. 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

$$B = 1_{i_1} C_1 1_{i_2} \ldots C_q 1_{i_{q+1}} \quad \text{and} \quad E = 0_{j_1} D_1 0_{j_2} \ldots D_r 0_{j_{r+1}}$$

where D_j and C_i satisfy the hyphothesis of the lemma and

$$i_1+\ldots+i_{q+1} = j_1+\ldots+j_{r+1} = \text{typeB} .$$

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

Q.E.D.

Proof of Lemma 4.5:a) $H(B)$ is of the form $H(B) = 1_{i_1} C_1 1_{i_2} C_2 \ldots C_m 1_{i_{m+1}}$ where C_i satisfies Lemma 5.3. Moreover, $i_1+\ldots+i_{m+1} = \text{type}(B)$. The result follows from Lemma 5.3.

b) We use Lemma 4.4. If B has a tail, then for all $B_* < H(B)$: B_* is to the right of $1(B)$ and $\hat{B}_*$ is to the left of $1(\hat{B})$. Hence, the claim follows.

If $B < H(B_1)$, then $1(B_1) < 1(B)$ and $1(\hat{B}_1) > 1(\hat{B})$. If $B < T(B_1)$, then $r(B_1) < 1(B)$ and $r(\hat{B}_1) > 1(\hat{B})$. In both these cases $\min\{\text{type}(B_1), q\} = q$ and the result follows.

Q.E.D.

Proof of Lemma 4.9: a) We prove easily that $\hat{a}_1 \ldots \hat{a}_{s_A}$ is equal to

$$0^{i_1} C_1 0^{i_2} C_2 \ldots C_m 0^{i_{m+1}}$$

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

b) Suppose B circles around (Otherwise, the claim is trivial). We observe

$$l(\varphi(B_*)) \geqq l(\varphi(B)) \Leftrightarrow l(\hat{B}_*) \in \{l(\hat{B}), \ldots, s_A\} = m \ .$$

$$r(\varphi(B_*)) \geqq l(\varphi(B)) \Leftrightarrow r(\hat{B}_*) \in m \text{ or } B_* = B_{END} \ .$$

$$\sum_{l(\hat{B}_*)\in m} \min\{q, type(B_*)\} + \sum_{r(\hat{B}_*)\in m} \min\{q, type(B_*)\} = \sum_{B_* \text{ circles around}} 2\min(q, type(B_*)) - \Delta_{\hat{B}}$$

Hence,

$$\Delta_{\varphi(B)} = \sum_{B_* \text{ block}} 2\min\{q, type(B_*)\} - \left(\sum_{B_* \text{ circles around}} 2\min(q, type(B_*)) - \Delta_{\hat{B}} + q\right) \ .$$

Since $\sum_{B_* \text{ block}} 2\min\{q, type(B_*)\} = n+q-\alpha_q$ the conclusion follows.

Q.E.D.

As in the proof of 4.5.a)we get

(5.8) the length of $B = |f(B)| + \Delta(B)$

where B is a block.

Lemma 5.4: If $\hat{B}$ circles around, then

$$l(\hat{B}) - 1 \leqq \sum_{r(\hat{B}_*) < l(\hat{B})} 2type(B_*) + \sum_{l(\hat{B}_*) < l(\hat{B}) < r(\hat{B}_*)} type(B_*) + (p+1)$$

Proof: We prove the lemma by induction with respect to $j = \text{level}(B)$. If $j = 1$, then $\hat{A}$ is of the form $\hat{A} = 0_{i_1}\hat{B}_1 0_{i_2}\hat{B}_2 \ldots 0_{i_s}\hat{B}_s 0_{i_{s+1}}\hat{B}\ldots$ where $\text{level}(B_i) = 1$. By (5.8)

$$l(B)-1 = (i_1+\ldots+i_{s+1})+(f(B_1)+\ldots+f(B_s))+(\Delta(B_1)+\ldots+\Delta(B_s)) .$$

Moreover,

$$f_1(l(\hat{B})-1) = -(i_1+\ldots+i_{s+1})+(f(B_1)+\ldots+f(B_s))\geq -(p+1) .$$

Hence,

$$l(\hat{B})-1 \leq 2(f(B_1)+\ldots+f(B_s))+(\Delta(B_1)+\ldots+\Delta(B_s))+p+1 .$$

and the claim follows.

Suppose the lemma is true for j. Suppose $\text{level}(B^*) = j$ is even (if j is odd the proof is analogous) and that

$$\hat{B}^* = 0_{i_1}\hat{B}_1 0_{i_1}\hat{B}_2 0_{i_3}\ldots 0_{i_s}\hat{B}_s 0_{i_{s+1}}\hat{B}\ldots$$

where $\text{level}(B_i) = \text{level}(B) = j+1$. By (5.8)

$$l(\hat{B})-l(\hat{B}^*) = (i_1+\ldots+i_{s+1})+(f(B_1)+\ldots+f(B_s))+(\Delta(B_1)+\ldots+\Delta(B_s))$$

Moreover,

$$f_{B^*}(l(\hat{B})-1) = -(i_1+\ldots+i_{s+1})+(f(B_1)+\ldots+f(B_s))\geq -f(B^*) .$$

Hence,

$$l(\hat{B})-l(\hat{B}^*) \leq (\Delta(B_1)+\ldots+\Delta(B_s))+2(f(B_1)+\ldots+f(B_s))+f(B^*)$$

Since $l(B)-1 = (l(B)-l(B^*))+l(B^*)-1$ and that the lemma is true for B^*, we get the desired conclusion.

Q.E.D.

We let $[i,j\rangle$ denote $\{i,\ldots,j-1\}$. We define for $q \leq p$:

$$(5.9) \qquad d^q(i,j) = (j-i) - \sum_{l(B_*)\in[i,j\rangle} \min\{q,type(B_*)\} - \sum_{r(B_*)\in[i,j\rangle} \min\{q,type(B_*)\}$$

Lemma 5.5: Suppose $type(B) \geq q$ and $i<j = l(B)$

a) $d^q(i,j) \geq 0$

b) If $i = l(B^*)$ where $type(B^*)>q$, then $d^q(i,j) \geq 1$.

c) If there does not start or end any block in positon i , then $d^q(i,j) \geq 1$.

d) If $i = r(B^*)$ where $type(B^*)>q$, then $d^q(i,j) \geq 2$.

Proof: a) It is sufficient to find an integer i_0 such that $i<i_0 \leq j$ and $d^q(i,i_0) \geq 0$. (Next we can find an integer i_1 such that $i_0<i_1 \leq j$ and $d^q(i_0,i_1) \geq 0$ etc.). We divide the proof into 6 cases. In all these cases B_i is a block and C_i satisfies $A = \ldots B_i C_i \ldots$ and

$$(5.10) \qquad 0 \neq |f_{C_i}(t)| \neq |f(C_i)| = type(B_i) \quad \text{for} \quad t\in[l(C_i),r(C_i)\rangle .$$

We want to use case 1),...,Case6) in the proof of b), c) and d). We therefore prove more than we need in some of the cases.

Case 1: There does not start or end a block in position i . Put $i_0 = i+1$, and we get $d^q(i,i_0) = 1$.

Case 2: $i = r(B_1)$ and $B<C_1$. We observe that $type(B_1)>q$. There exists a block B_s such that $B_s<C_1$, $level(B_s) = level(B_1)$,

$\text{type}(B_s) \geqq q$ and $l(B_s) \leqq l(B) = j$. Put $i_0 = l(B_s)$. Without loss of generality we suppose $\text{level}(B_1)$ is odd. B_1C_1 has therefore the form

$$B_1C_1 = B_1 0_{i_1} B_2 0_{i_2} \ldots B_{s-1} 0_{i_{s-1}} B_s \ldots$$

where $\text{level}(B_i) = \text{level}(B_1)$ for $i = 2,\ldots,s$. If $f_{C_1}(l(B_s)-1) \geqq -q$, then $f_{C_1}(r(B_s)) \geqq 0$ which is a contradiction by (5.10). Hence,

$$f_{C_1}(l(B_s)-1) = -(i_1+\ldots+i_{s-1})+f(B_2)+\ldots+f(B_{s-1}) < -q \ .$$

Hence,

(5.11) $\quad (i_1+\ldots+i_{s-1}) > q+f(B_2)+\ldots+f(B_{s-1})$

From (5.8) and (5.11) we get

$$(l(B_s)-r(B_1))-1 = \text{the length of } "0_{i_1} B_2 0_{i_2} \ldots B_{s-1} 0_{i_{s-1}}"$$

$$= (i_1+\ldots+i_{s-1})+(\Delta(B_2)+\ldots+\Delta(B_{s-1}))+(f(B_2)+\ldots+f(B_{s-1}))$$

$$> (\Delta(B_s)+\ldots+\Delta(B_{s-1}))+2(f(B_2)+\ldots+f(B_{s-1}))+q$$

$$\geqq \sum_{l(B_*)\in[i_1 0_1\rangle} \min\{q,\text{type}(B_*)\} + \sum_{r(B_*)\in[i,i_0\rangle} \min\{q,\text{type}(B_*)\} \ .$$

Hence, $d^q(i,i_0) \geqq 2$.

Case 3: $i = r(B_1)$ and $B \not< C_1$. There exists a chain of blocks $B_1 < \ldots < B_t$ such that $\text{level}(B_i) = \text{level}(B_{i+1})+1$, $B \not< B_i$ for $i = 1,\ldots,t-1$, and $\text{level}(B_t) = 1$ or $B < B_t$. We observe that $r(C_t)$ is not an endposition of any block.

Hence there exists a chain of blocks $B_1 < B_2 < \ldots < B_s$ such that $r(C_i) = r(B_{i+1})$ for $i = 1,\ldots,s-1$, and such that

$B<C_s$ or $r(C_s)$ is not an endpositon of any block. As in the proof of Lemma 4.9.a) we get

$$r(C_i)-r(B_i) = \text{the length of } C_i = \text{type}(B_i)+\Delta(C_i) .$$

Hence,

$$d^q(r(B_i),r(C_i))>0 \text{ if } \text{type}(B_i)>q, \text{ else } d^q(r(B_i),r(C_i)) = 0 .$$

If $B<C_s$ we find as in Case 2) an i_0 such that $d^q(r(B_s),i_0)\geq 2$. Hence,

$$d^q(i,i_0) = d^q(r(B_1),r(C_1))+\ldots+d^q(r(B_{s-1}),r(C_{s-1}))+d^q(r(B_s),i_0)\geq 2 .$$

Otherwise, we put $i_0 = r(C_s)+1$. Then we get

$d^q(r(B_s),i_0)\geq 1$. Hence, $d^q(i,i_0)\geq 1$.

If $\text{type}(B_1)>q$, we observe that $d^q(i,i_0)\geq 2$.

Case 4: $i = l(B_1)$ and $B<B_1$. We observe that $\text{type}(B_1)>q$. We let B_s be a block such that $B_s<B_1$, $\text{level}(B_s) = \text{level}(B_1)+1$, $\text{type}(B_s)\geq q$ and $l(B_s)\leq l(B) = j$. Put $i_0 = l(B_s)$. Without loss of generality we suppose $\text{level}(B_1)$ is odd. Then B_1 has the form

$$B_1 = 1^{i_1}B_2 1^{i_2}\ldots B_{s-1}1^{i_{s-1}}B_s\ldots$$

where $B_2,\ldots,B_s$ are all blocks in B_1 such that $\text{level}(B_i) = \text{level}(B_1)+1$ for $i = 2,\ldots,s$. Since $f_{B_1}(r(B_s))>0$ we get

$$q<f_{B_1}(l(B_s)-1) = (i_1+\ldots+i_{s-1})-(|f(B_2)|+\ldots+|f(B_{s-1})|) .$$

The remaining part of the proof is analogous with the proof of Case 2), and we get $d^q(i,i_0)\geq 1$.

Case 5: $i = l(B_1)$ and $B<C_1$. By (5.8)

(5.12) $r(B_1)-l(B_1)+1 = \text{length of } B_1 = |f(B_1)|+\Delta(B_1)$.

Since $\text{type}(B_1)>q$, we get $d^q(i,r(B_1))\geq 0$. By Case 2) there exists an $i_0\leq j$ such that $d^q(r(B_1),i_0)\geq 2$. Hence $d^q(i,i_0)\geq 2$.

Case 6: $i = l(B_1)$ and $B<B_1C_1$. By (5.12) we get $d^q(l(B_1),r(B_1))\geq -1$. By Case 3) there exists an $i_0\leq j$ such that $d^q(r(B_1),i_0)\geq 1$. Hence, $d^q(i,i_0)\geq 0$. If $\text{type}(B_1)>q$, we observe that $d^q(i,i_0)>0$.

b) follows from a) and Case 4), 5) and 6). c) follows from a) and Case 1). d) follows from a) and Case 2) and 3).

Q.E.D.

Proof of Lemma 4.11: We prove b) first. In the proof of b) B_* denotes a block which circles around by φ . We suppose $\text{type}(B) = q$. First we suppose B circles around. Then we have

$$d(B)-X(B) = d(\hat{B})-q-X(B)$$
$$= d(\hat{B})-\sum_{B_* \text{ circles around}} 2(\text{type}(B_*)-\min\{q,\text{type}(B_*)\})-(p+1)$$

$$= l(B)-(\Sigma 2(\text{type}(B_*)-\min\{q,\text{type}(B_*)\})$$
$$l(\hat{B}_*)>l(\hat{B})$$

$$+ \Sigma(2\text{type}(B_*)-\min\{q,\text{type}(B_*)\})+\Sigma 2\text{type}(B_*)+(p+1))\leq 1$$
$$l(\hat{B}_*)<l(B)<r(\hat{B}_*) \qquad\qquad r(\hat{B}_*)<l(\hat{B})$$

by Lemma 5.4. Next we suppose that B does not circle around. By Lemma 4.9.a) we get

$$(5.13)\quad \begin{cases} d^q(1,s_A+1) = s_A-\Sigma 2\min\{\text{type}(B_*),q\} = \\ \qquad\qquad B_* \text{ circles around} \\ (p+1)+\Sigma 2(\text{type}(B_*)-\min\{\text{type}(B_*),q\}) = X(B)+q\ . \\ \qquad B_* \text{ circles around} \end{cases}$$

Because of the maximality condition in the definition of s_A there are two possibilities: $\hat{a}_{s_A+1} = 0$ or there exists a $(p+1)$-block $B^\#$ such that $l(B^\#) = s_A+1$. Hence, $[i,j]=[s_A+1,l(B)]$ satisfies Lemma 5.5 b) or c). Hence

$$(5.14)\quad d^q(s_A+1,l(\hat{B}))>0\ .$$

By (5.13) and (5.14)

$$d(\hat{B}) = 1+d^q(1,l(\hat{B})) = 1+d^q(1,s_A+1)+d^q(s_A+1,l(\hat{B}))$$
$$>1+X(B)+q\ .$$

Hence by Lemma 4.6

$$d(B)-X(B) = d(\hat{B})-q-X(B)>1$$

a) Suppose $\text{type}(B) = q$. $[i,j] = [1,l(B)]$ satisfies Lemma 5.5 b) or c). Hence,

$$d(B) = 1+d^q(1,l(B)) \geqq 2 .$$

Let s be the least integer such that $\varphi^{-s}(B)$ circles around by φ. Then by Lemma 4.10 and 4.11 b)

$$d(B) \leqq d(\varphi^{-s}(B)) = d(\varphi^{-(s-1)}(B))-X(\varphi^{-(s-1)}(B))+\alpha_q \leqq 1+\alpha_q .$$

Q.E.D.

Proof of Lemma 4.13: If we consider A, we write $d^q(1,m) = d^q(A,1,m)$. We make the following observation: Suppose $B_{q,1},B_{q,2},\ldots,B_{q,r}$ are the q-blocks in A and

$$l(B_{q,1})<l(B_{q,2})<\ldots<l(B_{q,r}) .$$

Since each of the blocks $B_{q,1},\ldots,B_{q,r}$ circles around exactly X_q times by φ^s, we observe from Lemma 5.1 that

$$l(\varphi^s(B_{q,1}))<l(\varphi^s(B_{q,2}))<\ldots<l(\varphi^s(B_{q,r})) .$$

We suppose $A \neq \varphi^s(A)$. Then there exists a block B such that $l(B) \neq l(\varphi^s(B))$ or $r(B) \neq r(\varphi^s(B))$. Hence we can suppose

$$\begin{aligned} &l(\varphi^s(B_*))<m \text{ or } l(B_*)<m \Rightarrow l(\varphi^s(B_*)) = l(B_*) \\ &r(\varphi^s(B_*))<m \text{ or } r(B_*)<m \Rightarrow r(\varphi^s(B_*)) = r(B_*) \end{aligned} \tag{5.15}$$

and that (5.15) is not true for $m+1$. It is sufficient to prove the lemma in the following two cases (If $\varphi^s(A)$ satisfies the hyphothesis in Case 1 or Case 2, the proof is identical):

Case 1): There exists a block B such that $l(B) = m$ and $l(\varphi^s(B))>m$. Moreover, if $l(\varphi^s(B^*)) = m$ for a block B^*, we

suppose that $type(B^*)>type(B) = q$.

If $r(\varphi^s(B^*) = m$ and $type(B^*)\leq q$, we get $l(\varphi^s(B^*))<m$. By (5.15) $l(B^*)<m$. Since $type(B^*)\leq q$, then $r(B^*)<m$, and by (5.15) we get $r(\varphi^s(B^*)) = r(B^*)<m$. This is a contradiction. We therefore get that $[m,l(\varphi^s(B))]$ satisfies Lemma 5.5.b), c) or d). By Lemma 5.5 $d^q(\varphi^s(A),m,l(\varphi^s(B)))>0$. Hence,

$$\begin{aligned} d(\varphi^s(B)) &= 1+d^q(\varphi^s(A),1,m)+d^q(\varphi^s(A),m,l(\varphi^s(B))) \\ &> 1+d^q(\varphi^s(A),1,m) \\ &= 1+d^q(A,1,m) = d(B) \end{aligned}$$

which is a contradiction.

Case 2: There exists a block B such that $r(B) = m$ and $r(\varphi^s(B))>m$. Moreover, we suppose that $l(\varphi^s(B_*)) \neq m$ for all blocks $\varphi^s(B_*)$ in $\varphi^s(A)$. If $r(\varphi^s(B^*)) = m$, we suppose that $type(B^*)<type(B)$.

Suppose $r(\varphi^s(B^*)) = m$, then $l(\varphi^s(B^*))<m$. By (5.15) $l(B^*)<m$. Since $type(B^*)<type(B)$, we get $r(B^*)<m$, and by (5.15) $r(\varphi^s(B^*)) = r(B^*)<m$. This is a contradiction.

Since $m(\varphi^s(B)) = m(B)$ and $l(\varphi^s(B)) = l(B)$ there exists a block B^* such that

$$l(\varphi^s(B^*)) = m+1 \quad \text{and} \quad q = type(B^*)<type(B) .$$

By (5.15) $l(B^*)>m$. By Lemma 5.5 d), $d^q(A,r(B),l(B^*))\geq 2$. Hence

$$d(\varphi^s(B^*)) = 1+d^q(\varphi^s(A),1,m+1) = 2+d^q(\varphi^s(A),1,m) = 2+d^q(A,1,m)$$

and

$$d(B^{\#}) = 1+d^{q}(A,1,m)+d^{q}(A,m,l(B^{\#})) \geq 3+d^{q}(A,1,m) > d(\varphi^{s}(B^{\#}))$$

which is a contradiction.

Q.E.D.

INDEX OF NOTATION.

$s(A)$	Kap. 2	$m(B)$	(4.4)
$0_t, 1_t$	Kap. 2	$\hat{B}, \hat{A}$	(4.5), Lem. 4.4
$w(\cdot)$	Kap. 2	Δ_B	(4.6)
$l(\cdot), r(\cdot)$	Kap. 2	$d(B)$	(4.7)
$f(\cdot)$	(3.1), (3.2)	$\Delta(C)$	(4.8)
$t \in D$	(3.3)	s_A	Lem. 4.7
$C<D$	(3.4)	$\varphi(A), \varphi(B)$	(4.9), Lem. 4.8
type(B), level(B)	3.8)	circles around	(4.10)
θ	Kap. 3	$X(B)$	Lem. 4.10
α_j, γ_j	Kap. 3	$L_s(A)$	(4.11)
a', C'	(4.1)	$K(B)$	(5.1)
B_{END}	(4.2)	$\delta(A)$	(5.3)
$H(B), K(B)$	(4.3)	$d^{q}(i,j)$	(5.9)
The tail	Def. 4.3		

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. Combinatoriel Theory, Ser. A. 21 (1976), 165-187.

3. J. SØRENG, The periods of the sequences generated by some symmetric shift registers - Part 2, Preprint.