Pacific Journal of Mathematics

SYMMETRIC SHIFT REGISTERS. II

JAN SØRENG

Vol. 98, No. 1 March 1982

PACIFIC JOURNAL OF MATHEMATICS
Vol. 98, No. 1, 1982

SYMMETRIC SHIFT REGISTERS, PART 2

JAN SØRENG

We study symmetric shift registers defined by

$$(x_1, \cdots, x_n) \longrightarrow (x_2, \cdots, x_n, x_{n+1})$$

where $x_{n+1} = x_1 + S(x_2, \cdots, x_n)$ **and** S **is a symmetric polynomial over the field** GF(2).

Introduction. In this paper we study symmetric shift registers over the field $\mathrm{GF}(2) = \{0, 1\}$. In [2] we introduced the block structure of elements in $\{0, 1\}^n$ and developed a theory about this block structure. In this paper we will use the results in [2] about the block structure to determine the cycle structure of the symmetric shift registers.

The symmetric shift register θ_S corresponding to $S(x_2, \cdots, x_n)$ where S is a symmetric polynomial, is defined by

$$\theta_S(x_1, \cdots, x_n) = (x_2, \cdots, x_{n+1}) \quad \text{where} \quad x_{n+1} = x_1 + S(x_2, \cdots, x_n) .$$

q is the minimal period of $A \in \{0, 1\}^n$ with respect to θ_S if q is the least integer such that $\theta_S^q(A) = A$. Then $A \to \theta_S(A) \to \cdots \to \theta_S^q(A) = A$ is called the cycle corresponding to A. We will for all S solve the following three problems:

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

Moreover, the problems will be solved in a constructive way, a way which will describe how the minimal periods and the number of cycles can be calculated. In [1] (see also [2]) we reduced all the problems to the case $S = E_k + \cdots + E_{k+p}$ where E_i is defined by

$$E_i(x_2, \cdots, x_n) = 1 \quad \text{if and only if} \quad \sum_{j=2}^{n} x_j = i .$$

In this paper we will only study $S = E_k + \cdots + E_{k+p}$.

I will now roughly describe the structure of the proof. First we need a definition. Suppose $\mathscr{M} \subset \{0, 1\}^n$ is a set such that for all $A \in \mathscr{M}$ there exists an $i > 0$ such that $\theta_S^i(A) \in \mathscr{M}$. Then we define Index: $\mathscr{M} \to \{1, 2, \cdots\}$ and $\psi\colon \mathscr{M} \to \mathscr{M}$ in the following way:

Let $i > 0$ be the least integer such that $\theta_S^i(A) \in \mathscr{M}$, then we define $\operatorname{Index}(A) = i$ and $\psi(A) = \theta_S^i(A)$.

In the proof we need only consider certain subsets $\mathscr{M}$ which can be represented in a nice way. Each $A \in \mathscr{M}$ is uniquely determined by its block structure. In [2] we proved how we can determine the block structure of $\psi(A)$ by means of the block structure of A. We continue in this way and calculate the block structure of $\psi^2(A)$, $\psi^3(A)$, $\cdots$. Finally, we find a q such that A and $\psi^q(A)$ have the same block structure. Hence $A = \psi^q(A)$. Then

$$\text{Index}\,(A) + \text{Index}\,(\psi(A)) + \cdots + \text{Index}\,(\psi^{q-1}(A)) \quad \text{is the minimal period of } A\,.$$

Next we give a short outline of the paper. Section 2 contains some definitions and notations. In § 3 we compute ψ for a certain subset $\mathscr{M}$ and describe the main ideas. In the §§ 4, 5 and 6 we solve the Problems 1, 2 and 3 respectively for the set $\mathscr{M}$. In § 7 we generalize the results to all $A \in \{0, 1\}^n$. This generalization will not be difficult.

2. Preliminaries. We must repeat some of the definitions from [2]. First we define the blocks of $A \in \{0, 1\}^n$ ([2], Def. 3.1). Intuitively an i-block is i consecutive 1's in A. 0_i denotes i consecutive 0's in A and 1_i denotes i consecutive 1's in A for $i \geqq 0$.

We need some notation. We write $a_1 \cdots a_n = (a_1, \cdots, a_n) \in \{0, 1\}^n$. If $A = a_1 \cdots a_n \in \{0, 1\}^n$, we define

$$f(a_i \cdots a_j) = (\text{the number of 1's in } a_i \cdots a_j) - (\text{the number of 0's in } a_i \cdots a_j)\,.$$

If $r \leqq i \leqq j \leqq s$ and ($r \neq i$ or $j \neq s$) we write $a_i \cdots a_j < a_r \cdots a_s$. Moreover, $a \wedge b$ denotes the minimum of a and b, and we define $w(\cdot)$ by $w(a_1 \cdots a_n) = \sum_{i=1}^n a_i$.

We divide the definition of 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). We will say that a block B_i is on level i if it is contained in a chain $B_1 > B_2 > B_3 > \cdots > B_i$ of blocks.

DEFINITION 2.1, *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 that $D = a_r \cdots a_s$ 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 2.1, *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 $A = 0_{i_1}B_1\, 0_{i_2}B_2 \cdots B_m 0_{i_{m+1}}$ where B_j is a 1-structure. By definition $B_1, \cdots, B_m$ are the blocks in A on level 1.

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

$$(2.1) \qquad B = 1_{i_1}B_1\, 1_{i_2}B_2 \cdots B_m 1_{i_{m+1}} \quad \text{where} \quad B_j \text{ is a 0-structure} .$$

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

$$(2.2) \qquad B = 0_{i_1}B_1\, 0_{i_2}B_2 \cdots B_m 0_{i_{m+1}} \quad \text{where} \quad B_j \text{ is a 1-structure} .$$

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 (2.1). If $i \in \{4, 6, 8, \cdots\}$ and B is a block on level i, we docompose B as in (2.2).

(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.

We illustrate Definition 2.1 by the example $p = 2$ and

$$A = 0100111001011011000010110110011101$$

$$B_1 \quad B_2 \quad B_3 \quad B_7 \quad B_9 \quad B_4 \quad B_5 \quad B_8 \quad B_6 \quad B_{10}$$

where

$$B_1, B_2, B_3, B_4, B_5 \text{ and } B_6 \quad \text{are blocks of type 1}$$

B_7 and B_8	are blocks of type 2
B_9 and B_{10}	are blocks of type 3
B_1, B_9, B_4 and B_{10}	are blocks on level 1
B_7, B_3, B_5, B_8 and B_6	are blocks on level 2
B_2	is a block on level 3 .

We establish the convention that B always denotes a block. Moreover, we suppose k and p are fixed integers such that $0 \leqq k \leqq k + p \leqq n - 1$. The block structure is always determined with respect to p and we always work with $S = E_k + \cdots + E_{k+p}$. We write $\theta = \theta_S$. These conventions do not concern § 7.

If $A = a_1 \cdots a_n$, we write $l_A(a_i \cdots a_j) = i$ and $r_A(a_i \cdots a_j) = j$. Next we define $d(B)$ which measures how far the block B is to the left in A. Suppose $A = a_1 \cdots a_n$. We define

$$\begin{aligned} d_q(a_1 \cdots a_j) = j &- \sum \{q \wedge \text{type}\,(B)\colon l_A(B) \leqq j\} \\ &- \sum \{q \wedge \text{type}\,(B)\colon r_A(B) \leqq j\} \,. \end{aligned}$$

If B is a block of A, then we define $d(B) = 0$ if $l_A(B) = 1$. Otherwise,

$$d(B) = d_q(a_1 \cdots a_j) \quad \text{where} \quad j = l_A(B) - 1 \text{ and } q = \text{type}\,(B) \,.$$

In our example in this section we get

$$\begin{aligned} (d(B_1), d(B_2), d(B_3), d(B_4), d(B_5), d(B_6)) &= (1, 5, 6, 10, 11, 15) \\ (d(B_7), d(B_8)) &= (3, 7) \\ (d(B_9), d(B_{10})) &= (2, 4) \,. \end{aligned}$$

3. Main ideas. In this section we let $\gamma_1, \cdots, \gamma_{p+1}$ be fix integers such that $\gamma_i \geqq 0$ for $i = 1, \cdots, p$ and $\gamma_{p+1} > 0$. Moreover, we will only work with $A \in \{0, 1\}^n$ which contains γ_i i-blocks for $i = 1, \cdots, p + 1$, and such that $w(A) = k + p + 1$. That is; A contains $(k + p + 1)$ 1's.

In [2] we described how the blocks move by applying the shift register. We will reformulate these results by introducing new notation. First we have to repeat a lot of the notation from [2]. Moreover, we will mention some of the problems we must solve and describe the main ideas on an example.

In [2] we defined $(i = 1, \cdots, p + 1)$

$$\begin{aligned} \alpha_i &= n + i - 2\gamma_1 - 4\gamma_2 - \cdots - 2i\gamma_i - 2i(\gamma_{i+1} + \cdots + \gamma_{p+1}) \,. \\ m &= k + p + 1 - \gamma_1 - 2\gamma_2 - 3\gamma_3 - \cdots - (p + 1)\gamma_{p+1} \,. \end{aligned} \tag{3.1}$$

Since α_i and m are very important constants, we will give an interpretation of them. To do this we define a subset $\mathscr{M} \subset \{0, 1\}^n$ in the following way

$$(3.2) \qquad A \in \mathscr{M} \Longleftrightarrow \begin{cases} w(A) = k + p + 1 . \\ A \text{ starts with } 0 \text{ or a } (p+1)\text{-block} . \\ A \text{ contains } \gamma_i \ i\text{-blocks for } i = 1, \cdots, p+1 . \\ A \text{ ends with a } (p+1)\text{-block} . \end{cases}$$

In the §§ 3–6 we will study this subset, and in § 7 we reduce the general problem to $\mathscr{M}$. It can be proved that

$$(3.3) \qquad \alpha_i \geqq \max \{d(B): B \text{ is an } i\text{-block in } A\}$$

for each $A \in \mathscr{M}$. For some $A \in \mathscr{M}$ we will have equality in (3.3). Next, we will give an interpretation of m. We use the function $f(\cdot)$ defined in § 2. From the definition of blocks we have $f(B) \geqq p + 1$ when type $(B) = p + 1$. We suppose $A \in \mathscr{M}$. Then it can be proved that

$$m = \sum \{f(B) - (p+1): B \text{ is a } (p+1)\text{-block in } A\} .$$

m is in a way the sum of the superfluous 1's in the $(p+1)$-blocks in A.

The subset $\mathscr{M}$ we defined in (3.2) is very important. We will now study the key map $\psi: \mathscr{M} \to \mathscr{M}$ defined by

(3.4) if $A \in \mathscr{M}$, then $\psi(A) = \theta^i(A)$ where i is the least integer such that $\theta^i(A) \in \mathscr{M}$. Moreover we define Index $(A) = i$.

In [2] we called this map $\varphi_{\min}$. Moreover, if $\gamma_{p+1} = 1$ then $\varphi = \varphi_{\min}$ in [2]. By Lemma 4.11 (the case $\gamma_{p+1} = 1$) and Lemma 4.13 in [2] there exists a bijective correspondence (which we also call ψ)

$$(3.5) \qquad \psi: \{\text{the blocks in } A\} \longrightarrow \{\text{the blocks in } \psi(A)\}$$

which satisfies Condition 4.9 in [2]. That implies that the map (3.5) have a lot of nice properties which we describe now. We have

$$\text{type}\,(B) = \text{type}\,(\psi(B)) \qquad \text{and} \qquad |f(B)| = |f(\psi(B))|$$

where f is as in § 2. In [2] we also write $m(B) = |f(B)|$. But the most important thing which Condition 4.9 in [2] gives us is the following: Let i be an integer such that $1 \leqq i \leqq p + 1$ and

$$B_1, \cdots, B_{\gamma_i}$$

are the i-blocks in A ordered from left to right. Then there exists an integer r (depending on i) such that

$$\psi(B_{r+1}), \psi(B_{r+2}), \cdots, \psi(B_{\gamma_i}), \psi(B_1), \cdots, \psi(B_r)$$

are the i-blocks in $\psi(A)$ ordered from left to right. Moreover, there exists an integer β (depending on i) such that

$$d(\psi(B_i)) = \begin{cases} d(B_i) - \beta & \text{when} \quad d(B_i) \leqq \beta \\ d(B_i) - \beta + \alpha_i & \text{otherwise} . \end{cases}$$

We calculated these integers r and β in [2]. Unfortunately, these calculations are very complicated. We will return to these calculations in Lemmas 3.3 and 3.4. Moreover, we proved in [2] (Lemma 4.1(b) in [2]) the following fundamental result:

(3.6) If $A, A' \in \mathscr{M}$ and there is a correspondence $B \longrightarrow B'$ between the blocks of respectively A and A' such that

$$d(B) = d(B') \quad \text{for each block } B$$

and

$$f(B) = f(B') \quad \text{for each } (p+1)\text{-block } B ,$$

then $A = A'$.

Now we need a simple way to describe the block structure. To each $A \in \mathscr{M}$ we define $(p + 1)$ vectors which contains all information about the block structure of A.

DEFINITION 3.1. Let $A \in \mathscr{M}$. Suppose $1 \leqq i \leqq p + 1$ and

$$B_1, \cdots, B_{\gamma_i}$$

are the i-blocks in A ordered from left to right. If $1 \leqq i \leqq p$, we define

$$D_i(A) = (d(B_1), \cdots, d(B_{\gamma_i})) .$$

If $i = p + 1$, then we define

$$D_{p+1}(A) = (d(B_1), \cdots, d(B_{\gamma_{p+1}})) \times (f(B_1) - (p+1), \cdots, f(B_{\gamma_{p+1}}) - (p+1))$$

where f is as in § 2. As a convention we let $D_i(A)$ be the empty vector if $\gamma_i = 0$.

The last part of $D_{p+1}(A)$, namely $(f(B_1) - (p + 1), \cdots, f(B_{\gamma_{p+1}}) - (p + 1))$ tells us how large each $(p + 1)$-block in A is. Let A be as in our example in § 2. Then $n = 34$ and by putting $p = 2$ and $k = 15$ we get $A \in \mathscr{M}$. Moreover, we get

(3.7)

$$\gamma_1 = 6 , \quad \gamma_2 = 2 , \quad \gamma_3 = 2 , \quad \alpha_1 = 15 , \quad \alpha_2 = 8 ,$$
$$\alpha_3 = 5 \quad \text{and} \quad m = 2 .$$
$$D_1(A) = (1, 5, 6, 10, 11, 15) , \quad D_2(A) = (3, 7) \quad \text{and}$$
$$D_3(A) = (2, 4) \times (1, 1) .$$

These results from [2] indicate that we must solve the following 3 problems: Let $A \in \mathscr{M}$.

1. Let i be an integer such that $1 \leqq i \leqq p+1$. How can we obtain $D_i(\psi^t(A)) = D_i(A)$?

2. How can we determine an integer t such that $D_i(\psi^t(A)) = D_i(A)$ for all $i \in \{1, \cdots, p+1\}$.

3. Suppose we have solved Problem 2. By (3.6) we have $\psi^t(A) = A$. How can we determine an integer "per" such that $\psi^t(A) = \theta^{\text{per}}(A)$?

By using Definition 3.1 we can define a map

$$g = D_1 \times D_2 \times \cdots \times D_{p+1} .$$

By (3.6) g is a bijective correspondence

$$g \colon \mathscr{M} \longrightarrow g(\mathscr{M}) .$$

One of the main ideas in this paper is that we work with $g(\mathscr{M})$ instead on $\mathscr{M}$. For example, later we will count some subsets of $\mathscr{M}$. Then we instead count the corresponding subset of $g(\mathscr{M})$. In [2] we described $g(\mathscr{M})$ in a nice way as in the following lemma.

LEMMA 3.2. (a) *If* $1 \leqq i \leqq p$, *then*

$$D_i(\mathscr{M}) = \{(t_1, \cdots, t_{\gamma_i}) \colon 1 \leqq t_1 \leqq t_2 \leqq \cdots \leqq t_{\gamma_i} \leqq \alpha_i\} .$$

We use the convention that $D_i(\mathscr{M}) = \{(\varnothing)\}$ *where* $(\varnothing)$ *is the empty vector, when* $\gamma_i = 0$.

(b)

$$\begin{aligned} D_{p+1}(\mathscr{M}) = \{&(t_1, \cdots, t_{\gamma_{p+1}}) \times (s_1, \cdots, s_{\gamma_{p+1}}) \colon t_i \geqq 0,\ s_i \geqq 0, \\ &s_1 + \cdots + s_{\gamma_{p+1}} = m,\ t_i + s_i \leqq t_{i+1}\ (i = 1, \cdots, \gamma_{p+1} - 1) \\ &\textit{and } t_{\gamma_{p+1}} + s_{\gamma_{p+1}} = \alpha_{p+1}\} . \end{aligned}$$

(c)

$$g(\mathscr{M}) = \mathop{\times}_{i=1}^{p+1} D_i(\mathscr{M}) .$$

PROOF. The lemma is a reformulation of Lemma 4.1(c).

Instead of $\psi \colon \mathscr{M} \to \mathscr{M}$ we will later use the corresponding map on $g(\mathscr{M})$. That is; we will find a map $\hat{\psi}$ such that the following diagram commutes:

$$\begin{tikzcd} \mathscr{M} \arrow[r, "g"'] \arrow[d, "\psi"'] & g(\mathscr{M}) \arrow[d, "\hat{\psi}"] \\ \mathscr{M} \arrow[r, "g"'] & g(\mathscr{M}) . \end{tikzcd}$$

$\hat{\psi}$ will be defined implicitly in Lemmas 3.3 and 3.4. We do not need an explicit definition of $\hat{\psi}$.

The next two lemmas describe how we calculate $D_i(\psi(A))$ from $D_i(A)$.

LEMMA 3.3. (a) *Suppose* $A \in \mathscr{M}$ *and* $\gamma_{p+1} = 1$. *We define* $r_p, \cdots, r_1$ *and* $\beta_p, \cdots, \beta_1$ *inductively in the following way:*

$$\begin{aligned} \beta_p &= 1 \\ r_p &= \textit{the number of } p\textit{-blocks } B \textit{ in } A \textit{ such that } d(B) \leqq \beta_p . \\ &\vdots \\ \beta_i &= (p+1-i) + 2r_{i+1} + 4r_{i+2} + 6r_{i+3} + \cdots + 2(p-i)r_p \\ r_i &= \textit{the number of } i\textit{-blocks } B \textit{ in } A \textit{ such that } d(B) \leqq \beta_i . \\ &\vdots \end{aligned}$$

Suppose $1 \leqq i \leqq p$ *and* $D_i(A) = (t_1, \cdots, t_{\gamma_i})$. *Then we have*

$$D_i(\psi(A)) = (t'_{r_i+1}, \cdots, t'_{\gamma_i}, t'_1, \cdots, t'_{r_i})$$

where

$$t'_j = \begin{cases} t_j + \alpha_i - \beta_i & \textit{if} \quad j \leqq r_i \\ t_j - \beta_i & \textit{otherwise} . \end{cases}$$

Moreover, $D_{p+1}(\psi(A)) = D_{p+1}(A)$ *and* $0 \leqq \beta_i \leqq \alpha_i$ *for* $1 \leqq i \leqq p$ *and*

$$\mathrm{Index}\,(A) = (n+p+1) + 2r_1 + 4r_2 + \cdots + 2\cdot p\cdot r_p .$$

We also write $r_i(A) = r_i$ *and* $\beta_i(A) = \beta_i$.

PROOF. (a) $\varphi(A)$ in Lemma 4.11 in [2] is equal to $\psi(A)$. By Lemma 4.11(b) and (d) in [2] $\beta_i = x_i(A)$ and $r_i = r_i$ where $x_i(A)$ and r_i are used in Lemma 4.11. Then it is not difficult to see that this lemma is a reformulation of Lemma 4.11 in [2]. $\square$

LEMMA 3.4. (a) *Suppose* $A \in \mathscr{M}$ *and* $\gamma_{p+1} > 1$. *We define* $r_{p+1}, \cdots, r_1$ *and* $\beta_{p+1}, \cdots, \beta_1$ *inductively in the following way:*

$$\begin{aligned} \beta_{p+1} &= d(B) + f(B) - (p+1) \textit{ where } B \textit{ is the first } (p+1)\textit{-block in } A . \\ r_{p+1} &= 1 \\ \beta_p &= \beta_{p+1} + 2r_{p+1} \\ r_p &= \textit{the number of } p\textit{-blocks } B \textit{ in } A \textit{ such that } d(B) \leqq \beta_p . \\ &\vdots \\ \beta_i &= \beta_{p+1} + 2r_{i+1} + 4r_{i+2} + \cdots + 2(p+1-i)r_{p+1} \\ r_i &= \textit{the number of } i\textit{-blocks in } A \textit{ such that } d(B) \leqq \beta_i . \\ &\vdots \end{aligned}$$

Suppose $1 \leqq i \leqq p$ *and* $D_i(A) = (t_1, \cdots, t_{r_i})$. *Then we have*

$$D_i(\psi(A)) = (t'_{r_i+1}, \cdots, t'_{r_i}, t'_1, \cdots, t'_{r_i})$$

where

$$t'_j = \begin{cases} t_j + \alpha_i - \beta_i & \text{if } \ j \leqq r_i \\ t_j - \beta_i & \text{otherwise} . \end{cases}$$

Suppose $D_{p+1}(A) = (t_1, \cdots, t_{r_{p+1}}) \times (s_1, \cdots, s_{r_{p+1}})$. *Then we have*

$$D_{p+1}(\psi(A)) = (t'_2, t'_3, \cdots, t'_{r_{p+1}}, t'_1) \times (s_2, \cdots, s_{r_{p+1}}, s_1)$$

where

$$t'_j = \begin{cases} t_j - \beta_{p+1} & \text{if } \ j \geqq 2 \\ t_1 + \alpha_{p+1} - \beta_{p+1} = \alpha_{p+1} - s_1 & \text{if } \ j = 1 . \end{cases}$$

Moreover, we have $0 < \beta_i < \alpha_i$ *for* $1 \leqq i \leqq p$ *and*

$$\text{Index}\,(A) = \beta_{p+1} + 2r_1 + 4r_2 + \cdots + 2(p+1)r_{p+1} .$$

We also write $r_i(A) = r_i$ *and* $\beta_i(A) = \beta_i$.

PROOF. Since ψ is equal to $\varphi_{\min}$ in [2] this is a reformulation of Lemma 4.13 in [2].

We will illustrate this lemma by our example in § 2. We get

$$\begin{array}{lll} \beta_3 = 2 + 1 = 3 & \beta_2 = 3 + 2\cdot 1 = 5 & \beta_1 = 3 + 2\cdot 1 + 4\cdot 1 = 9 \\ r_3 = 1 & r_2 = 1 & r_1 = 3 . \end{array}$$

Since $D_1(A) = (1, 5, 6, 10, 11, 15)$ and $\alpha_1 = 15$ we get

$$\begin{aligned} D_1(\psi(A)) &= (10 - \beta_1, 11 - \beta_1, 15 - \beta_1, 1 + \alpha_1 - \beta_1, 5 + \alpha_1 - \beta_1, 6 + \alpha_1 - \beta_1) \\ &= (1, 2, 6, 7, 11, 12) . \end{aligned}$$

Since $D_2(A) = (3, 7)$ and $\alpha_2 = 8$ we get

$$D_2(\psi(A)) = (7 - \beta_2, 3 + \alpha_2 - \beta_2) = (2, 6) .$$

Since $D_3(A) = (2, 4) \times (1, 1)$ and $\alpha_3 = 5$ we get

$$D_3(\psi(A)) = (4 - \beta_3, 2 + \alpha_3 - \beta_3) \times (1, 1) = (1, 4) \times (1, 1) .$$

In our forthcoming proofs we need not know what $\psi(A)$ looks like. But, if we want, we can successively construct

$$K_3 = K_3(\psi(A)) \longrightarrow K_2 = K_2(\psi(A)) \longrightarrow K_1(\psi(A)) = \psi(A)$$

as in the proof of Lemma 4.1 in [2]. We will only sketch this method:

$$K_3 = 01111000001111$$

since K_3 is the unique vector satisfying: K_3 contains only 3-blocks, $D_3(K_3) = D_3(A)$ and the length of $K_3 = n - 2\gamma_1 - 4\gamma_2 = 14$.

By putting in 1100 or 0011 between certain positions in K_3 we get a vector K_2 which only contains 2- and 3-blocks and satisfies: $D_i(K_2) = D_i(A)$ for $i = 2, 3$ and the length of $K_2 = n - 2\gamma_1 = 22$. we get

$$K_2 = 0111001110000011001111 .$$

By putting in 10 or 01 between certain positions in K_2 we finally get:

$$\psi(A) = K_3 = 010110110011101001000011010010111 1 .$$

Next we will determine q such that $D_j(\psi^q(A)) = D_j(A)$. To do this we must be able to determine $D_j(\psi^q(A))$ directly from $D_j(A)$. We will develop a method in Lemma 3.6. First we need more notation.

DEFINITION 3.5. When it is clear which $A \in \{0, 1\}^n$ we are working with, we define $(s = 0, 1, 2, \cdots)$

$$\beta_j(s) = \beta_j(\psi^s(A)) \quad \text{and} \quad r_j(s) = r_j(\psi^s(A))$$
$$\mathscr{B}_j(s) = \beta_j(0) + \cdots + \beta_j(s-1) \quad \text{and} \quad \mathscr{R}_j(s) = r_j(0) + \cdots + r_j(s-1) .$$

LEMMA 3.6. *Suppose $A \in \mathscr{M}$, $1 \leqq j \leqq p$ and $D_j(A) = (t_1, \cdots, t_{\gamma_j})$. Then we determine $D_j(\psi^s(A))$ in the following way:*

We determine integers f and β^* such that

$$\mathscr{B}_j(s) = f \cdot \alpha_j + \beta^* \quad \textit{and} \quad 0 \leqq \beta^* < \alpha_j .$$

We let r^* = the number of coordinates t_i in $D_j(A)$ such that $t_i \leqq \beta^*$.

Then we have

$$D_j(\psi^s(A)) = (t'_{r^*+1}, \cdots, t'_{\gamma_j}, t'_1, \cdots, t'_{r^*}) \quad \textit{where}$$

$$t'_i = \begin{cases} t_i + \alpha_j - \beta^* & \textit{when} \quad 1 \leqq i \leqq r^* \\ t_i - \beta^* & \textit{when} \quad i > r^* . \end{cases}$$

(If $r^* = \gamma_j$, then $D_j(\psi^s(A)) = (t'_1, \cdots, t'_{\gamma_j})$.) Moreover, $\mathscr{R}_j(s) = f \cdot \gamma_j + r^*$.

PROOF. We suppose the lemma is true for s, and we will prove that it is true for $(s + 1)$. We write

$$D_j(\psi^s(A)) = (u_1, \cdots, u_{\gamma_j}) .$$

By Lemma 3.3 or Lemma 3.4 we have $(\beta^{**} = \beta_j(s)$ and $r^{**} = r_j(s))$

$$D_j(\psi^{s+1}(A)) = (u'_{r^{**}+1}, \cdots, u'_{\gamma_j}, u'_1, \cdots, u'_{r^{**}}) \qquad \text{where}$$
$$u'_i = \begin{cases} u_i + \alpha_j - \beta^{**} & \text{for} \quad 1 \leqq i \leqq r^{**} \\ u_i - \beta^{**} & \text{for} \quad i > r^{**}\,. \end{cases}$$

We suppose $\beta^* + \beta^{**} \geqq \alpha_j$ (the case $\beta^* + \beta^{**} < \alpha_j$ is treated analogously). We observe

$$t'_{\gamma_j} = t_{\gamma_j} - \beta^* \leqq \alpha_j - \beta^* \leqq \beta^{**}\,.$$

Hence we get

$$\begin{aligned} D_j(\psi^s(A)) &= (\underbrace{t'_{r^*+1}, \cdots, t'_{\gamma_j}, t'_1, \cdots, t'_v}, t'_{v+1}, \cdots, t'_{r^*}) \\ &= (\underbrace{u_1, \quad \cdots \qquad \cdots \quad u_{r^{**}}}, u_{r^{**}+1}, \cdots) \end{aligned}$$

and

$$D_j(\psi^{s+1}(A)) = (t''_{v+1}, \cdots, t''_{\gamma_j}, t''_1, \cdots, t''_v) \qquad \text{where}$$
$$t''_i = \begin{cases} t_i + \alpha_j - (\beta^* + \beta^{**} - \alpha_j) & \text{if} \quad 1 \leqq i \leqq v \\ t_i - (\beta^* + \beta^{**} - \alpha_j) & \text{if} \quad i > v\,. \end{cases}$$

(For example, if $1 \leqq i \leqq v$ we get: $t''_i = t'_i + \alpha_j - \beta^{**} = (t_i + \alpha_j - \beta^*) + \alpha_j - \beta^{**} = t_i + \alpha_j - (\beta^* + \beta^{**} - \alpha_j)$).

Now we will prove that this is in accordance with the lemma:

$$\mathscr{B}_j(s+1) = f\alpha_j + \beta^* + \beta^{**} = (f+1)\alpha_j + (\beta^* + \beta^{**} - \alpha_j)\,.$$

If $1 \leqq i \leqq v$, then we have

$$t_i = (t_i + \alpha_j - \beta^*) + \beta^* - \alpha_j = t'_i + \beta^* - \alpha_j \leqq \beta^{**} + \beta^* - \alpha_j\,.$$

If $v < i \leqq r^*$, then we have

$$t_i = (t_i + \alpha_j - \beta^*) + \beta^* - \alpha_j = t'_i + \beta^* - \alpha_j > \beta^{**} + \beta^* - \alpha_j\,.$$

If $v > r^*$, then we have

$$t_i > \beta^* \geqq \beta^* + \beta^{**} - \alpha_j\,.$$

Hence, $v =$ the number of coordinates t_i in $D_j(A)$ such that $t_i \leqq \beta^* + \beta^{**} - \alpha_j$.

We observe $v = r^* + r^{**} - \gamma_j$. Hence,

$$\mathscr{R}_j(s+1) = \mathscr{R}_j(s) + r^{**} = f \cdot \gamma_j + r^* + r^{**} = (f+1) \cdot \gamma_j + v$$

and the proof is complete.

Now we return to our example. We divide the treatment into 5 steps:

Step 1. We have $D_2(A) = (3, 7)$ and $\alpha_2 = 8$. If $\beta^* = 0, 1, 2, \cdots, 7$

respectively in Lemma 3.6 we get that $D_2(\psi^s(A))$ is equal to (3, 7), (2, 6), (1, 5), (4, 8), (3, 7), (2, 6), (1, 5), (4, 8) respectively. Hence, $\beta^* = 0$ or 4 gives $D_2(\psi^s(A)) = (3.7)$ and therefore

$$D_2(\psi^s(A)) = D_2(A) \Longleftrightarrow \mathscr{B}_2(s) \text{ is a multiple of } 4 . \tag{3.8}$$

Step 2. In the same way as in Step 1 we get

$$D_1(\psi^s(A)) = D_1(A) \Longleftrightarrow \mathscr{B}_1(s) \text{ is a multiple of } 5 . \tag{3.9}$$

Step 3. By using Lemma 3.4 we get

$$\begin{array}{lll} D_3(A) = (2, 4) \times (1, 1) & \beta_3(A) = 3 & r_3(A) = 1 \\ D_3(\psi(A)) = (1, 4) \times (1, 1) & \beta_3(\psi(A)) = 2 & r_3(\psi(A)) = 1 \\ D_3(\psi^2(A)) = (2, 4) \times (1, 1) . & & \end{array}$$

Hence, we get $D_3(A) = D_3(\psi^2(A)) = D_3(\psi^4(A)) = \cdots$ and

$$\begin{array}{lll} \mathscr{B}_3(2) = 5 , & \mathscr{B}_3(4) = 10, \cdots , & \mathscr{B}_3(2\cdot X_3) = 5\cdot X_3, \cdots \\ \mathscr{R}_3(2) = 2 , & \mathscr{R}_3(4) = 4, \cdots , & \mathscr{R}_3(2\cdot X_3) = 2\cdot X_3, \cdots \end{array}$$

where X_3 is an integer.

Step 4. We will determine Y such that $D_i(\psi^Y(A)) = D_i(A)$ for $i = 2, 3$. By Step 3

$$Y = 2\cdot X_3 \quad \text{for an integer} \quad X_3 .$$

By Lemma 3.4 and Step 3

$$\begin{aligned} \mathscr{B}_2(Y) &= \sum_{s=0}^{Y-1} \beta_3(s) + 2r_3(s) = \mathscr{B}_3(Y) + 2.\mathscr{R}_3(Y) \\ &= \mathscr{B}_3(2X_3) + 2.\mathscr{R}_3(2X_3) = 5X_3 + 4X_3 = 9X_3 . \end{aligned}$$

By (3.8) $\mathscr{B}_2(Y)$ must be a multiple of 4. Hence, the possible values of X_3 and $Y = 2\cdot X_3$ are

$$X_3 = 4, 8, 12, \cdots \qquad \text{and} \qquad Y = 8, 16, 24, \cdots .$$

Direct calculation gives us

$$\mathscr{R}_2(8) = 9 , \qquad \mathscr{R}_2(16) = 18 , \qquad \mathscr{R}_2(24) = 27 , \quad \text{etc.}$$

Later, of course, we must do this in a more sofisticated way. But at the present stage, this will obscure the ideas.

Step 5. We will determine Y such that $D_i(\psi^Y(A)) = D_i(A)$ for $i = 1, 2, 3$. The possible values of Y are $Y = 8, 16, 24, \cdots$. By Lemma 3.4 we have

$$\mathscr{B}_1(Y) = \sum_{s=0}^{Y-1} \beta_3(s) + 2r_2(s) + 4r_3(s) = \mathscr{B}_3(Y) + 2\mathscr{R}_2(Y) + 4\mathscr{R}_3(Y) .$$

Hence, by Step 3 and Step 4 we get

$$\mathscr{B}_1(8) = \mathscr{B}_3(8) + 2\mathscr{R}_2(8) + 4\mathscr{R}_3(8) = 20 + 18 + 32 = 70$$

which is a multiple of 5. Hence $Y = 8$ is the least Y such that $\psi^Y(A) = A$.

Now I will try to sketch thoroughly the ideas on the case $S = E_k + E_{k+1} + E_{k+2}$. Instead I will delete the general proof of how the minimal periods are determined. We suppose $A \in \mathscr{M}$, $\gamma_{p+1} > 1$ and again we divide the treatment of A into 5 steps.

Step 1. Suppose $D_2(A) = (t_1, \cdots, t_{\gamma_2})$. We will find a formula similar to (3.8). To do this we define Λ_2 in the following way:

If $t_1 = \cdots = t_r = 1$ and $t_{r+1} > 1$ we define $\Lambda_2(t_1, \cdots, t_r, \cdots, t_{\gamma_2}) = (t_{r+1} - 1, \cdots, t_{\gamma_2} - 1, t'_1, \cdots, t'_r)$ where $t'_1 = \cdots = t'_r = \alpha_2$.

By Lemma 3.4 we get

$$\begin{aligned} D_2(\psi(A)) &= \Lambda_2^{\beta_2(A)}(D_2(A)) \\ D_2(\psi^2(A)) &= \Lambda_2^{\beta_2(A)+\beta_2(\psi(A))}(D_2(A)) = \Lambda_2^{\mathscr{B}_2(2)}(D_2(A)) \\ &\vdots \\ D_2(\psi^s(A)) &= \quad\cdots\quad = \Lambda_2^{\mathscr{B}_2(s)}(D_2(A)) . \end{aligned}$$

The next problem is to determine when $\Lambda_2^\alpha(D_2(A)) = D_2(A)$. First we observe that this is true for $\alpha = \alpha_2$. Next we let α be the least α such that $\Lambda_2^\alpha(D_2(A)) = D_2(A)$. We will now describe how $D_2(A)$ looks in this case. We must have $\alpha_2 = r\alpha$ for an integer r. We let γ be the maximum integer such that $t_\gamma \leqq \alpha$. By definition of Λ_2^α we get

$$\begin{aligned} \Lambda_2^\alpha(D_2(A)) &= (t_{\gamma+1} - \alpha, \cdots, t_{\gamma_2} - \alpha, t_1 + \alpha_2 - \alpha, \cdots, t_\gamma + \alpha_2 - \alpha) \\ &= D_2(A) . \end{aligned}$$

Now we get obviously that $D_2(A)$ must have the form

$$\begin{aligned} D_2(A) = (&\underbrace{t_1, \cdots, t_\gamma}_{\text{Part 1}}, \underbrace{t_1 + \alpha, \cdots, t_\gamma + \alpha}_{\text{Part 2}}, \cdots, \\ &\underbrace{t_1 + (r-1)\alpha, \cdots, t_\gamma + (r-1)\alpha}_{\text{Part } r}) \end{aligned} \tag{3.10}$$

where $\alpha_2 = r\alpha$.

Now we will prove that (3.10) is a sufficient condition. Therefore we suppose (3.10) is true. Then we get by Lemma 3.2 that

$$t_{r_2} = t_r + (r-1)\alpha \leqq \alpha_2 \quad \text{and} \quad t_1 > 0 .$$

Hence

$$t_r \leqq \alpha \quad \text{and} \quad t_{r+1} > \alpha .$$

Hence, $\Lambda^\alpha(D_2(A)) = D_2(A)$.

We let α_2^* be the least α such that $\Lambda^\alpha(D_2(A)) = D_2(A)$. We get

$$D_2(\psi^s(A)) = D_2(A) \Longleftrightarrow \mathscr{B}_2(s) = X_2\alpha_2^* \quad \text{for an integer} \quad X_2 .$$

Moreover, if $\mathscr{B}_2(s) = X_2\alpha_2^*$, then

$$\mathscr{R}_2(s) = X_2\gamma_2^* \quad \text{where} \quad \gamma_2^* = \frac{\alpha_2^*}{\alpha_2}\gamma_2 . \tag{3.11}$$

We prove (3.11) as follows: If $0 \leqq z < r$, then by (3.10) the number of coordinates less than or equal to $z\cdot\alpha_2^*$ is $z\cdot\gamma_2^*$. We suppose $\mathscr{B}_2(s) = (wr + z)\alpha_2^* = w\alpha_2 + z\cdot\alpha_2^*$ where $0 \leqq z < r$. By Lemma 3.6 we get

$$\mathscr{R}_2(s) = w\gamma_2 + z\gamma_2^* = (wr + z)\gamma_2^*$$

and the proof of (3.11) is complete.

Step 2. Suppose $D_1(A) = (t_1, \cdots, t_{r_1})$. Analoguosly with Step 1 we define Λ_1 in the following way:

If $t_1 = \cdots = t_r = 1$ and $t_{r+1} > 1$ we define $\Lambda_1(t_1, \cdots, t_{r_1}) = (t_{r+1} - 1, t_{r+2} - 1, \cdots, t_{r_1} - 1, t_1', \cdots, t_r')$ where $t_1' = \cdots = t_r' = \alpha_1$.

We let α_1^* be the least integer such that $\Lambda_1^{\alpha_1^*}(D_1(A)) = D_1(A)$. Analogously with Step 1 we get

$$D_1(\psi^s(A)) = D_1(A) \Longleftrightarrow \mathscr{B}_1(s) = X_1\alpha_1^* \quad \text{for an integer} \quad X_1$$

and

$$\text{If } \mathscr{B}_1(s) = X_1\alpha_1^*, \text{ then } \mathscr{R}_1(s) = X_1\gamma_1^* \text{ where } \gamma_1^* = \frac{\alpha_1^*}{\alpha_1}\gamma_1 .$$

Step 3. Suppose $D_3(A) = (t_1, \cdots, t_{r_3}) \times (s_1, \cdots, s_{r_3})$. Now we will determine when $D_3(\psi^q(A)) = D_3(A)$. Again we define a function Λ_3 in the following way:

$$\Lambda_3(t_1, \cdots, t_{r_3}) \times (s_1, s_2, \cdots, s_{r_3}) = (t_2', \cdots, t_{r_3}', t_1') \times (s_2, \cdots, s_{r_3}, s_1)$$

where

$$t_i' = \begin{cases} t_1 + \alpha_3 - (s_1 + t_1) = \alpha_3 - s_1 & \text{for} \quad i = 1 \\ t_i - (s_1 + t_1) & \text{for} \quad i = 2, 3, \cdots, \gamma_3 . \end{cases}$$

We observe by Lemma 3.4 that

$$D_3(\psi(A)) = \Lambda_3(D_3(A)), \cdots, D_3(\psi^q(A)) = \Lambda_3^q(D_3(A)), \cdots .$$

By definition of Λ_3 we have for $1 \leqq q \leqq \gamma_3$ that

$$\text{(3.12)} \quad \begin{cases} \Lambda_3^q(t_1, \cdots, t_{\gamma_3}) \times (s_1, \cdots, s_{\gamma_3}) \\ \qquad = (t''_{q+1}, \cdots, t''_{\gamma_3}, t''_1, \cdots, t''_q) \times (s_{q+1}, \cdots, s_{\gamma_3}, s_1, \cdots, s_q) \\ \text{where} \\ \qquad t''_i = \begin{cases} t_i + \alpha_3 - (s_q + t_q) & \text{for} \quad i = 1, \cdots, q \\ t_i - (s_q + t_q) & \text{for} \quad i = q+1, \cdots . \end{cases} \end{cases}$$

For example if $q = 2$ and $i > 2$ we get

$$\begin{aligned} t''_i &= t'_i - (s_2 + t'_2) = t_i - (s_1 + t_1) - s_2 - (t_2 - (s_1 + t_1)) \\ &= t_i - (s_2 + t_2) . \end{aligned}$$

Specially, if $q = \gamma_3$ we get ($s_{\gamma_3} + t_{\gamma_3} = \alpha_3$ by Lemma 3.2)

$$t''_i = t_i + \alpha_3 - (s_{\gamma_3} + t_{\gamma_3}) = t_i \quad \text{for} \quad i = 1, \cdots, \gamma_3 .$$

Hence, $\Lambda^{\gamma_3}(D_3(A)) = D_3(A)$.
If $D_3(A) = (t_1, \cdots, t_{\gamma_3}) \times (s_1, \cdots, s_{\gamma_3})$ and $1 \leqq q \leqq \gamma_3$, we have by Lemma 3.4 that

$$D_3(\psi^q(A)) = (t''_{q+1}, \cdots, t''_{\gamma_3}, t''_1, \cdots) \times (s_{q+1}, \cdots, s_{\gamma_3}, s_1, \cdots, s_q)$$

where

$$t''_i = \begin{cases} t_i + \alpha_3 - (\beta_3(0) + \cdots + \beta_3(q-1)) \\ \qquad\qquad = t_i + \alpha_3 - \mathscr{B}_3(q) & \text{for} \quad 1 \leqq i \leqq q \\ t_i - (\beta_3(0) + \cdots + \beta_3(q-1)) \\ \qquad\qquad = t_i - \mathscr{B}_3(q) & \text{for} \quad i > q . \end{cases}$$

Hence,

$$\text{(3.13)} \qquad \mathscr{B}_3(q) = s_q + t_q \quad \text{for} \quad 1 \leqq q \leqq \gamma_3 .$$

The next problem is to determine when $\Lambda^\gamma(D_3(A)) = D_3(A)$. Next we suppose γ is the least integer such that $\Lambda^\gamma(D_3(A)) = D_3(A)$. Then we have $\gamma_3 = r\gamma$ for an integer r, and by (3.12) we get that $D_3(A)$ has the form

$$\text{(3.14)} \quad \begin{aligned} D_3(A) = (&\underbrace{t_1, \cdots, t_\gamma}_{\text{Part 1}}, \underbrace{t_1 + \alpha, \cdots, t_\gamma + \alpha}_{\text{Part 2}}, \cdots, \\ &\underbrace{t_1 + (r-1)\alpha, \cdots, t_\gamma + (r-1)\alpha}_{\text{Part } r}) \\ &\times (\underbrace{s_1, \cdots, s_\gamma}_{\text{Part 1}}, \underbrace{s_1, \cdots, s_\gamma}_{\text{Part 2}}, \cdots, \underbrace{s_1, \cdots, s_\gamma}_{\text{Part } r}) \end{aligned}$$

where $\alpha r = \alpha_3$ (which is equivalent to $\alpha = s_\gamma + t_\gamma$). (We get directly from (3.12) that (3.14) is true with $\alpha = s_\gamma + t_\gamma$. But this is equivalent to $\alpha r = \alpha_3$ because $s_{\gamma_3} + t_{\gamma_3} = (s_\gamma + t_\gamma) + (r-1)\alpha = \alpha_3$ by Lemma 3.2.)

We let γ_3^* be the least integer γ such that $\Lambda_3^\gamma(D_3(A)) = D_3(A)$. Then we have

$$D_3(\psi^Y(A)) = D_3(A) \Longleftrightarrow Y = X_3\gamma_3^* \quad \text{for an integer} \quad X_3 .$$

Moreover, if $Y = X_3\gamma_3^*$, then

$$\mathscr{B}_3(Y) = X_3\alpha_3^* \quad \text{where} \quad \alpha_3^* = \frac{\gamma_3^*}{\gamma_3}\alpha_3 . \tag{3.15}$$

We prove (3.15) as follows: By (3.13) and (3.14) we have

$$\mathscr{B}_3(q \cdot \gamma_3^*) = t_{q\cdot\gamma_3^*} + s_{q\cdot\gamma_3^*} = q\alpha_3^* \quad \text{for} \quad 0 \leqq q < r ,$$

where $r = \gamma_3/\gamma_3^*$, and

$$\mathscr{B}_3(r\gamma_3^*) = \mathscr{B}_3(\gamma_3) = s_{\gamma_3} + t_{\gamma_3} = \alpha_3 = r\alpha_3^* ,$$

and (3.15) follows.

Step 4. Next, we will determine Y such that $D_i(\psi^Y(A)) = D_i(A)$ for $i = 2, 3$. By Step 3 we must have $Y = X_3 \cdot \gamma_3^*$. Moreover in this case

$$\mathscr{B}_2(Y) = \mathscr{B}_3(Y) + 2\mathscr{R}_3(Y) = X_3\alpha_3^* + 2X_3\gamma_3^* .$$

Moreover, by Step 1, we must have

$$\mathscr{B}_2(Y) = X_2\alpha_2^* \quad \text{for an integer} \quad X_2 .$$

Hence, we get the equation $X_2\alpha_2^* = X_3\alpha_3^* + 2X_3\gamma_3^*$.

Step 5. Next, we will determine Y such that $D_i(\psi^Y(A)) = D_i(A)$ for $i = 1, 2, 3$. By Step 2 this is true for $i = 2, 3$ if and only if there exist integers X_2 and X_3 such that $X_2\alpha_2^* = X_3\alpha_3^* + 2X_3\gamma_3^*$ and $Y = X_3\gamma_3^*$. Moreover by the previous steps we have

$$\mathscr{B}_3(Y) = X_3\alpha_3^* , \qquad \mathscr{R}_3(Y) = X_3\gamma_3^* , \qquad \mathscr{B}_2(Y) = X_2\alpha_2^* \qquad \text{and}$$
$$\mathscr{R}_2(Y) = X_2\gamma_2^* .$$

Hence,

$$\mathscr{B}_1(Y) = \mathscr{B}_3(Y) + 2\mathscr{R}_2(Y) + 4\mathscr{R}_3(Y) = X_3\alpha_3^* + 2X_2\gamma_2^* + 4X_3\gamma_3^* .$$

Moreover, by Step 2 we must have

$$\mathscr{B}_1(Y) = X_1\alpha_1^* \quad \text{for an integer} \quad X_1 .$$

Hence, we get the equation

$$X_1\alpha_1^* = X_3\alpha_3^* + 2X_2\gamma_2^* + 4X_3\gamma_3^* \ .$$

Conclusion. $\psi^Y(A) = A \Leftrightarrow D_i(\psi^Y(A)) = D_i(A) \quad i = 1, 2, 3 \Leftrightarrow$ There exists integers X_1, X_2 and X_3 such that

$$\begin{aligned} X_2\alpha_2^* &= X_3\alpha_3^* + 2X_3\gamma_3^* \\ X_1\alpha_1^* &= X_3\alpha_3^* + 2X_2\gamma_2^* + 4X_3\gamma_3^* \\ Y &= X_3\gamma_3^* \ . \end{aligned}$$

Let X_1, X_2, X_3 be the least integral solution. Then ($\mathscr{R}_1(Y) = X_1\gamma_1^*$ follows from Step 2)

$$\begin{aligned} \sum_{s=0}^{Y-1} \text{Index}\,(\psi^s(A)) &= \sum_{s=0}^{Y-1} \beta_3(s) + 2r_1(s) + 4r_2(s) + 6r_3(s) \\ &= \mathscr{B}_3(Y) + 2\mathscr{R}_1(Y) + 4\mathscr{R}_2(Y) + 6\mathscr{R}_3(Y) \\ &= X_3\alpha_3^* + 2X_1\gamma_1^* + 4X_2\gamma_2^* + 6X_3\gamma_3^* \end{aligned}$$

which is the minimal period of A.

If $A \in \mathscr{M}$ and $\gamma_{p+1} = 1$ we must use Lemma 3.3 instead of Lemma 3.4. Then we have always $D_3(\psi(A)) = D_3(A)$. Hence, we need only to modify Steps 4 and 5 as follows.

Step 4. By Lemma 3.3 we get $\mathscr{B}_2(Y) = Y$. We must have $\mathscr{B}_2(Y) = Y = X_2\alpha_2^*$ for an integer X_2. In this case $\mathscr{R}_2(Y) = X_2\gamma_2^*$.

Step 5. By Lemma 3.3 we get

$$\mathscr{B}_1(Y) = \sum_{s=0}^{Y-1} (2 + 2r_2(s)) = 2Y + 2\mathscr{R}_2(Y) = 2Y + 2X_2\gamma_2^* \ .$$

We must have $\mathscr{B}_1(Y) = 2Y + 2X_2\gamma_2^* = X_1\alpha_1^*$ for an integer X_1. In this case $\mathscr{R}_1(Y) = X_1\gamma_1^*$.

Conclusion. $A = \psi^Y(A) \Leftrightarrow$ There exist integers X_1 and X_2 such that $X_2\alpha_2^* = Y$ and $X_1\alpha_1^* = 2Y + 2X_2\gamma_2^*$. Suppose X_1, X_2 is the least solution. Then we get

$$\begin{aligned} \sum_{s=0}^{Y-1} \text{Index}\,(\psi^s(A)) &= \sum_{s=0}^{Y-1} [(n + 3) + 2r_1(s) + 4r_2(s)] \\ &= Y(n + 3) + 2\mathscr{R}_1(Y) + 4\mathscr{R}_2(Y) \\ &= Y(n + 3) + 2X_1\gamma_1^* + 4X_2\gamma_2^* \end{aligned}$$

which is the minimal period.

4. **The minimal periods.** Now I will formulate the results

from § 3 for a general p and very roughly sketch the proof. As before

$$A \in \mathscr{M} \Longleftrightarrow \begin{cases} w(A) = k + p + 1 \\ A \text{ starts with } 0 \text{ or a } (p+1)\text{-block} \\ A \text{ contains } \gamma_i \ i\text{-blocks for } i = 1, \cdots, p+1 \\ A \text{ ends with a } (p+1)\text{-block} . \end{cases}$$

The blocks in A are determined with respect to p. $D_i(A)$ ($i = 1, \cdots, p+1$) is defined in Definition 3.1.

DEFINITION 4.1. Let $A \in \mathscr{M}$ be given.

(a) Suppose $1 \leqq j \leqq p$ and $D_j(A) = (t_1, \cdots, t_{\gamma_j})$. We define Λ_j in the following way:

If $t_1 = \cdots = t_r = 1$ and $t_{r+1} > 1$ we define
$\Lambda_j(t_1, \cdots, t_{\gamma_j}) = (t_{r+1} - 1, \cdots, t_{\gamma_j} - 1, t'_1, \cdots, t'_r)$
where $t'_1 = \cdots = t'_r = \alpha_j$.

Let α_j^* be the least integer such that

$$\Lambda_j^{\alpha_j^*}(D_j(A)) = D_j(A) .$$

(b) Suppose $D_{p+1}(A) = (t_1, \cdots, t_{\gamma_{p+1}}) \times (s_1, \cdots, s_{\gamma_{p+1}})$. We define Λ_{p+1} in the following way:

$$\Lambda_{p+1}(t_1, \cdots, t_{\gamma_{p+1}}) \times (s_1, \cdots, s_{\gamma_{p+1}}) = (t'_2, \cdots, t'_{\gamma_{p+1}}, t'_1) \times (s_2, \cdots, s_{\gamma_{p+1}}, s_1)$$

where

$$t'_i = \begin{cases} \alpha_{p+1} - s_1 & \text{for } \ i = 1 \\ t_i - (s_1 + t_1) & \text{for } \ i > 1 . \end{cases}$$

Let γ_{p+1}^* be the least integer such that

$$\Lambda_{p+1}^{\gamma_{p+1}^*}(D_{p+1}(A)) = D_{p+1}(A) .$$

(c) If $1 \leqq i \leqq p$, we define $\gamma_i^* = \gamma_i \cdot \alpha_i^* / \alpha_i$. Moreover, we define $\alpha_{p+1}^* = \alpha_{p+1} \cdot \gamma_{p+1}^* / \gamma_{p+1}$.

As in the previous section we can prove that γ_i^* ($1 \leqq i \leqq p$) and α_{p+1}^* are integers.

THEOREM 4.2. *Suppose $A \in \mathscr{M}$. We associate p equations to A in the following way*:

$$\begin{array}{ll} (p) & \alpha_p^* \cdot X_p = \alpha_{p+1}^* X_{p+1} + 2\gamma_{p+1}^* X_{p+1} \\ (p-1) & \alpha_{p-1}^* X_{p-1} = \alpha_{p+1}^* X_{p+1} + 2\gamma_p^* X_p + 4\gamma_{p+1}^* X_{p+1} \\ & \qquad \vdots \\ (1) & \alpha_1^* X_1 = \alpha_{p+1}^* X_{p+1} + 2\gamma_2^* X_2 + 4\gamma_3^* X_3 + \cdots + 2p\gamma_{p+1}^* X_{p+1} . \end{array}$$

If $\gamma_i = 0$, *we replace equation* (i) *by* $X_i = 0$. *We let* $X_1, \cdots, X_{p+1}$ *be the least integral solution of the equations.*

Then $X_{p+1}\alpha^*_{p+1} + \sum_{i=1}^{p+1} 2i \cdot \gamma^*_i \cdot X_i$ *is the minimal period of* A *with respect to the shift register* $(x_1, \cdots, x_n) \to (x_2, \cdots, x_{n+1})$ *where*

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

If $\gamma_i = 0$ for $i = 1, \cdots, p$, we observe that the minimal period $= X_{p+1}\alpha^*_{p+1} + 2(p+1)\gamma^*_{p+1}X_{p+1} = \alpha^*_{p+1} + 2(p+1)\gamma^*_{p+1} = (\gamma^*_{p+1}/\gamma_{p+1})(\alpha_{p+1} - 2(p+1)\gamma_{p+1}) = (\gamma^*_{p+1}/\gamma_{p+1})(n+p+1)$.

The existence of the minimal solution $X_1, \cdots, X_{p+1}$ is proved as indicated in § 3 in [2].

Proof. We only sketch the proof since it is only a generalization of the case $p = 2$ which we treated in § 3.

First we suppose $\gamma_{p+1} > 1$.

We get

$$D_{p+1}(\psi^Y(A)) = D_{p+1}(A) \Longleftrightarrow Y = X_{p+1}\gamma^*_{p+1} \quad \text{for an integer} \quad X_{p+1} .$$

In this case $\mathscr{B}_{p+1}(Y) = X_{p+1}\alpha^*_{p+1}$ and $\mathscr{R}_{p+1}(Y) = X_{p+1}\gamma^*_{p+1}$. If $1 \leqq j \leqq p$ we get (if $\gamma_j \neq 0$)

$$D_j(\psi^Y(A)) = D_j(A) \Longleftrightarrow \mathscr{B}_j(Y) = X_j\alpha^*_j \quad \text{for an integer} \quad X_j .$$

In this case we have $\mathscr{R}_j(Y) = X_j\gamma^*_j$.

Suppose $X_1, \cdots, X_{p+1}$ satisfy the equations. Put $Y = X_{p+1}\gamma^*_{p+1}$. We prove by induction that

$$\mathscr{B}_i(Y) = X_i\alpha^*_i \quad \text{when} \quad \gamma_i \neq 0 \quad \text{and} \quad 1 \leqq i \leqq p . \tag{4.1}$$

Suppose (4.1) is true for $i = p, p-1, \cdots, j+1$. Then we have

$$\begin{aligned}\mathscr{B}_j(Y) &= \mathscr{B}_{p+1}(Y) + 2\mathscr{R}_{j+1}(Y) + \cdots + 2(p+1-j)\mathscr{R}_{p+1}(Y)\\ &= X_{p+1}\alpha^*_{p+1} + 2\gamma^*_{j+1}X_{j+1} + \cdots + 2(p+1-j)\gamma^*_{p+1}X_{p+1} = \alpha^*_jX_j .\end{aligned}$$

Hence (4.1) is true for $j = 1, \cdots, p$. Then we get $\psi^Y(A) = A$ and $\psi^Y(A) = \theta^t(A)$ where

$$\begin{aligned}t &= \mathscr{B}_{p+1}(Y) + 2\mathscr{R}_1(Y) + \cdots + 2(p+1)\mathscr{R}_{p+1}(Y)\\ &= X_{p+1}\alpha^*_{p+1} + \sum_{i=1}^{p+1} 2i \cdot \gamma^*_i \cdot X_i .\end{aligned}$$

Moreover, it is easily seen that all Y such that $\psi^Y(A) = A$ is obtained in this way.

Finally, we suppose $\gamma_{p+1} = 1$ and $\gamma_i \neq 0$ for at least one $i < p+1$. We only sketch the proof since the proof is analogous with the case

$\gamma_{p+1} > 1$. We get

$$\psi^{Y}(A) = A \Longleftrightarrow \mathscr{R}_i(Y) = X_i \cdot \alpha_i^* \quad \text{when} \quad \gamma_i \neq 0 \quad \text{and} \quad 1 \leqq i \leqq p\ .$$

In the same way as in § 3 (the case $\gamma_{p+1} = 1$) this is equivalent to: $X_1, \cdots, X_p, Y$ satisfy the equations $(1)', \cdots, (p)'$ given by

$$(q)' \begin{cases} X_q \cdot \alpha_q^* = Y(p + 1 - q) + \sum_{t=q+1}^{p} 2(t - q) X_t \gamma_t^* & \text{if} \quad \gamma_q \neq 0 \\ X_q = 0 & \text{if} \quad \gamma_q = 0\ . \end{cases}$$

Let $X_1, \cdots, X_p, Y$ be the least solution of the equations $(1)', \cdots, (p)'$. Then Y is the least Y such that $\psi^{Y}(A) = A$. We calculate the minimal period of A in the following way

$$\sum_{s=0}^{Y-1} \left[(n + p + 1) + 2 \sum_{i=1}^{p} i \cdot r_i(s) \right] = Y(n + p + 1) + 2 \sum_{i=1}^{p} i \cdot \mathscr{R}_i(Y)$$
$$= Y(n + p + 1) + 2 \sum_{i=1}^{p} i \cdot \gamma_i^* \cdot X_i\ .$$

The proof will be complete if we can prove the following claim: Suppose $X_1, \cdots, X_{p+1}$ is the least solutions $(1), \cdots, (p)$. Let

$$Y = X_{p+1} \qquad \text{and} \qquad \hat{X}_t = \begin{cases} 0 & \text{if} \quad \gamma_t = 0 \\ X_t - Y \cdot \dfrac{\gamma_t}{\gamma_t^*} & \text{if} \quad \gamma_t \neq 0\ . \end{cases}$$

Then $\hat{X}_1, \cdots, \hat{X}_p, Y$ is the least solution of the equations $(1)', \cdots, (p)'$, and

$$Y(n + p + 1) + \sum_{i=1}^{p} 2i \cdot \hat{X}_i \cdot \gamma_i^* = X_{p+1} \alpha_{p+1}^* + \sum_{i=1}^{p+1} 2i \cdot X_i \cdot \gamma_i^*\ .$$

Now we will prove this claim. Since $\gamma_{p+1} = \gamma_{p+1}^* = 1$, then $\alpha_{p+1} = \alpha_{p+1}^*$. We use the definition of α_{p+1} and get

$$X_{p+1}\alpha_{p+1}^* + \sum_{i=1}^{p+1} 2i \cdot X_i \cdot \gamma_i^*$$
$$= Y\left(n + p + 1 - \sum_{i=1}^{p+1} 2i\gamma_i\right) + \sum_{i=1}^{p} 2i\gamma_i^*\left(\hat{X}_i + Y\frac{\gamma_i}{\gamma_i^*}\right) + 2(p + 1)\gamma_{p+1} Y$$
$$= Y(n + p + 1) + \sum_{i=1}^{p} 2i \cdot \gamma_i^* \cdot \hat{X}_i\ .$$

Next we prove that the following 3 equations are equivalent (we use $\alpha_i^* \cdot \gamma_i / \gamma_i^* = \alpha_i$):

$$\alpha_i^* X_i = X_{p+1}\alpha_{p+1}^* + \sum_{t=i+1}^{p+1} 2(t - i)\gamma_i^* X_i$$

$$\alpha_i^* \hat{X}_i + \alpha_i Y = Y\alpha_{p+1} + \sum_{t=i+1}^{p} 2(t - i)\gamma_i^* \hat{X}_i + Y \sum_{t=i+1}^{p+1} 2(t - i)\gamma_i$$

$$\hat{X}_i\alpha_i^* = Y(p+1-i) + \sum_{t=i+1}^{p} 2(t-i)\gamma_i^*\hat{X}_i + Z$$

where

$$Z = Y\Big(-\alpha_i + \alpha_{p+1} + \sum_{t=i+1}^{p+1} 2(t-i)\gamma_i + i - (p+1)\Big)\,.$$

$Z = 0$ follows from the definition of α_{p+1} and α_i. Hence, the proof of the claim is complete.

Finally we will include an alternative way to determine α_i^* and γ_i^*:

PROPOSITION 4.3. *Let $A \in \mathscr{M}$.*

(a) *Suppose $1 \leqq j \leqq p$. We define the map ρ_j in the following way: If $D_j(A) = (t_1, \cdots, t_{\gamma_j})$, then*

$$\rho_j(D_j(A)) = (d_1, \cdots, d_{\gamma_j})$$

where

$$d_i = \begin{cases} t_1 + \alpha_j - t_{\gamma_j} & \text{for} \quad i = 1 \\ t_{i+1} - t_i & \text{for} \quad i > 1\,. \end{cases}$$

Then γ_j^* is the cycle period of $(d_1, \cdots, d_{\gamma_j})$, that is; γ_j^* is the least integer such that

$$(d_{\gamma_j^*+1}, \cdots, d_{\gamma_j}, d_1, \cdots, d_{\gamma_j^*}) = (d_1, \cdots, d_{\gamma_j})\,.$$

(b) *Suppose $D_{p+1}(A) = (t_1, \cdots, t_{\gamma_{p+1}}) \times (s_1, \cdots, s_{\gamma_{p+1}})$. Then we define*

$$\eta_{p+1}(D_{p+1}(A)) = (d_1, \cdots, d_{\gamma_{p+1}}) \times (s_1, \cdots, s_{\gamma_{p+1}})$$

where

$$d_i = \begin{cases} t_1 + \alpha_{p+1} - (t_{\gamma_{p+1}} + s_{\gamma_{p+1}}) = t_1 & \text{for} \quad i = 1 \\ t_{i+1} - (t_i + s_i) & \text{for} \quad i > 1\,. \end{cases}$$

Then γ_{p+1}^* is the least cycle period of $(d_1, \cdots, d_{\gamma_{p+1}}) \times (s_1, \cdots, s_{\gamma_{p+1}})$. That is; γ_{p+1}^* is the least integer such that

$$\begin{aligned}(d_{\gamma_{p+1}^*+1}, \cdots, d_{\gamma_{p+1}}, d_1, \cdots, d_{\gamma_{p+1}^*}) \times (s_{\gamma_{p+1}^*+1}, \cdots, s_{\gamma_{p+1}}, s_1, \cdots, s_{\gamma_{p+1}^*}) \\ = (d_1, \cdots, d_{\gamma_{p+1}}) \times (s_1, \cdots, s_{\gamma_{p+1}})\,.\end{aligned}$$

Proof. (a) By (3.10) we have that γ_j^* is the least integer such that $D_j(A)$ has the form

$$\begin{aligned} D_j(A) = (&\underbrace{t_1, \cdots, t_{\gamma_j^*}}_{\text{Part 1}}, \underbrace{t_1 + \alpha_j^*, \cdots, t_{\gamma_j^*} + \alpha_j^*}_{\text{Part 2}}, \cdots, \\ &\underbrace{t_1 + (r-1)\alpha_j^*, \cdots, t_{\gamma_j^*} + (r-1)\alpha_j^*}_{\text{Part } r}) \end{aligned} \tag{4.2}$$

and

$$\alpha_j = r\alpha_j^*\,.$$

Moreover, this is equivalent to that $\rho_j(D_j(A))$ has the form

$$(4.3)\quad \begin{aligned} &\rho_j(D_j(A)) = (\underbrace{d_1, \cdots, d_{\gamma_j^*}}_{\text{Part 1}}, \underbrace{d_1, \cdots, d_{\gamma_j^*}}_{\text{Part 2}}, \cdots, \underbrace{d_1, \cdots, d_{\gamma_j^*}}_{\text{Part } r}) \quad \text{and} \\ &d_1 + \cdots + d_{\gamma_j^*} = \alpha_j^* . \end{aligned}$$

We indicate how this is proved: Suppose (4.2) is satisfied, then

$$\begin{aligned} d_1 &= t_1 + \alpha_j - t_{\gamma_j} = t_1 + \alpha_j - (t_{\gamma_j^*} + (r-1)\alpha_j^*) \\ &= t_1 + \alpha_j^* - t_{\gamma_j^*} = t_{\gamma_j^*+1} - t_{\gamma_j^*} = d_{\gamma_j^*+1} , \quad \text{etc.} \end{aligned}$$

Suppose (4.3) is satisfied, then

$$t_{\gamma_j^*+1} = \sum_{i=2}^{\gamma_j^*+1} (t_i - t_{i-1}) + t_1 = \sum_{i=2}^{\gamma_j^*+1} d_i + t_1 = \alpha_j^* + t_1 , \quad \text{etc.}$$

Since (4.2) is equivalent to (4.3), (a) follows easily.

(b) We define ρ_j for $j = p + 1$ as in (a). Since (3.14) is analogous with (3.10) we get as in (a) that γ_{p+1}^* is the least common cycle period for $\rho_{p+1}(D_{p+1}(A))$ and $(s_1, \cdots, s_{\gamma_{p+1}})$. This is equivalent with that γ_{p+1}^* is the least cycle period of $\eta_{p+1}(D_{p+1}(A))$.

5. The possible periods. By Theorem 4.2 the minimal periods of $A \in \mathscr{M}$ are completely determined by $(\gamma_1^*, \cdots, \gamma_{p+1}^*)$ since $\alpha_i^* = (\gamma_i^*/\gamma_i)\alpha_i$. We define

$$\begin{aligned} &\mathrm{PER}\,(\gamma_1^*, \cdots, \gamma_{p+1}^*) \\ &\quad = X_{p+1}\alpha_{p+1}^* + 2X_1\gamma_1^* + 4X_2\gamma_2^* + \cdots + 2(p+1)\gamma_{p+1}^*X_{p+1} \end{aligned}$$

where $X_1, \cdots, X_{p+1}$ is the least solution of the equations corresponding to $(\gamma_1^*, \cdots, \gamma_{p+1}^*)$ in Theorem 4.2. Moreover, we let

$$m = k + p + 1 - \gamma_1 - 2\gamma_2 - \cdots - (p+1)\gamma_{p+1} .$$

THEOREM 5.1. (a) *The possible periods of the elements in* $\mathscr{M}$ *are:*

$$\{\mathrm{PER}\,(\gamma_1^*, \cdots, \gamma_{p+1}^*) : (\gamma_1^*, \cdots, \gamma_{p+1}^*) \textit{ corresponds to an } A \in \mathscr{M}\} .$$

(b) *There exists* $A \in \mathscr{M}$ *corresponding to* $(\gamma_1^*, \cdots, \gamma_{p+1}^*)$ *if and only if*

$$\frac{\gamma_i}{\gamma_i^*} \quad (i = 1, \cdots, p+1) , \qquad \alpha_i \cdot \frac{\gamma_i^*}{\gamma_i} \quad (i = 1, \cdots, p+1) \qquad \textit{and}$$

$$m \cdot \frac{\gamma_{p+1}^*}{\gamma_{p+1}} \quad \textit{are integers.}$$

Proof. (a) is obvious. We let $\rho_1, \cdots, \rho_p, \eta_{p+1}$ be as in Proposition 4.3. By Lemma 3.2 we get easily

$$\rho_1 \times \rho_2 \times \cdots \times \rho_p \times \eta_{p+1}\left\{\bigtimes_{i=1}^{p+1} D_i(A) : A \in \mathscr{M}\right\} = \bigtimes_{i=1}^{p+1} \mathscr{N}_i$$

where

$$\begin{aligned} \mathscr{N}_i = \{(d_1, \cdots, d_{\gamma_i}) &: d_1 > 0,\ d_j \geqq 0\ (j = 2, \cdots, \gamma_i) \text{ and} \\ & d_1 + \cdots + d_{\gamma_i} = \alpha_i\} \quad \text{for} \quad 1 \leqq i \leqq p \qquad \text{and} \\ \mathscr{N}_{p+1} = \{(d_1, \cdots, d_{\gamma_{p+1}}) &\times (s_1, \cdots, s_{\gamma_{p+1}}) : d_i \geqq 0,\ s_i \geqq 0, \\ & d_1 + \cdots + d_{\gamma_{p+1}} = \alpha_{p+1} - m \text{ and } s_1 + \cdots + s_{\gamma_{p+1}} = m\} \end{aligned}$$

where $m = k + p + 1 - \gamma_1 - 2\gamma_2 - \cdots - (p + 1)\gamma_{p+1}$.

By Proposition 4.3 we get {the possible $(\gamma_1^*, \cdots, \gamma_{p+1}^*)$} is equal to the set

$$\bigtimes_{i=1}^{p+1} \{\text{the cycle periods of elements in } \mathscr{N}_i\} .$$

Finally, we get easily that {the possible cycle periods of elements in $\mathscr{N}_i$} is equal to the set

$$\left\{\gamma_i^* : \frac{\gamma_i}{\gamma_i^*} \text{ and } \alpha_i \cdot \frac{\gamma_i^*}{\gamma_i} \text{ are integers}\right\}$$

for $1 \leqq i \leqq p$. Moreover, we get

$$\{\text{the possible cycle periods of elements in } \mathscr{N}_{p+1}\}$$

is equal to the set

$$\left\{\gamma_{p+1}^* : \frac{\gamma_{p+1}}{\gamma_{p+1}^*},\ \alpha_{p+1} \cdot \frac{\gamma_{p+1}^*}{\gamma_{p+1}} \text{ and } m \cdot \frac{\gamma_{p+1}^*}{\gamma_{p+1}} \text{ are integers}\right\}$$

and the proof is complete.

6. The number of cycles.

In this section we will count the number of cycles $\mathscr{C}$ in

$$\bar{\mathscr{M}} = \{A \in \{0, 1\}^n : \exists\, i \text{ such that } \theta^i(A) \in \mathscr{M}\}$$

corresponding to a given $(\gamma_1^*, \cdots, \gamma_{p+1}^*)$. That means: If $A \in \mathscr{C} \cap \mathscr{M}$, then $(\gamma_1^*, \cdots, \gamma_{p+1}^*)$ corresponds to A. We let $\sharp$ denote "the number of elements in". Moreover, we let $\mathscr{N}_i$ $(i = 1, \cdots, p + 1)$ be as in § 5. That is;

$$\begin{aligned} \mathscr{N}_i = \{(d_1, \cdots, d_{\gamma_i}) &: d_1 > 0,\ d_j \geqq 0\ (j = 2, \cdots, \gamma_i) \text{ and} \\ & d_1 + \cdots + d_{\gamma_i} = \alpha_i\} \quad \text{for} \quad 1 \leqq i \leqq p \qquad \text{and} \\ \mathscr{N}_{p+1} = \{(d_1, \cdots, d_{\gamma_{p+1}}) &\times (s_1, \cdots, s_{\gamma_{p+1}}) : d_i \geqq 0,\ s_i \geqq 0, \\ & d_1 + \cdots + d_{\gamma_{p+1}} = \alpha_{p+1} - m \text{ and } s_1 + \cdots + s_{\gamma_{p+1}} = m\} . \end{aligned}$$

THEOREM 6.1. *Suppose* $X_1, \cdots, X_{p+1}$ *is the least solution of the equations corresponding to* $(\gamma_1^*, \cdots, \gamma_{p+1}^*)$ *in Theorem* 4.2. *Then the number of cycles in* $\bar{\mathscr{M}}$ *corresponding to* $(\gamma_1^*, \cdots, \gamma_{p+1}^*)$ *is*

$$\prod_{i=1}^{p+1} w_i / X_{p+1}\gamma_{p+1}^*$$

where

$$w_{p+1} = \#\{\textit{the elements in } \mathscr{N}_{p+1} \textit{ with cycle period } \gamma_{p+1}^*\}$$

and for $1 \leqq j \leqq p$

$$w_j = \sum_{t=1}^{\alpha_j^*} t \cdot w_{j,t}$$

where

$$w_{j,t} = \#\{(d_1, \cdots, d_{r_j}) \in \mathscr{N}_j \textit{ with cycle period } \gamma_j^* \textit{ and } d_1 = t\} .$$

Proof. Suppose $A \in \mathscr{M}$ corresponds to $(\gamma_1^*, \cdots, \gamma_{p+1}^*)$. In the proof of Theorem 4.2 we prove that $Y = X_{p+1}\gamma_{p+1}^*$ is the least integer such that $\psi^Y(A) = A$. Hence, there are $X_{p+1}\gamma_{p+1}^*$ elements in $\mathscr{M}$ on the same cycle as A. Hence, the proof will be complete if we can prove

$$\#\{A \in \mathscr{M} : A \text{ corresponds to } (\gamma_1^*, \cdots, \gamma_{p+1}^*)\} = \prod_{i=1}^{p+1} w_i .$$

We get by Lemma 3.2 that

$$\begin{aligned}\#\{A \in \mathscr{M} &: A \text{ corresponds to } (\gamma_1^*, \cdots, \gamma_{p+1}^*)\} \\ &= \prod_{i=1}^{p+1} \#\{D_i(A) : D_i(A) \text{ corresponds to } \gamma_i^* \text{ and } A \in \mathscr{M}\} .\end{aligned}$$

Hence, the proof will be complete if we can prove $(1 \leqq i \leqq p+1)$

$$\#\{D_i(A) : D_i(A) \text{ corresponds to } \gamma_i^* \text{ and } A \in \mathscr{M}\} = w_i . \tag{6.1}$$

First we will prove that (6.1) is true for $i = p+1$. It is sufficient to prove that the map

$$\eta_{p+1} : \{D_{p+1}(A) : A \in \mathscr{M}\} \longrightarrow \mathscr{N}_{p+1}$$

defined in Proposition 4.3 is bijective: Let $(d_1, \cdots, d_{r_{p+1}}) \times (s_1, \cdots, s_{r_{p+1}}) \in \mathscr{N}_{p+1}$. Then there exists one and only one $D_{p+1}(A)$ such that

$$\eta_{p+1}(D_{p+1}(A)) = (d_1, \cdots, d_{r_{p+1}}) \times (s_1, \cdots, s_{r_{p+1}}) .$$

This $D_{p+1}(A) = (t_1, \cdots, t_{r_{p+1}}) \times (s_1, \cdots, s_{r_{p+1}})$ is given by $t_1 = d_1$, $t_2 = d_2 + t_1 + s_1$, $t_3 = d_3 + t_2 + s_2$, etc.

Next we will prove (6.1) in the case $i < p+1$, and we do the following observation ($i = 1, \cdots, p$):

To each $(d_1, \cdots, d_{\gamma_i}) \in \mathscr{N}_i$ there exists exactly d_1 elements $D = D_i(A)$ such that $\rho_i(D) = (d_1, \cdots, d_{\gamma_i})$ where ρ_i is as in Proposition 4.3.

These elements are

$$\left(s, s + d_2, s + d_2 + d_3, \cdots, s + \sum_{j=2}^{\gamma_i} d_j\right) \text{ where } s = 1, \cdots, d_1 .$$

(6.1) follows from this observation in the case $i < p + 1$.

The next theorem gives us a way of calculating w_{p+1} and $w_{j,t}$.

THEOREM 6.2. (a) *We let $\sigma(r, s, t)$ = the number of elements in*

$$\mathscr{C}(r, s, t) = \{(d_1, \cdots, d_s) : d_i \geqq 0,\ d_1 = r,\ d_1 + \cdots + d_s = t \text{ and } (d_1, \cdots, d_s) \text{ has trivial period } s\} .$$

Then $\sigma(r, s, t)$ can be calculated inductively by the following formula:

$$\sigma(r, s, t) = \binom{t + s - r - 2}{s - 2} - \sum \left\{\sigma\left(r, \frac{s}{s'}, \frac{t}{s'}\right) : \frac{s}{s'} \text{ and } \frac{t}{s'} \text{ are integers}\right\} .$$

( ) is the binomial coefficient.

(b) *We let $\sigma(s, t)$ = the number of elements in*

$$\mathscr{C}(s, t) = \{(d_1, \cdots, d_s) : d_i \geqq 0,\ d_1 + \cdots + d_s = t \text{ and } (d_1, \cdots, d_s) \text{ has trivial period } s\} .$$

Then $\sigma(s, t)$ can be calculated inductively by the following formula:

$$\sigma(s, t) = \binom{t + s - 1}{s - 1} - \sum \left\{\sigma\left(\frac{s}{s'}, \frac{t}{s'}\right) : \frac{s}{s'} \text{ and } \frac{t}{s'} \text{ are integers}\right\} .$$

(c) *The number of elements in*

$$\mathscr{Q}(s, t) = \{(d_1, \cdots, d_s) : d_i \geqq 0 \text{ and } d_1 + \cdots + d_s = t\} \text{ is } \binom{s + t - 1}{s - 1} .$$

(d) *$w_{i,t} = \sigma(t, \gamma_i^*, \alpha_i^*)$ for $1 \leqq i \leqq p$ and $1 \leqq t \leqq \alpha_i^*$.*

(e) *Let $m^* = m \cdot \gamma_{p+1}^* / \gamma_{p+1}$. Then we have*

$$w_{p+1} = r_1 \cdot q_1 + r_2 \cdot q_2 - r_1 \cdot r_2$$

where

$$r_1 = \sigma(\gamma_{p+1}^*, \alpha_{p+1}^* - m^*) \quad \textit{and} \quad q_1 = \binom{m^* + \gamma_{p+1}^* - 1}{\gamma_{p+1}^* - 1}$$

$$r_2 = \sigma(\gamma_{p+1}^*, m^*) \quad \textit{and} \quad q_2 = \binom{\alpha_{p+1}^* - m^* + \gamma_{p+1}^* - 1}{\gamma_{p+1}^* - 1} .$$

Proof. (a)

$$\begin{aligned}\{(d_1, \cdots, d_s)&: d_i \geqq 0,\ d_1 = r \text{ and } d_1 + \cdots + d_s = t\}^\# \\ &= \{(d_2, \cdots, d_s): d_i \geqq 0 \text{ and } d_2 + \cdots + d_s = t - r\}^\# \\ &= \text{the number of ways to divide } (t - r) \text{ 1's into} \\ &\quad (s-1) \text{ groups} \\ &= \text{the number of ways to put } s - 2 \text{ 0's into} \\ &\quad (t + s - r - 2) \text{ positions} \\ &= \binom{t + s - r - 2}{s - 2} .\end{aligned}$$

We subtract those $(d_1, \cdots, d_s)$ with trivial period less than s. For each s' such that s/s' and t/s' are integers, $(d_1, \cdots, d_s) \to (d_1, \cdots, d_{s/s'})$ is a bijective correspondence between

$$\{(d_1, \cdots, d_s): 0 \leqq d_i,\ d_1 = r,\ d_1 + \cdots + d_s = t \text{ and } (d_1, \cdots, d_s) \text{ has trivial period } s/s'\}$$

and

$$\mathscr{C}(r, s/s', t/s') .$$

By using these correspondences (a) follows.

(b) and (c) are proved in the same way.

(d) By definition $w_{i,t}$ is the number of elements in the set

$$\mathscr{A}_1 = \{(d_1, \cdots, d_{\gamma_i}) \in \mathscr{N}_i;\ d_1 = t \text{ and } (d_1, \cdots, d_{\gamma_i}) \text{ has cycle period } \gamma_i^*\} .$$

The map from $\mathscr{A}_1$ into $\mathscr{C}(t, \gamma_i^*, \alpha_i^*)$ given by

$$(d_1, \cdots, d_{\gamma_i}) \longrightarrow (d_1, \cdots, d_{\gamma_i^*})$$

is bijective, and (d) follows.

(e) By definition w_{p+1} is the number of elements in the set

$$\mathscr{A}_2 = \{(d_1, \cdots, d_{\gamma_{p+1}}) \times (s_1, \cdots, s_{\gamma_{p+1}}) \in \mathscr{N}_{p+1} \text{ which has cycle period } \gamma_{p+1}^*\} .$$

We define

$$\begin{aligned}\mathscr{A}_3 = \{&(d_1, \cdots, d_{\gamma_{p+1}^*}) \times (s_1, \cdots, s_{\gamma_{p+1}^*}): d_i \geqq 0,\ s_i \geqq 0, \\ &d_1 + \cdots + d_{\gamma_{p+1}^*} = \alpha_{p+1}^* - m^*,\ s_1 + \cdots + s_{\gamma_{p+1}^*} = m^* \text{ and} \\ &(d_1, \cdots, d_{\gamma_{p+1}^*}) \text{ or } (s_1, \cdots, s_{\gamma_{p+1}^*}) \text{ has cycle period } \gamma_{p+1}^*\} .\end{aligned}$$

The map from $\mathscr{A}_2$ into $\mathscr{A}_3$ given by

$$(d_1, \cdots, d_{r_{p+1}}) \times (s_1, \cdots, s_{r_{p+1}}) \longrightarrow (d_1, \cdots, d_{r^*_{p+1}}) \times (s_1, \cdots, s_{r^*_{p+1}})$$

is bijective. We observe that

$$\# \mathscr{A}_3 = r_1 \cdot q_1 + r_2 \cdot q_2 - r_1 \cdot r_2$$

where

$$r_1 = \# \mathscr{C}(\gamma^*_{p+1}, \alpha^*_{p+1} - m^*) \quad \text{and} \quad q_1 = \mathscr{Q}(\gamma^*_{p+1}, m^*)$$
$$r_2 = \# \mathscr{C}(\gamma^*_{p+1}, m^*) \quad \text{and} \quad q_2 = \mathscr{Q}(\gamma^*_{p+1}, \alpha^*_{p+1} - m^*)$$

and (e) follows.

7. The reduction. We will reduce the cycle structure problem to the set studied in the §§ 3–6. First we need two lemmas. $C < D$ means C contained in D and $C \neq D$. If $D = a_r \cdots a_s$, we define $(t \in D \Leftrightarrow r \leqq t \leqq s)$ and $f_D(t) = f(a_r \cdots a_t)$.

We need more precise notation. If we are working with A we write

$$\alpha_i(A),\ \gamma_i(A) \text{ and } m_A \text{ instead of } \alpha_i,\ \gamma_i \text{ and } m\ .$$

LEMMA 7.1. *Suppose* $A = 0_{i_1} B_1 C_1 0_{i_2} B_2 C_2 \cdots 0_{i_f} B_f$ *where* B_i *is a block on level* 1. *Moreover, we suppose* $f(C_i) = -type\,(B_i)$ *and* $0 > f_{C_i}(t) \geqq -type\,(B_i)$ *for* $t \in C_i$.

Then we have

$$n + type\,(B_f) = \left(\sum_{i=1}^{p+1} 2i\gamma_i\right) + m_A + (i_1 + \cdots + i_f)\ ,$$

and if $type\,(B_f) \geqq type\,(B_i)$ *for* $i = 1, \cdots, f$ *then*

$$\alpha_{type\,(B_f)}(A) = m_A \Longleftrightarrow i_1 + \cdots + i_f = 0\ .$$

Proof. We let $C_f = 0_{\mathrm{type}\,(B_f)}$ and consider $A^* = AC_f = 0_{i_1} B_1 C_1 \cdots 0_{i_f} B_f C_f$.

As in the proof of Lemma 4.13 in [2] we get

$$\text{the length of } \ B_i = f(B_i) + \sum \{2 \cdot \mathrm{type}\,(B^*) \colon B^* < B_i\}\ ,$$
$$\text{the length of } \ C_i = \mathrm{type}\,(B_i) + \sum \{2 \cdot \mathrm{type}\,(B^*) \colon B^* < C_i\}\ .$$

If $\mathrm{type}\,(B_i) = p + 1$, we therefore have

$$\text{the length of } \ B_i C_i = [f(B_i) - (p+1)] + \sum \{2 \cdot \mathrm{type}\,(B^*) \colon B^* < B_i C_i\}\ .$$

Otherwise,

$$\text{the length of } \ B_i C_i = \sum \{2 \cdot \mathrm{type}\,(B^*) \colon B^* < B_i C_i\}\ .$$

Hence,

$$\begin{aligned}\text{the length of } A^* &= \sum \{f(B_i) - (p+1)\colon \text{type}\,(B_i) = p+1\} \\ &\quad + \sum \{2\cdot \text{type}\,(B^*)\colon B^* \text{ a block}\} + (i_1 + \cdots + i_f) \\ &= m_A + \left(\sum_{i=1}^{p+1} 2i\gamma_i\right) + (i_1 + \cdots + i_f)\,.\end{aligned}$$

The equivalence follows by the definition of $\alpha_{\text{type}\,(B_f)}(A)$. □

We write

$$\theta_{k,p} = \theta_{E_k + \cdots + E_{k+p}}\,. \tag{7.1}$$

LEMMA 7.2. *We suppose the block structure of $A \in \{0, 1\}^n$ is determined with respect to p. Moreover, we suppose $w(A) = k + p + 1$. Then we have*

$$\begin{aligned}&([\gamma_{p+1}(A) \neq 0 \text{ and } \alpha_{p+1}(A) = m_A] \text{ or} \\ &\quad [z = \sup_i \{i\colon \gamma_i(A) \neq 0\} < p + 1 \text{ and } \alpha_z(A) = 0]) \\ &\qquad \Longleftrightarrow \theta^j_{k,p}(A) = \theta^j_{k,p'}(A) \quad \text{for} \quad p' > p \quad \text{and every} \quad j\,.\end{aligned}$$

Proof. We suppose first $\gamma_{p+1}(A) \neq 0$. By Lemma 4.4 in [2] there exists q such that $\bar{A} = \theta^q_{k,p}(A)$ satisfies $\gamma_i(A) = \gamma_i(\bar{A})$, $\alpha_i(A) = \alpha_i(\bar{A})$, $m_A = m_{\bar{A}}$, $\bar{A}$ ends with a $(p+1)$-block, $\bar{A}$ starts with 0 or a $(p+1)$-block and $w(\bar{A}) = k + p + 1$.

Moreover, $\bar{A}$ has the form

$$\bar{A} = 0_{i_1} B_1 C_1 0_{i_2} B_2 C_2 \cdots 0_{i_f} B_f \quad \text{as in Lemma 7.1}\,.$$

(If $f = 1$, then $\bar{A} = 0_{i_1} B_1$.)

We suppose $\theta^j_{k,p}(A) = \theta^j_{k,p'}(A)$ for $p' > p$. If $i_1 \neq 0$, then $w(\theta_{k,p+1}(A)) = k + p + 2 \neq w(\theta_{k,p}(A))$. Hence, $i_1 = 0$. By Lemma 5.7 in [2] we have

$$w(\theta^s_{k,p}(\bar{A})) = k + p + 1 \quad \text{where} \quad s = \text{length of } B_1 C_1\,.$$

In the same way we prove $i_1 = \cdots = i_f = 0$. By Lemma 7.1 $\alpha_{p+1}(\bar{A}) = m_{\bar{A}}$. Hence, $\alpha_{p+1}(A) = m_A$.

Next we suppose $\alpha_{p+1}(A) = m_A$. Hence, $\alpha_{p+1}(\bar{A}) = m_{\bar{A}}$. By Lemma 7.1 we have $i_1 + \cdots + i_f = 0$. Hence, type $(B_1) = p + 1$. Moreover. let $j = \inf\{i > 1\colon \text{type}\,(B_i) = p + 1\}$. Put $C_1'' = '' C_1 B_2 C_2 \cdots B_{j-1} C_{j-}$ and $B_2'' = '' B_j$. By continuing in this way we can suppose type $(B_1) = \cdots =$ type $(B_f) = p + 1$. Hence, by Lemma 5.6(c) in [2] we get $\theta^j_{k,p}(\bar{A}) = \theta^j_{k,p'}(\bar{A})$ for $p' > p$.

Finally we treat the case $z = \sup_i \gamma_i(A) < p + 1$. By Lemma 5.6 (a) in [2] we have $\theta^j_{k,p}(A) = \theta^j_{k_1,p_1}(A)$ where $k_1 = p + 1 - z$ and $p_1 = z - 1$. By Lemma 4.4 in [2] there exists q such that $\bar{A} = \theta^q_{k,p}(A)$ satisfies:

$\gamma_i(A) = \gamma_i(\bar{A})$, $\alpha_i(A) = \alpha_i(\bar{A})$, $m_A = m_{\bar{A}} = 0$, $\bar{A}$ ends with a z-block, $\bar{A}$ starts with 0 or a z-block and $w(\bar{A}) = k + p + 1$. Moreover, $\bar{A}$ has the form

$$\bar{A} = 0_{i_1} B_1 C_1 0_{i_2} B_2 C_2 \cdots 0_{i_f} B_f \quad \text{as in Lemma 7.1.}$$

We suppose $\theta^j_{k,p}(A) = \theta^j_{k,p'}(A)$ for $p' > p$. As in the case $\gamma_{p+1}(A) \neq 0$ we prove $i_1 = \cdots = i_f = 0$. By Lemma 7.1 $\alpha_z(A) = m_A = 0$.

Next we suppose $\alpha_z(A) = 0$. Hence, $\alpha_z(\bar{A}) = m_{\bar{A}} = 0$. By Lemma 7.1 we have $i_1 + \cdots + i_f = 0$. As before we can suppose type $(B_1) = \cdots =$ type $(B_f) = z$. Hence, by Lemma 5.6 (c) we get $\theta^j_{k,p}(\bar{A}) = \theta^j_{k,p'}(\bar{A})$ for $p' > p$. □

Previously in this paper we have not mentioned the possible values of $(\gamma_1, \cdots, \gamma_{p+1})$. However, by Lemma 4.1 in [2] we have the following result (k, p and n are given)

$(\gamma_1, \cdots, \gamma_{p+1})$ is a possible vector if and only if

$$\exists m \geqq 0 \text{ such that } m + \sum_{i=1}^{p+1} i \cdot \gamma_i = k + p + 1$$

and

$$m + 2 \cdot \sum_{i=1}^{p+1} i \cdot \gamma_i \leqq n + p + 1$$

(m corresponds to m defined previously).

The results obtained in this paper give a complete description of the cycle structure of $\mathscr{M}$ where

(7.2) $\mathscr{M}$ = the union of all $\mathscr{M}$ defined in (3.2) corresponding to the possible vectors $(\gamma_1, \cdots, \gamma_{p+1})$ satisfying $\gamma_{p+1} \neq 0$.

Now we start the reduction process. For $\mathscr{S} \subset \{0, 1\}^n$, we define the closure of $\mathscr{S}$ with respect to θ by

$$\bar{\mathscr{S}} = \{\theta^i(A) \colon A \in \mathscr{S}\}.$$

We let $\theta = \theta_{k,p}$ and we define

$$\mathscr{F} = \{A \colon k \leqq w(\theta^i(A)) \leqq w(A) \leqq k + p + 1 \ \forall\, i\}.$$

If $A \notin \bar{\mathscr{F}}$, then $\theta^i(A) = C^i(A)\ \forall\, i$, where $C(a_1, \cdots, a_n) = a_2 \cdots a_n a_1$ is the pure cycling register. Hence, it is enough to study $\bar{\mathscr{F}}$. We define

$$\mathscr{D}(i, j) = \{A \in \mathscr{F} \colon k + i = \inf_s w(\theta^s(A)) \leqq w(A) = k + j\}.$$

Then we have obviously that

$$\bar{\mathscr{F}} = \bigcup_{i \leq j} \overline{\mathscr{D}(i, j)}$$

is a disjoint union. Hence, it is sufficient to determine the cycle structure of the sets $\overline{\mathscr{D}(i, j)}$. First we need an observation:

Observation 7.3. Suppose $\theta = \theta_{k,p}$, $w(A) = k + p + 1$ and $0 \leqq p' < p$. Then we have

$$\begin{aligned} &\gamma_{p'+1} \neq 0 \quad \text{ and} \\ &\gamma_{p'+2} = \cdots = \gamma_{p+1} = 0 \Longleftrightarrow \inf_s w(\theta^s(A)) = k + p - p' . \end{aligned}$$

Proof. This follows directly from the definition of the blocks, or for example from Lemma 5.1 in [2].

We also need very precise notation. If we are working with p we write α_i^p, γ_i^p and m^p instead of α_i, γ_i and m.

Case 1. $\overline{\mathscr{D}(0, p + 1)} = \bar{\mathscr{M}}$ where $\mathscr{M}$ is as in (7.2).

Proof. Let $A \in \mathscr{D}(0, p+1)$. By Observation 7.3 we have $\gamma_{p+1} \neq 0$. By Lemma 4.4 in [2] there exists s such that $\theta^s(A) \in \mathscr{M}$ and the claim follows.

Case 2. If $0 \leqq i < j < p + 1$, we can determine $\overline{\mathscr{D}(i, j)}$ in the following way: Let $k' = k + i$, $p' = j - i - 1$ and let $\mathscr{M}$ be as in (7.2) with respect to k' and p'. Then

$$\begin{aligned} \overline{\mathscr{D}(i, j)} &= \overline{\{A \in \mathscr{M} : \alpha_{p'+1} = 0\}} \quad \text{if} \quad i > 0 \\ \overline{\mathscr{D}(i, j)} &= \{A \in \mathscr{M} : \alpha_{p'+1} = m\} \quad \text{if} \quad i = 0 \end{aligned}$$

where $\alpha_{p'+1}$ and m are determined with respect to p'. Moreover, the closure of $\mathscr{D}(i, j)$ with respect to $\theta_{k,p}$ and $\theta_{k',p'}$ respectively are equal.

Proof. Let $p'' = j - 1$ and $A \in \mathscr{D}(i, j)$. By Lemma 7.2 there are two possibilities:

(1) If $\gamma_{p''+1}^{p''} \neq 0$, then $\alpha_{p''+1}^{p''} = m^{p''}$.

(2) If $\gamma_z^{p''} \neq 0$ and $\gamma_{z+1}^{p''} = \cdots = \gamma_{p''+1}^{p''} = 0$, then $\alpha_z^{p''} = 0$.

We suppose first that $i > 0$. By Observation 7.3 we are in Case 2 with $z = j - i$ since

$$k + p'' + 1 - (j - i) = k + i \leqq w(\theta^s(A)) \leqq k + p'' + 1 .$$

Hence, we have $\alpha_z^{p''} = \alpha_{p'+1}^{p''} = 0$ and $\gamma_z^{p''} = \gamma_{p'+1}^{p''} \neq 0$. Since, $\gamma_{z+1}^{p''} = \cdots = \gamma_{p''+1}^{p''} = 0$ we have

$$\alpha^{p'}_{p'+1} = \alpha^{p''}_{p'+1} = 0 \quad \text{and} \quad \gamma^{p'}_{p'+1} = \gamma^{p''}_{p'+1} \neq 0 .$$

By Lemma 4.4 in [2] there exists s such that $\theta^s_{k',p'}(A) \in \mathscr{M}$ where $\mathscr{M}$ is defined as in (7.2) with respect to k' and p'.

Next we suppose $i = 0$. Then we are in Case 1 and $p'' = p'$. Hence, we have $\alpha^{p'}_{p'+1} = m^{p'}$ and $\gamma^{p'}_{p'+1} \neq 0$. By Lemma 4.4 in [2] there exists s such that $\theta^s_{k',p'}(A) \in \mathscr{M}$ where $\mathscr{M}$ is defined as in (7.2) with respect to k' and p'.

Case 3. If $0 < i < j = p + 1$, then

$$\overline{\mathscr{D}(i, j)} = \overline{\{A \in \mathscr{M} : m = 0\}}$$

where $\mathscr{M}$ and m is defined with respect to $k' = k + i$ and $p' = p - i$. Moreover, the closure of $\mathscr{D}(i, j)$ with respect to $\theta_{k,p}$ and $\theta_{k',p'}$ respectively are equal.

Proof. Let $A \in \mathscr{D}(i, j)$. By Observation 7.3 we have

$$(*) \qquad \gamma^{p'}_{p'+2} = \cdots = \gamma^{p'}_{p+1} = 0 .$$

Hence, $m^{p'} = 0$. Namely, if $m^{p'} \neq 0$, then (*) would not be true.

Moreover, by Lemma 5.6 in [2] we have

$$\theta^s_{k,p'}(A) = \theta^s_{k,p}(A) \quad \forall\, s$$

and there exists s such that $\theta^s_{k',p'}(A) \in \mathscr{M}$ where $\mathscr{M}$ is defined with respect to k' and p'. Hence the proof of Case 3 is complete.

Case 4. If $i = j$, then $\overline{\mathscr{D}(i, i)} = \varnothing$ except in the following case: If $k + p + 1 = n$, then $\overline{\mathscr{D}(p + 1, p + 1)} = \{A = 1_n\}$.

The proof of Case 4 is obvious.

Finally we will mention how to determine the minimal period for $A \in \{0, 1\}^n$ with respect to $\theta_{k,p}$ in the following 4 steps:

1. If $w(A) \notin \{k, \cdots, k + p + 1\}$, then $\theta_{k,p}(A) = \xi(A)$ where $\xi(a_1 \cdots a_n) = (a_2 \cdots a_n a_1)$ and the problem is trivial. We therefore suppose $w(A) \in \{k, \cdots, k + p + 1\}$.

2. We calculate $w(A), w(\theta_{k,p}(A)), \cdots, w(\theta^{2n}_{k,p}(A))$ and choose j such that $A^* = \theta^j_{k,p}(A)$ satisfies

$$w(A^*) = \sup_{1 \leq i \leq 2n} w(\theta^i_{k,p}(A)) = \sup_i w(\theta^i_{k,p}(A)) .$$

3. Put $p' = w(A^*) - k - 1$. Then we can use $\theta_{k,p'}$ instead of $\theta_{k,p}$ (Lemma 5.6 (b) in [2]). We have $w(A^*) = k + p' + 1$.

4. Next we determine the block structure of A^* with respect to p'. We put $j = \sup\{i : \gamma^{p'}_i(A) \neq 0\}$, and $k'' = p' - j$ and $p'' = j - 1$. Then we can use $\theta_{k'',p''}$ instead of $\theta_{k,p}$ (Lemma 5.6 (a) in [2]). More-

over, we have $w(A^*) = k'' + p'' + 1$ and $\gamma^{p''}_{p''+1}(A^*) \neq 0$. Hence, we can use Theorem 4.2.

REFERENCES

1. J. Søreng, *The periods of the sequences generated by some shift registers*, J. Combinatorial Theory, Ser. A, **21** (1976), 165–187.
2. ———, *Symmetric shift registers*, Pacific J. Math., **85** (1979), 201–229.

Received September 19, 1978 and in revised form November 2, 1979.

UNIVERSITY OF OSLO
BLINDERN, OSLO 3, NORWAY

PACIFIC JOURNAL OF MATHEMATICS

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced, (not dittoed), double spaced with large margins. Please do not use built up fractions in the text of the manuscript. However, you may use them in the displayed equations. Underline Greek letters in red, German in green, and script in blue. The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. Please propose a heading for the odd numbered pages of less than 35 characters. Manuscripts, in triplicate, may be sent to any one of the editors. Please classify according to the scheme of Math. Reviews, Index to Vol. **39**. Supply name and address of author to whom proofs should be sent. All other communications should be addressed to the managing editor, or Elaine Barth, University of California, Los Angeles, California, 90024.

50 reprints to each author are provided free for each article, only if page charges have been substantially paid. Additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is issued monthly as of January 1966. Regular subscription rate: $102.00 a year (6 Vols., 12 issues). Special rate: $51.00 a year to individual members of supporting institutions.

Subscriptions, orders for numbers issued in the last three calendar years, and changes of address shoud be sent to Pacific Journal of Mathematics, P.O. Box 969, Carmel Valley, CA 93924, U.S.A. Old back numbers obtainable from Kraus Periodicals Co., Route 100, Millwood, NY 10546.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.). 8-8, 3-chome, Takadanobaba, Shinjuku-ku, Tokyo 160, Japan.

Pacific Journal of Mathematics

Vol. 98, No. 1 March, 1982