ISBN 82-553-0353-7
Mathematics
No 10 - September
SYMmetric Shift Registers
part 2
by
Jan Søreng
Oslo

PREPRINTS SERIES - Matematisk institutt, Universitetet i Oslo
Abstract

We study symmetric shift registers defined by

\[(x_1, \ldots, x_n) \rightarrow (x_2, \ldots, x_{n+1})\]

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

Introduction

In this paper we study symmetric shift registers over the field \(GF(2) = \{0, 1\}\). 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 \(\theta_S\) corresponding to \(S(x_2, \ldots, x_n)\) where \(S\) is a symmetric polynomial, is defined by

\[\theta_S(x_1, \ldots, x_n) = (x_2, \ldots, x_{n+1})\]  where \(x_{n+1} = x_1 + S(x_2, \ldots, x_n)\).

\(q\) is the minimal period of \(A \in \{0, 1\}^n\) with respect to \(\theta_S\) if \(q\) is the least integer such that \(\theta_S^q(A) = A\). Then \(A \rightarrow \theta_S(A) \rightarrow \ldots \rightarrow \theta_S^q(A) = A\) 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 \( S = E_k + \ldots + E_{k+p} \) where \( E_i \) is defined by

\[
E_i(x_2, \ldots, x_n) = 1 \text{ if and only if } \sum_{j=2}^{n} x_j = i.
\]

In this paper we will only study \( S = E_k + \ldots + E_{k+p} \).

I will now roughly describe the structure of the proof. First we need a definition. Suppose \( \mathcal{M} \subseteq \{0,1\}^n \) is a set such that for all \( A \in \mathcal{M} \) there exists an \( i > 0 \) such that \( \theta_i^S(A) \in \mathcal{M} \). Then we define \( \text{Index} : \mathcal{M} \rightarrow \{1,2,\ldots\} \) and \( \psi : \mathcal{M} \rightarrow \mathcal{M} \) in the following way:

Let \( i > 0 \) be the least integer such that \( \theta_i^S(A) \in \mathcal{M} \), then we define \( \text{Index}(A) = i \) and \( \psi(A) = \theta_i^S(A) \).

In the proof we need only consider certain subsets \( \mathcal{N} \) which can be represented in a nice way. We will find for each \( A \in \mathcal{N} \) a minimal \( q > 0 \) such that \( \psi^q(A) = A \). Then

\[
\text{Index}(A) + \text{Index}(\psi(A)) + \ldots + \text{Index}(\psi^{q-1}(A))
\]

is the minimal period of \( A \).

We give now a short outline of the paper. Section 2 contains some definitions and notations. In Section 3 we study a function \( \Lambda \) which we need later. In Section 4 we compute \( \psi \) for a certain subset \( \mathcal{M} \). In the Sections 5, 6 and 7 we solve the problems 1, 2 and 3 respectively for the set \( \mathcal{M} \). In Section 8 we generalize the results to all \( A \in \{0,1\}^n \). This generalization will not be difficult.

[2] is revised. In an appendix we give a summary of the new results in the revised version.
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 $i \geq 0$.

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

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

Moreover, $a \wedge b$ denotes the minimum of $a$ and $b$.

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).

**Def. 2.1**: With respect to $p$ we define that $D = a_r \ldots a_s$ is a 1-structure of mass $q$ of $A^* = a_1 \ldots a_n a_{n+1} \ldots a_{n+p+1} \in \{0,1\}^{n+p+1}$ if the following 3 conditions are satisfied:

1) $0 < f(a_r \ldots a_i) \leq f(a_r \ldots a_s) = q$ for $i \in \{r, \ldots , s\}$.

2) There exists $t > s$ such that $0 > f(a_s \ldots a_i) > f(a_{s+1} \ldots a_t) = -q \wedge (p+1)$ for $i \in \{s+1, \ldots , t\}$.

3) If $a_i \ldots a_j \leq a_r \ldots a_s$, then $f(a_i \ldots a_j) > -q \wedge (p+1)$.

$D$ is a 0-structure of mass $q$ if $D$ satisfies 1), 2) and 3) with $f$ replaced by $-f$. 
3) implies that the 0's in a 1-structure (respectively the 1's in a 0-structure) are not too close to each other. If $q \leq p + 1$, then 3) follows from 1) by using $f(a_r \ldots a_i \ldots a_j) = f(a_r \ldots a_i) + f(a_{i+1} \ldots a_j)$.

Def. 2.2: Suppose $A = a_1 \ldots a_n \in \{0,1\}^n$. Let $A^* = a_1 \ldots a_n a_{n+1} \ldots a_{n+p+1} = A_{0 \ldots p+1}$. We define the blocks in $A^*$ with respect to $p$ by induction with respect to the level of the blocks:

**Basisstep:** $A^*$ is a block on level 0.

**Induction step:** Suppose $B$ is a block on level $i$. If $i \in \{0,2,4,\ldots\}$, we can decompose $B$ (uniquely) in the following way:

$$B = i_1 B_1 0_i B_2 \ldots B_m 0_{m+1}$$

where $B_i$ is a 1-structure.

If $i$ is odd, we can decompose $B$ (uniquely) in the following way:

$$B = i_1 B_1 1_i B_2 \ldots B_m 1_{m+1}$$

where $B_i$ is a 0-structure.

By definition $B_i$ is a block on level $(i+1)$. We denote the mass of $B_i$ by $m(B_i)$. We define $\text{type}(B_i) = m(B_i) \wedge (p+1)$.

By definition {the blocks of $A$} are {the blocks of $A^*$} \( \{A^*\} \).

We establish the convention that $B$ always denotes a block. Moreover, we suppose $k$ and $p$ are fixed integers such that $0 \leq k \leq k+p \leq n-1$. The block structure is always determined with respect to $p$ and we always work with $S = E_k \ldots + E_{k+p}$. We write $\theta = \theta_S$. These conventions do not concern Section 8.

If $A = a_1 \ldots a_n$, we write $l_A(a_i \ldots a_j) = i$ and $r_A(a_i \ldots a_j) = j$. Next we define $d(B)$ which measures how far the block $B$ is to the left in $A$. Suppose $A = a_1 \ldots a_n$. We
define
\[ d_q(a_1 \ldots a_j) = j - \Sigma \{ q \in \text{type}(B) : l_A(B) \leq j \} - \Sigma \{ q \in \text{type}(B) : r_A(B) \leq j \}. \]

If \( B \) is a block of \( A \), then we define \( d(B) = 0 \) if \( l_A(B) = 1 \). Otherwise,
\[ d(B) = d_q(a_1 \ldots a_j) \quad \text{where} \quad j = l_A(B) - 1 \quad \text{and} \quad q = \text{type}(B). \]

Moreover, we define \( w(\cdot) \) by \( w(a_1 \ldots a_n) = \Sigma_{i=1}^{n} a_i \).

3. The function \( \Lambda \).

In this section we study the functions \( \Lambda(a) \) and \( \Lambda(a,m) \). We will use these functions to formulate and study how \( d(B) \) (the distance of a block \( B \)) changes by applying the shift register.

Def. 3.1: a) For \( (t_1, \ldots, t_\gamma) \in \bigcup (a) = \{(t_1, \ldots, t_\gamma) : 1 \leq t_1 \leq \ldots \leq t_\gamma \leq a\} \)
we define
\[ \Lambda(a)(t_1, \ldots, t_\gamma) = (t_1 - 1, \ldots, t_\gamma - 1, a, \ldots, a) \in \{1, 2, \ldots, a\}^\gamma \]
where \( i \) is the least index such that \( t_i > 1 \). Specially,
\[ \Lambda(a)(1, \ldots, 1) = (a, \ldots, a). \]

b) We define \( \bigcup(a,m) \) by
\[ [(t_1^{s_1}, \ldots, t_\gamma^{s_\gamma})] \in \bigcup(a,m) \]
if and only if
\[ 0 \leq t_1 \leq t_2 \ldots \leq t_\gamma \leq a \]
\[ t_i + s_i \leq t_{i+1} \quad \text{for} \quad i = 1, \ldots, \gamma - 1 \]
\[ t_\gamma + s_\gamma = a \]
\[ s_i \geq 0 \quad \text{and} \quad s_1 + \ldots + s_\gamma = m. \]

For \( \tilde{t} = [(t_1^{s_1}, \ldots, t_\gamma^{s_\gamma})] \in \bigcup(a,m) \) we define
\[ \Lambda(\alpha, m)(\xi) = \left[ \begin{array}{c}
\left( t_2 - t_1 - s_1 \right) \\
\left( t_3 - t_1 - s_1 \right) \\
\vdots \\
\left( t_\gamma - t_1 - s_1 \right) \\
\left( a - s_1 \right) 
\end{array} \right] \]

We observe that \( \Lambda(\alpha) : D(\alpha) \rightarrow D(\alpha) \) and \( \Lambda(\alpha, m) : D(\alpha, m) \rightarrow D(\alpha, m) \). We will now indicate how to use these functions. First we need a definition.

**Def. 3.2:** Suppose \( B_1, \ldots, B_\gamma \) are the \( i \)-blocks of \( A \in \{0,1\}^n \) ordered from the left to the right. We define

\[
D_i(A) = (d(B_1), \ldots, d(B_\gamma)) \quad \text{if} \quad i \leq p.
\]

\[
D_{p+1}(A) = \left[ \left( \frac{d(B_1)}{m(B_1)-(p+1)} \right), \ldots, \left( \frac{d(B_\gamma)}{m(B_\gamma)-(p+1)} \right) \right] \quad \text{if} \quad i = p+1.
\]

The vectors \( D_1(A), \ldots, D_{p+1}(A) \) determine the blockstructure of \( A \) completely. In the next sections we will study a subset \( M \subset \{0,1\}^n \) where it is possible to define \( \psi \) as in the introduction. For each \( A \in M \) and \( q > 0 \) we will determine integers \( \alpha_i, m \) and \( \beta_i \) such that (\( \alpha_i \) and \( m \) will be independent of \( q \))

\[
D_i(\psi^q(A)) = \Lambda(\alpha_i, m)(D_i(A)) \quad \text{for} \quad i = 1, \ldots, p \quad \text{and}
\]

\[
D_{p+1}(\psi^q(A)) = \Lambda(\alpha_{p+1}, m)(D_{p+1}(A)).
\]

We will now prove two lemmas which determine when

\[ \xi = \Lambda(\alpha)(\xi) \quad \text{and} \quad \xi = \Lambda(\alpha, m)(\xi). \]

**Def. 3.3:** a) The difference vector of \( \xi = (t_1, \ldots, t_\gamma) \) with respect to \( \alpha \) is

\[
(a+t_1-t_\gamma, t_2-t_1, t_3-t_2, \ldots, t_\gamma-t_\gamma-1).
\]
b) The difference vector of \( t = \left[ \begin{array}{c} t_1 \\ \vdots \\ t_{\gamma} \end{array} \right] \) with respect to \( a \) is

\[
\left[ \begin{array}{c}
(a + t_1 - t_{\gamma})/s_1 \\
(t_2 - t_1)/s_2 \\
(t_3 - t_2)/s_3 \\
\vdots \\
(t_{\gamma} - t_{\gamma-1})/s_{\gamma} 
\end{array} \right].
\]

**Def. 3.4:** The trivial period of \((r_1, \ldots, r_{\gamma})\) is the least integer \( \gamma^* > 0 \) such that \((r_1, \ldots, r_{\gamma}) = (r_{\gamma^*+1}, \ldots, r_{\gamma}, r_1, \ldots, r_{\gamma^*})\).

**Lemma 3.5:** Suppose \( \gamma^* \) is the trivial period of the difference vector of \( \tilde{t} = (t_1, \ldots, t_{\gamma}) \in \mathbb{D}(a) \) with respect to \( a \).

Then \( \gamma/\gamma^* \) and \( a^* = a \cdot \gamma^*/\gamma \) are integers. Moreover,

\[
\Lambda(a)^\beta(\tilde{t}) = \tilde{t} \iff \beta = 0 \mod a^*.
\]

We write \( \gamma^* = \gamma^*(a, \tilde{t}) \) and \( a^* = a^*(a, \tilde{t}) \).

**Proof:** We denote the difference vector of \( \tilde{t} \) with respect to \( a \) by

\[
(r_1, \ldots, r_{\gamma}) = (a + t_1 - t_{\gamma}, t_2 - t_1, \ldots, t_{\gamma} - t_{\gamma-1}).
\]

We get

\[
\sum_{j=1}^{\gamma} r_j = (a + t_1 - t_{\gamma}) + (t_2 - t_1) + \cdots + (t_{\gamma} - t_{\gamma-1}) = \alpha.
\]

By the hypothesis \( \gamma = s\gamma^* \) for an integer \( s \) and

\[
r_1 + \cdots + r_{\gamma^*} = r_{\gamma^*+1} + \cdots + r_{2\gamma^*} = \cdots = r(s-1)\gamma^*+1 + \cdots + r_{s\gamma^*}.
\]

Hence, \( r_1 + \cdots + r_{\gamma^*} = \alpha/s = a \cdot \gamma^*/\gamma = a^* \) is an integer.

We will now prove

\[
(3.1) \quad \begin{cases}
t_j - t_j - \gamma^* = a^* & \text{for } \gamma^* < j \leq \gamma \\
t_j - t_j - \gamma^* + \gamma = a^* - a & \text{for } 1 \leq j \leq \gamma^*.
\end{cases}
\]
If $y^* < j \leq \gamma$, then
\[ t_j - t_{j - \gamma} = \sum_{i=1}^{\gamma} (t_{j - \gamma + i} - t_{j - \gamma + i - 1}) = \sum_{i=1}^{\gamma} t_{j - \gamma + i} = \alpha^*. \]

If $1 \leq j \leq \gamma^*$, then
\[ t_j - t_{j - \gamma^* + \gamma^* + \alpha} = \sum_{i=1}^{\gamma^* - j} (t_{j - \gamma^* + \gamma^* + i} - t_{j - \gamma^* + \gamma^* + i - 1}) + (t_1 - t_{\gamma^* + \alpha}) \]
\[ + \sum_{i=2}^{\gamma^*} (t_i - t_{i - 1}) = r_{\gamma - \gamma^* + j + 1} + \ldots + r_1 r_1 + \ldots + r_j = \alpha^*, \]

and the proof of (3.1) is complete.

Next, we compute $\Lambda(a)^{\alpha^*}(\xi)$. Since $t_1 > 0$ and by using (3.1) we get
\[ t_{\gamma^*} = t_{\gamma} + \alpha^* - a \leq \alpha^* \quad \text{and} \quad t_{\gamma^* + 1} = t_{1 + \alpha^*} > \alpha^*. \]

Hence, by definition
\[ \Lambda(a)^{\alpha^*}(\xi) = (t_{\gamma^* + 1 - \alpha^*}, \ldots, t_{\gamma} - \alpha^*, t_{1 + \alpha^*}, \ldots, t_{\gamma^* + \alpha - \alpha^*}). \]

By using (3.1) we get $\Lambda(a)^{\alpha^*}(\xi) = \xi$.

Finally, we will prove that $\Lambda(a)^{\beta}(\xi) = \xi$ implies $\beta = 0$ modulo $\alpha^*$. It is sufficient to prove that $0 \leq \beta \leq \alpha^*$ implies $\beta = 0$ or $\beta = \alpha^*$. Let $i$ be the maximal $i$ such that $t_i \leq \beta$. By definition
\[ \Lambda(a)^{\beta}(\xi) = (t_{i+1} - \beta, \ldots, t_{\gamma} - \beta, t_{1 + \alpha - \beta}, \ldots, t_1 + \alpha - \beta). \]

Hence,
\[ (3.3) \quad \text{the difference vector of } \Lambda(a)^{\beta}(\xi) \text{ with respect to } \alpha \text{ is } (r_{i+1}, \ldots, r_{\gamma}, r_1, \ldots, r_1). \]

Hence, $(r_1, \ldots, r_\gamma) = (r_{i+1}, \ldots, r_{\gamma}, r_1, \ldots, r_1)$. By the hypothesis $i = 0$ or $i = \gamma^*$. If $i = \gamma^*$, we get by (3.1) that $t_{\gamma^* + 1 - \beta} = t_1 = t_{\gamma^* + 1 - \alpha^*}$. If $i = 0$, then $t_1 - \beta = t_1$. Hence, $\beta = \alpha^*$ or $\beta = 0$.

Q.E.D.
Lemma 3.6: Suppose $\gamma^*$ is the trivial period of the difference vector of $\vec{t} = [\frac{t_1}{s_1}, ..., \frac{t_y}{s_y}] \in \mathcal{D}(a,m)$ with respect to $a$.

Then $\gamma/\gamma^*$, $a^* = a \cdot (\gamma^*/\gamma)$ and $m \cdot (\gamma^*/\gamma)$ are integers,

Moreover,

$$\Lambda(a,m)^\beta(\vec{t}) = \vec{t} \iff \beta = 0 \mod \gamma^*.$$

We write $\gamma^* = \gamma^*(a,\vec{t})$ and $a^* = a^*(a,\vec{t})$.

Proof: As in the proof of Lemma 3.5 we prove that $\gamma/\gamma^*$, $a^* = (\gamma^*/\gamma) \cdot a$ and $(\gamma^*/\gamma) \cdot m$ are integers. Moreover, (3.1) is true and $s_j = s_1$ when $j = i \mod \gamma^*$.

By induction

$$\Lambda(a,m)^i(\vec{t}) = \left[ \left( \frac{t_{i+1} - (s_i + t_i)}{s_{i+1}}, \frac{t_{i+2} - (s_i + t_i)}{s_{i+2}} \right), ..., \right] \text{ for } i=1, ..., \gamma^*.$$ 

By (3.1) and since $\gamma^* = \gamma \mod \gamma^*$, we get

$s_{\gamma^*} + t_{\gamma^*} = s_{\gamma^*} + (t_{\gamma^*} + a^* - a)$. By the definition of $\mathcal{D}(a,m)$ we have

$s_{\gamma} + t_{\gamma} = a$. Hence, $s_{\gamma^*} + t_{\gamma^*} = a^*$. Therefore,

$$\Lambda(a,m)^{\gamma^*}(\vec{t}) = \left[ \left( \frac{t_{\gamma+1} - a^*}{s_{\gamma^* + 1}}, ..., \left( \frac{t_{\gamma} - a^*}{s_{\gamma}}, \left( \frac{t_{1} + a - a^*}{s_{1}}, ..., \left( \frac{t_{\gamma^*} + a - a^*}{s_{\gamma^*}} \right) \right) \right) \right].$$

By (3.1) we get $\Lambda(a,m)^{\gamma^*}(\vec{t}) = \vec{t}$.

Suppose $\Lambda(a,m)^j(\vec{t}) = \vec{t}$. It is sufficient to prove that $0 \leq j \leq \gamma^*$ implies $j = 0$ or $j = \gamma^*$. By definition there exists an integer $a \geq 0$ such that

$$\Lambda(a,m)^j(\vec{t}) = \left[ \left( \frac{t_j + a}{s_{j+1}}, ..., \left( \frac{t_{\gamma} - a}{s_{\gamma}}, \left( \frac{t_{1} + a - a}{s_{1}}, ..., \left( \frac{t_{j} + a - a}{s_{j}} \right) \right) \right) \right].$$

If $[\frac{r_1}{s_1}, ..., \frac{r_{\gamma}}{s_{\gamma}}]$ is the difference vector of $\vec{t}$, then
\[
\begin{bmatrix}
(X_{i+1}^{j+1}), \ldots, (X_{1}^{j+1}), (X_{1}^{j}), \ldots, (X_{1}^{j})
\end{bmatrix}
\]
is the difference vector of 
\(\Lambda(\alpha, m)^{j}(\xi)\). By the hypothesis, \(j = 0\) or \(j = \gamma^{*}\).

Q.E.D.

Later we will also need the following definition and lemmas.

**Def. 3.7:** Suppose \(\xi = (t_{1}, \ldots, t_{\gamma}) \in \mathbb{D}(\alpha)\) and \(0 \leq \beta \leq \alpha\). If 
\(t_{1} > \beta\), we define \(r(\beta, \xi) = 0\). Otherwise \(r(\beta, \xi)\) is the maximal integer \(r\) such that 
\(t_{r} \leq \beta\).

**Lemma 3.8:** Suppose \(\xi \in \mathbb{D}(\alpha)\) and \(\alpha^{*} = \alpha^{*}(\alpha, \xi)\) and \(\gamma^{*} = \gamma^{*}(\alpha, \xi)\). Suppose 
\(0 \leq \beta_{i} \leq \alpha\) and \(\beta_{0} + \cdots + \beta_{s-1} = X \cdot \alpha^{*}\). Then 
\[\begin{align*}
 r(\beta_{0}, \xi) + \sum_{i=1}^{s-1} r(\beta_{i}, \Lambda(\alpha) \beta_{0} + \cdots + \beta_{i-1}(\xi)) = X \cdot \gamma^{*}.
\end{align*}\]

**Proof:** Suppose \(0 \leq \beta_{0} + \beta_{1} \leq \alpha\). We observe that
\((3.5)\) \(r(\beta_{0} + \beta_{1}, \xi) = r(\beta_{0}, \xi) + r(\beta_{1}, \Lambda(\alpha) \beta_{0}(\xi))\).

\((3.2)\) in the proof of Lemma 3.5 implies \(r(\alpha^{*}, \xi) = \gamma^{*}\). Hence, the case \(X = 1\) follows from \((3.5)\).

If \(X > 1\), we choose \(q\) such that \(\beta_{0} + \cdots + \beta_{q-1} < \alpha^{*}\) and \(\beta_{0} + \cdots + \beta_{q} > \alpha^{*}\). We choose \(\beta'\) and \(\beta''\) such that \(\beta' + \beta'' = \beta_{q}\) and \(\beta_{0} + \cdots + \beta_{q-1} + \beta' = \alpha^{*}\). The claim follows by induction with respect to \(X\) by studying \(\beta_{0} + \cdots + \beta_{q-1} + \beta' + \beta'' + \beta_{q+1} + \cdots + \beta_{s-1}\).

Q.E.D.

**Lemma 3.9:** Suppose \(\xi \in \mathbb{D}(\alpha, m)\) and \(\alpha^{*} = \alpha^{*}(\alpha, \xi)\) and 
\(\gamma^{*} = \gamma^{*}(\alpha, \xi)\). We denote 
\[\Lambda(\alpha, m)^{i}(\xi) = \left[\begin{bmatrix}
(t_{1}^{i}), \ldots, (t_{1}^{i})
\end{bmatrix}, \ldots, \left[\begin{bmatrix}
(t_{1}^{i})
\end{bmatrix}
\right]\right].\] Then 
\[\sum_{i=0}^{X \cdot \gamma^{*} - 1} (t_{1}^{i} + s_{1}^{i}) = X \cdot \alpha^{*} .\]
Proof: By (3.4) and we get
\[ \gamma \sum_{i=0}^{\gamma-1} (t_i^1 + s_i^1) = \gamma \sum_{i=1}^{\gamma-1} [(t_i^1 + s_i^1) + (t_{i+1}^1 + s_{i+1}^1)] = t_{\gamma-1}^1 + s_{\gamma-1}^1 = a \]

The last equality is proved in the proof of Lemma 3.6.

Q.E.D.

Finally, we do the following observation.

Observation 3.10: If \( t \in \mathbb{D}(a) \), then the trivial periods of the difference vectors of \( t \) and \( \Lambda(a)^{(i)}(t) \) are equal.

If \( t \in \mathbb{D}(a,m) \), then the trivial periods of the difference vectors of \( t \) and \( \Lambda(a,m)^{(i)}(t) \) are equal.

This observation follows from (3.4) and the proof of Lemma 3.6.

4. Computation of \( \psi \).

We will in Section 4 - 7 study the set \( \mathcal{M} \subset \{0,1\}^n \) defined by

\[ A \in \mathcal{M} \iff \begin{cases} A \text{ ends with a } (p+1)\text{-block}. \\ A \text{ starts with } 0 \text{ or a } (p+1)\text{-block}. \\ w(A) = k+p+1. \end{cases} \]

By lemma 4.11 and 4.13 in [2] there exists an \( i > 0 \) such that \( \theta^i(A) \in \mathcal{M} \) for all \( A \in \mathcal{M} \). We define \( \text{Index}: \mathcal{M} \to \{1,2,\ldots\} \) and \( \psi: \mathcal{M} \to \mathcal{M} \) in the following way:

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

In [2] we denoted \( \psi \) by \( \psi_{\min} \). If \( A \in \mathcal{M} \) contains 1 \( (p+1)\text{-block} \), we also denoted \( \psi \) by \( \Phi \) in [2]. We get the following lemma:
Lemma 4.1: If $A \in \mathcal{M}$ and $q$ is the least integer $q > 0$ such that $\psi^q(A) = A$, then $\text{Index}(A) + \ldots + \text{Index}(\psi^{q-1}(A))$ is the minimal period of $A$ with respect to $\emptyset$.

First we will reformulate how $\psi$ works. Lemma 4.2 and 4.3 are reformulations of Lemma 4.11 and 4.13 in [2] respectively.

We define

\[
\begin{align*}
\gamma_i(A) &= \text{the number of } i\text{-blocks in } A, \\
\alpha_i(A) &= n + i - \sum_{j=1}^{i} 2j \cdot \gamma_j(A) - 2i \cdot \sum_{j=i+1}^{p+1} \gamma_j(A). 
\end{align*}
\]

Moreover, $D_i(A)$ is defined in Def. 3.2.

Lemma 4.2: Suppose $A \in \mathcal{M}$ contains a $(p+1)$-block. We let $\alpha_i = \alpha_i(A)$ for $i = 1, \ldots, p+1$. We define $r_q = r_q(A)$ and $\beta_q = \beta_q(A)$ inductively for $q = 1, \ldots, p$ by the formulae:

\[
\begin{align*}
\beta_1 &= 1, \\
\beta_q &= (p+1-q) + \sum_{i=q+1}^{p} 2 \cdot (i-q) \cdot r_i \\
r_q &= \text{the number of } q\text{-blocks } B \text{ in } A \text{ such that } d(B) \leq \beta_q \text{ and } r_q = r(\beta_q, D_q(A)).
\end{align*}
\]

Then $D_{p+1}(\psi(A)) = D_{p+1}(A)$. If $\gamma_i(A) \neq 0$ and $1 \leq i \leq p$, then $D_i(A) \in \bigcup \left( \alpha_i \right)$ and $D_i(\psi(A)) = \bigwedge (\alpha_i)^{\beta_i}(D_i(A))$.

Moreover,

\[
\text{Index}(A) = n + p + 1 + \sum_{i=1}^{p} 2 \cdot i \cdot r_i \leq 2n.
\]

Proof: By Lemma 4.1 c) in [2] we have $D_i(A) \in \bigcup (\alpha_i)$ for $i = 1, \ldots, p$. $\phi(A)$ in Lemma 4.11 in [2] is equal to $\psi(A)$. By Lemma 4.11 b) and d)
in [2] \( \beta_q = \chi_q(A) \) and \( r_q \) is identical with the \( r_q \) in Lemma 4.11 in [2]. Then it is not difficult to see that this lemma is a reformulation of Lemma 4.11 in [2].

Q.E.D.

**Lemma 4.3:** Suppose \( A \in \mathcal{M} \) contains more than 1 \((p+1)\)-block. Let \( m = m_A = \Sigma \{m(B) - (p+1) \mid B \) is a \((p+1)\) - block in \( A \} \).

Suppose \( B_\Gamma \) is the first \((p+1)\)-block in \( A \).

Moreover, \( \alpha_i = \alpha_i(A) \) for \( i = 1, \ldots, p+1 \).

We define \( \beta_q = \beta_q(A) \) \((q=1, \ldots, p)\) and \( \beta_q = \beta_q(A) \) \((q=1, \ldots, p)\)

inductively by the formulae

\[
\beta_{p+1} = 1 ,
\]

\[
\beta_q = \left[ d(B_\Gamma) + m(B_\Gamma) - (p+1) \right] + \sum_{i=q+1}^{p+1} 2 \cdot (i-q) \cdot r_i ,
\]

and for \( q = 1, \ldots, p \):

\[
\beta_q = \text{the number of } q\text{-blocks } B \text{ in } A
\]

such that \( d(B) \leq \beta_q \) \((r_q = r(\beta_q, d_q(A))))\).

Then we have

\[
D_{p+1}(A) \in \mathcal{D}(\alpha_{p+1}, m) \text{ and } D_{p+1}(\psi(A)) = \Lambda(\alpha_{p+1}, m)(D_{p+1}(A)) .
\]

If \( \gamma_i(A) \neq 0 \) and \( 1 \leq i \leq p \), then we have \( D_i(A) \in \mathcal{D}(\alpha_i) \) and

\[
D_i(\psi(A)) = \Lambda(\alpha_i)^{\beta_i}(D_i(A)) .
\]

Moreover,

\[
\text{Index } (A) = \left[ d(B_\Gamma) + m(B_\Gamma) - (p+1) \right] + \sum_{i=1}^{p+1} 2i \cdot r_i \leq n .
\]

**Proof:** By Lemma 4.1 c) in [2] we have \( D_i(A) \in \mathcal{D}(\alpha_i) \) for \( i = 1, \ldots, p \)

and \( D_{p+1}(A) \in \mathcal{D}(\alpha_{p+1}, m) \).

\( \varphi_{\text{min}}(A) \) in Lemma 4.13 in [2] is equal to \( \psi(A) \). It is easy to see that this lemma follows from Lemma 4.13 in [2].

Q.E.D.
In the forthcoming proof we represent the elements of $\mathcal{M}$ by

$$\pi(A) = D_1(A) \times \cdots \times D_{p+1}(A).$$

It is easy to define $\psi_\pi$ and $\text{Index}_\pi$ on $\pi(\mathcal{M})$ such that $\psi_\pi \circ \pi = \pi \circ \psi$ and $\text{Index}_\pi \circ \pi = \pi \circ \text{Index}$, and study $\psi_\pi$ and $\text{Index}_\pi$ instead of $\psi$ and $\text{Index}$. By using $\text{Index}_\pi$ and $\psi_\pi$ the structure of the proof would be somewhat clearer. But to avoid complicated notation we do not do so.

In the next section we will calculate $\psi_i(A)$ for certain $i$. In these calculations we need the following lemma.

First we need a definition

\begin{equation}
\beta_q^S(A) = \beta_q(A) + \beta_q(\psi(A)) + \cdots + \beta_q(\psi^{S-1}(A)).
\end{equation}

**Def. 4.4:** For each $A \in \mathcal{M}$ we define $\gamma_i^*(A) = \gamma^*(\alpha_i(A), D_1(A))$ and $\alpha_i^*(A) = \alpha^*(\alpha_i(A), D_1(A))$.

**Lemma 4.5:** We suppose $A \in \mathcal{M}$. Let $\gamma_i = \gamma_i(A)$, $\gamma_i^* = \gamma^*(A)$ and $\alpha_i^* = \alpha_i^*(A)$. Moreover, we suppose

for $t \in \{q+1, \cdots, p\}$:

$$\beta_t^Y(A) = X_t \cdot \alpha_t^* \quad \text{if} \quad \gamma_t \neq 0.$$  

$$X_t = 0 \quad \text{if} \quad \gamma_t = 0.$$  

a) If $\gamma_{p+1} = 1$, then

$$\beta_q^Y(A) = Y(p+1-q) + \sum_{t=q+1}^p 2 \cdot (t-q) \cdot X_t \cdot \gamma_t^e.$$  

b) If $\gamma_{p+1} > 1$ and $Y = X_{p+1} \cdot \gamma_{p+1}^*$, then

$$\beta_q^Y(A) = X_{p+1} \cdot \alpha_{p+1}^* + \sum_{t=q+1}^{p+1} 2 \cdot (t-q) \cdot X_t \cdot \gamma_t^e.$$  

**Proof:** Suppose $\gamma_t \neq 0$. We write $\beta_{t,s} = \beta_t(\psi^s(A))$. By
Lemma 4.2 and 4.3 we get

\[(4.3) \quad D_t(\psi^S(A)) = \Lambda(\alpha_t) \beta_{t,0}^{s-1}(D_t(A)) .\]

By the hypothesis

\[(4.4) \quad \beta_{t,0}^{s-1}(D_t, Y-1) = X_t \cdot \alpha^* .\]

We have \( D_t(A) \in \sum(\sigma_t) , \, \alpha^*_t = \alpha^*(\alpha_t, D_t(A)) \) and \( \gamma^*_t = \gamma^*(\alpha_t, D_t(A)) \). Hence, by (4.3), (4.4) and Lemma 3.8 we get

\[(4.5) \quad \sum_{s=0}^{Y-1} r_t(\psi^S(A)) = \sum_{s=0}^{Y-1} r(\beta_{t,s}, D_t(\psi^S(A)) = X_t \cdot \gamma^* .\]

The proof of a): By Lemma 4.2 and (4.5) we get

\[
\beta^*_{q}(A) = \sum_{s=0}^{Y-1} \beta^*_{q}(\psi^S(A)) = \sum_{s=0}^{Y-1} r(\beta_{t,s}, D_t(\psi^S(A)) = X_t \cdot \gamma^* .
\]

\[
\quad = Y(p+1-q) + \sum_{t=q+1}^{p} 2(t-q) \cdot X_t \cdot \gamma^* .
\]

The proof of b): By Lemma 4.3 we get

\[(4.6) \quad r_{p+1}(\psi^j(A)) = 1 \text{ for all } j .\]

We write

\[
D_{p+1}(\psi^j(A)) = [(t^j_s), \cdots] .
\]

(If \( B^j_F \) is the first \((p+1)\)-block in \( \psi^j(A) \), then
\[
t^j_1 = d(B^j_F) \text{ and } s^j_1 = m(B^j_F) - (p+1) .\)

Since \( Y = X_{p+1}^{\gamma^*} \) we have by Lemma 3.9

\[
(4.7) \quad \sum_{j=0}^{Y-1} (t^j_s + s^j_1) = X_{p+1}^{\alpha^*} .
\]
By (4.5), (4.6), (4.7) and Lemma 4.3 we get

\[ \beta_q^Y(A) = \sum_{j=0}^{Y-1} \beta_q^j(A) \]

\[ = \sum_{j=0}^{Y-1} \left[ \sum_{t=1}^{p+1} s_j + \sum_{t=q+1}^{2(t-q) \cdot \tau(t)} \sum_{t=q+1}^{2(p+1-q) \cdot \tau(t)} \right] \]

\[ = \alpha_{p+1}^* \cdot X_{p+1} + \sum_{t=q+1}^{2(p+1-q) \cdot \tau(t)} X_t y_t^* + 2(p+1-q) \cdot Y. \]

Since \( Y = X_{p+1} y_{p+1}^* \) the proof is complete.

\[ \text{Q.E.D.} \]

5. How to determine the minimal period.

We will now determine the minimal periods of \( A \in \mathcal{M} \). \( \gamma_i(A) \) and \( a_i(A) \) are defined in (4.1). \( D_i(A) \) is defined in Def. 3.2.

Moreover, \( \gamma_i^*(A) \) and \( a_i^*(A) \) are defined in Def. 4.4 and \( \mathcal{M} \) is defined in Section 4. We repeat the definitions of \( \gamma_i^*(A) \) and \( a_i^*(A) \): Suppose first \( 1 \leq i \leq p \) and \( D_i(A) = (t_1, \ldots, t_\gamma_i) \).

Then \( \gamma_i^*(A) \) is the trivial period of

\( (t_1 - t_\gamma_i + a_i(A), t_2 - t_1, t_3 - t_2, \ldots, t_\gamma_i - t_1). \)

Next we suppose \( D_{p+1}(A) = \left[ \begin{array}{c} t_1 \\ \cdot \cdot \cdot \\ t_{p+1} \end{array} \right] \). Let

\( t' = t_1 - t_{p+1} + a_{p+1}(A) \) and \( t'' = t_{p+1} - t_{p+1} - 1 \). Then \( \gamma_{p+1}(A) \) is the trivial period of

\[ \left[ \begin{array}{c} t' \\ \cdot \cdot \cdot \\ t'' \end{array} \right]. \]

Moreover, \( a_i^*(A) = a_i(A) \cdot (\gamma_i^*(A)/\gamma_i(A)) \) for \( i = 1, \ldots, p+1 \).
Theorem 5.1: Suppose $A \in \mathbb{M}$. We let $\gamma_i = \gamma_i(A)$, $\alpha_i = \alpha_i(A)$, $\gamma_i^* = \gamma_i^*(A)$ and $\alpha_i^* = \alpha_i^*(A)$.

If $\gamma_i = 0$ for $i = 1, \ldots, p$ we let $X_{p+1} = 1$ and $X_1 = \ldots = X_p = 0$. Otherwise, we define equation (q) by

$$\begin{cases} \alpha_i^* X_q = \alpha_i^* X_{p+1} + \sum_{i=q+1}^{p+1} 2(i-q) \gamma_i X_i \gamma_i^* & \text{if } \gamma_q \neq 0 \\ X_q = 0 & \text{if } \gamma_q = 0 \end{cases} \quad \text{for } q = 1, \ldots, p.$$ 

Moreover, we let $X_1, \ldots, X_{p+1}$ be the least positive integral solution of the equations (1), \ldots, (p).

Then $X_{p+1} \alpha_i^* + \sum_{i=1}^{p+1} 2i \gamma_i \gamma_i^* X_i$ is the minimal period of $A$ with respect to the shift register $(x_1, \ldots, x_n) \rightarrow (x_2, \ldots, x_{n+1})$ where

$$X_{n+1} = x_1 + (E_1 + \ldots + E_{k+p})(x_2, \ldots, x_n).$$

If $\gamma_i = 0$ for $i = 1, \ldots, p$, we observe that the minimal period is

$$X_{p+1} \alpha_i^* + 2(p+1) \gamma_i X_{p+1} = \alpha_i^* + 2(p+1) \gamma_i^*$$

$$= \frac{\gamma_{p+1}(\alpha_i^* - 2(p+1) \gamma_i^*)}{\gamma_{p+1}} = \frac{\gamma_{p+1}(n+p+1)}{\gamma_{p+1}}.$$

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

Proof: $\beta_{\gamma_i}^{Y}(A)$ is defined in (4.2). We suppose first that $\gamma_{p+1} > 1$. If $\gamma_i \neq 0$ and $i \leq p$, then Lemma 4.3 and 3.5 imply

$$D_i(Y(A)) = D_i(A) \iff A(\alpha_i) = \beta_i^Y(A) \quad \text{(5.1)}$$

$$\iff \beta_i^Y(A) = X_i \cdot \alpha_i^* \quad \text{for some } X_i.$$
Moreover, Lemma 4.3 and 3.6 imply (m = m_A is defined in Lemma 4.3)

\[
\begin{align*}
D_{p+1}(\psi^Y(A)) &= D_{p+1}(A) \\
\L(A_{p+1}; m)^Y(D_{p+1}(A)) &= D_{p+1}(A) \\
\iff Y &= X_{p+1} \cdot \gamma^* 
\end{align*}
\]

for some \( X_{p+1} \).

By Lemma 4.1 in [2] \( A \) is uniquely determined by \( D_i(A) \) \((i = 1, \ldots, p+1)\). Hence, by (5.1) and (5.2) we get

\[
(5.3) \quad \psi^Y(A) = A \iff \left\{ \begin{array}{l}
\beta^Y_1(A) = X_1 \cdot \alpha^*_1 \text{ when } \gamma_1 \neq 0 \quad (i=1, \ldots, p) \\
Y = X_{p+1} \cdot \gamma^* 
\end{array} \right.
\]

We suppose \( \gamma_i \neq 0 \) for at least one \( i < p+1 \). First we will prove

\[
(5.4) \quad \{ Y : \psi^Y(A) = A \} = \{ X_{p+1} \cdot \gamma^* : X_1, \ldots, X_{p+1} \text{ is a solution of the equations } (1), \ldots, (p) \}.
\]

Suppose \( \psi^Y(A) = A \). By (5.3) there exist \( X_1, \ldots, X_{p+1} \) such that

\[
Y = X_{p+1} \cdot \gamma^* \text{ and } \beta^Y_1(A) = X_1 \cdot \alpha^*_1 \text{ when } \gamma_1 \neq 0 \text{ and } i < p.
\]

If \( \gamma_i = 0 \), we put \( X_i = 0 \). We suppose the equations

\((q+1), \ldots, (p)\) are satisfied. We suppose \( \gamma_q \neq 0 \). By Lemma 4.5 b)

\[
\beta^Y_q(A) = X_{p+1} \cdot \gamma^*_q + \sum_{t=q}^{p+1} 2 \cdot (t-q) \cdot X_t \cdot \gamma^*_t.
\]

Since \( \beta^Y_q(A) = X_q \cdot \gamma_q^* \), the equation (q) is satisfied. Hence,

\[
Y = X_{p+1} \cdot \gamma^*_p \text{ and } X_1, \ldots, X_{p+1} \text{ satisfy the equations.}
\]

Next we suppose \( Y = X_{p+1} \cdot \gamma^*_p \) and that \( X_1, \ldots, X_{p+1} \) satisfy the equations. We prove by induction

\[
(5.5) \quad \beta^Y_i(A) = X_i \cdot \alpha^*_i \text{ for } 1 \leq i \leq p \text{ and } \gamma_i \neq 0.
\]

We suppose (5.5) is true for \( i = q+1, \ldots, p \) and \( \gamma_q \neq 0 \).
By Lemma 4.5 b) and the equation (q)

$$\beta_q^y(A) = x_{p+1}^{a_p} + \sum_{t=q+1}^{p+1} 2 \cdot (t-q) \cdot y_t^* \cdot x_t = x_q^{a_q^*}.$$  

Hence, the proof of (5.5) is complete. By (5.3) we get $\psi^y(A) = A$.

Suppose $x_1, \ldots, x_{p+1}$ is the least solution of the equations (1), \ldots, (p). By (5.4)

$y = x_{p+1}^* y_{p+1}^*$ is the least $y$ such that $\psi^y(A) = A$. By Lemma 4.1 the following sum is the least period of $A$:

$$(5.6) \quad J(Y) = \sum_{j=0}^{Y-1} \text{Index}(\psi^j(A)).$$

We will now calculate this sum. We suppose $B_j^i$ is the first $(p+1)$-block in $\psi^j(A)$.

By (4.7) in the proof of Lemma 4.5 we get

$$(5.7) \quad \sum_{j=0}^{Y-1} (d(B_j^i) + m(B_j^i) - (p+1)) = x_{p+1}^{a_{p+1}^*}.$$

By Lemma 4.3, (5.7) and (4.5) (in the proof of Lemma 4.5) we get

$$J(Y) = \sum_{j=0}^{Y-1} (d(B_j^i) + m(B_j^i) - (p+1)) + \sum_{i=1}^{p+1} 2 \cdot \sum_{i=1}^{p+1} i \cdot y_i^* \cdot x_i = x_{p+1}^{a_{p+1}^*} + X_{p+1} \cdot a_{p+1}^* + 2 \sum_{i=1}^{p+1} i \cdot y_i^* \cdot x_i.$$

Next we suppose $y_{p+1} > 1$ and $y_i = 0$ for $i = 1, \ldots, p$.

Let $x_{p+1} = 1$ and $x_1 = \ldots = x_p = 0$.

By (5.3) we get

$$(5.8) \quad y = x_{p+1}^{y_{p+1}^*} = x_{p+1}^*$$

is the least $y$ such that $\psi^y(A) = A$.

We calculate $J(Y)$ in (5.6) as before.

Now we suppose $y_{p+1} = 1$ and $y_i = 0$ for $i = 1, \ldots, p$.

It is very easy to see that the least period of $A$ is $n+p+1$.

By computation we get

$$a_{p+1}^* x_{p+1} + \sum_{i=1}^{p+1} 2 \cdot i \cdot y_i^* \cdot x_i = n+p+1,$$

where
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 \( \gamma_{p+1} > 1 \).

Lemma 4.2 and 3.5 imply that (5.1) is true. By Lemma 4.2

\[
D_{p+1}(\psi^Y(A)) = D_{p+1}(A).
\]

Hence,

\[
\psi^Y(A) = A \iff \beta_i^Y(A) = X_i \cdot \alpha_i^* \quad \text{when} \quad \gamma_i \neq 0 \quad \text{and} \quad 1 \leq i \leq p.
\]

By using Lemma 4.5 a) this is equivalent to: \( X_1, \ldots, X_p, Y \) satisfy the equations \((1)', \ldots, (p)'\) given by

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

Let \( X_1, \ldots, X_p, Y \) be the least solution of the equations \((1)', \ldots, (p)'\). Then \( Y \) is the least \( Y \) such that \( \psi^Y(A) = A \).

By Lemma 4.2 and (4.5) we calculate the minimal period of \( A \) in the following way

\[
\Sigma \text{Index}(\psi^j(A)) = \Sigma [(n+p+1) + 2 \sum_{i=1}^{i} \gamma_i \cdot X_i].
\]

The proof will be complete if we can prove the following claim:

Suppose \( X_1, \ldots, X_{p+1} \) is the least solution of the equations \((1), \ldots, (p)\).

Let \( Y = X_{p+1} \) and \( \hat{X}_t = \begin{cases} 0 & \text{if} \quad \gamma_t = 0 \\ X_t - \frac{Y_t}{Y_t^*} & \text{if} \quad \gamma_t \neq 0 \end{cases} \)

Then \( \hat{X}_1, \ldots, \hat{X}_p, Y \) is the least solution of the equations \((1)', \ldots, (p)'\), and
\[
Y(n+p+1) + \sum_{i=1}^{p+1} 2i \cdot \hat{X}_i \cdot \gamma_i = X_{p+1} a_{p+1}^* + \sum_{i=1}^{p+1} 2i \cdot \hat{X}_i \cdot \gamma_i^* .
\]

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

\[
X_{p+1} a_{p+1}^* + \sum_{i=1}^{p+1} 2i \cdot \hat{X}_i \cdot \gamma_i^* = Y(n+p+1 - \sum_{i=1}^{p+1} 2i \gamma_i)
\]

\[
+ \sum_{i=1}^{p+1} 2i \gamma_i^* (\hat{X}_i + \gamma_i) + 2(p+1) Y_{p+1} Y = Y(n+p+1) + \sum_{i=1}^{p+1} 2i \gamma_i^* \cdot \hat{X}_i .
\]

Next we prove that the following 3 equations are equivalent (we use \( a_i^* \gamma_i = a_i \)):

\[
a_i^* X_i = X_{p+1} a_{p+1}^* + \sum_{t=i+1}^{p+1} 2(t-i) \gamma_i^* X_i,
\]

\[
a_i^* \hat{X}_i + a_i Y = Ya_{p+1} + \sum_{t=i+1}^{p+1} 2(t-i) \gamma_i^* \hat{X}_i + Y \sum_{t=i+1}^{p+1} 2(t-i) \gamma_i,
\]

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

where \( Z = Y(-a_i + a_{p+1} + \sum_{t=i+1}^{p+1} 2(t-i) \gamma_i + i - (p+1)) \).

\( Z = 0 \) follows from the definition of \( a_{p+1} \) and \( a_i \). Hence, the proof of the claim is complete. Hence, the proof of the theorem is complete. For later use we observe:

\((5.9)\) \( X_{p+1} Y_{p+1}^* \) is the least \( Y \) such that \( \psi^Y(A) = A \).

In the case \( \gamma_{p+1} \) this follows from (5.4) and (5.8). Q.E.D.
6. The possible periods

In this section we will find the possible periods of elements in $\mathcal{M}$. First we introduce more notation.

**Def. 6.1:** a) Suppose $\mu = \gamma \times \gamma^*$ where $\gamma = (\gamma_1, \ldots, \gamma_{p+1})$ and $\gamma^* = (\gamma^*_1, \ldots, \gamma^*_{p+1})$. We define

$$a_i(\gamma) = n+i - \sum_{t=1}^{i} 2t \gamma_t - 2i \sum_{t=i+1}^{p+1} \gamma_t,$$

$$a^*_i(\mu) = \frac{\gamma^*_i}{\gamma_i} a_i(\gamma), \quad \gamma^*_i(\mu) = \gamma^*_i \text{ and } \gamma_i(\mu) = \gamma_i.$$

If $\gamma_i = 0$ for $i = 1, \ldots, p$, we let $X_{p+1}(\mu) = 1$ and $X_i(\mu) = \ldots = X_p(\mu) = 0$. Otherwise, we let $X_i(\mu), \ldots, X_{p+1}(\mu)$ be the least integral solution of the equations (1), $\ldots$, (p) in the Thm. 5.1 with $a^*_i = a^*_i(\mu)$ and $\gamma^*_i = \gamma^*_i(\mu)$.

Moreover, we let

$$MP(\mu) = X_{p+1}(\mu) a^*_{p+1}(\mu) + \sum_{i=1}^{p+1} 2i X_i(\mu) \gamma^*_i(\mu).$$

b) For each $A \in \mathcal{M}$, we define $\gamma(A) = (\gamma_1(A), \ldots, \gamma_{p+1}(A))$, $\gamma^*(A) = (\gamma^*_1(A), \ldots, \gamma^*_{p+1}(A))$ and $\mu(A) = \gamma(A) \times \gamma^*(A)$. Moreover, we let

$$\mathcal{P}_1 = \{\gamma(A) : A \in \mathcal{M}\} \text{ and } \mathcal{P}_2(\gamma) = \{\gamma^*(A) : A \in \mathcal{M} \text{ and } \gamma(A) = \gamma\}.$$ 

Theorem 6.2 follows from Theorem 5.1:

**Theorem 6.2:** The possible minimal periods of elements in $\mathcal{M}$ are

$$\{MP(\mu) : \mu \in \mathcal{P}\} \text{ where }$$

$$\mathcal{P} = \bigcup_{\gamma \in \mathcal{P}_1} \gamma \times \mathcal{P}_2(\gamma).$$

In the next theorem we construct $\mathcal{P}_1$ and $\mathcal{P}_2(\gamma)$ for each $\gamma \in \mathcal{P}_1$. 
Theorem 6.3: a) \( \gamma = (\gamma_1, \ldots, \gamma_{p+1}) \in \mathcal{D}_1 \) if and only if there exists \( m \geq 0 \) such that

\[
m + \sum_{i=1}^{p+1} i \cdot \gamma_i = k + p + 1, \quad m + 2 \sum_{i=1}^{p+1} i \cdot \gamma_i \leq n + p + 1 \quad \text{and} \quad \gamma_{p+1} \neq 0.
\]

We denote \( m \) by \( m(\gamma) \).

b) Let \( \gamma = (\gamma_1, \ldots, \gamma_{p+1}) \in \mathcal{D}_1 \). For \( i = 1, \ldots, p \) we define

\[
\Omega_i(\gamma) = \{ \frac{\gamma_i}{r} : \frac{\alpha_i(\gamma)}{r} \text{ and } \frac{m(\gamma)}{r} \text{ are integers} \}.
\]

Moreover, we let

\[
\Omega_{p+1}(\gamma) = \{ \frac{\gamma_{p+1}}{r} : \frac{\alpha_{p+1}(\gamma)}{r} \text{ and } \frac{m(\gamma)}{r} \text{ are integers} \}.
\]

Then \( \mathcal{G}_2(\gamma) = \bigcap_{i=1}^{p+1} \Omega_i(\gamma) \).

In the proof we need the following definition and lemma.

Def. 6.4: Suppose \( \gamma \in \mathcal{D}_1 \). Let \( \mathcal{M}(\gamma) = \{ A \in \mathcal{M} : (\gamma_1(A), \ldots, \gamma_{p+1}(A)) = \gamma \} \). For \( i = 1, \ldots, p \) we define

\[
\mathcal{N}_i(\gamma) = \{ (d_1, \ldots, d_{\gamma_1}) : d_1 > 0, d_i \geq 0 \ (i = 2, \ldots, \gamma_i) \text{ and } d_1 + \ldots + d_{\gamma_i} = \alpha_i(\gamma) \}.
\]

Moreover, we define

\[
\mathcal{N}_{p+1}(\gamma) = \left\{ \left[ \frac{d_1}{s_1}, \ldots, \frac{d_{p+1}}{s_{p+1}} \right] : d_1 + \ldots + d_{p+1} = \alpha_{p+1}(\gamma) - m(\gamma)
\]

\[
\text{and } s_1 + \ldots + s_{p+1} = m(\gamma), \ d_i \geq 0 \ \text{and} \ s_i \geq 0 \right\}.
\]

Lemma 6.5: a) For \( i = 1, \ldots, p \) we define \( \rho_i : (d_i(A) : A \in \mathcal{M}(\gamma)) \rightarrow \mathcal{N}_i(\gamma) \) by \( \rho_i(t_1, \ldots, t_{\gamma_i}) = (t_1 - t_{\gamma_i} + \alpha_i(\gamma), t_2 - t_1, \ldots, t_{\gamma_i} - t_{\gamma_{i-1}}) \).

Then \( \rho_i \) is surjective.
b) We define \( \rho_{p+1}: \{ D_{p+1}(A) : A \in \mathcal{M}(\gamma) \} \to \mathcal{N}_{p+1}(\gamma) \) by
\[
\rho_{p+1}((t_1, \ldots, t_{p+1})) = (d_1, \ldots, d_{p+1})
\]
where
\[
d_i = \begin{cases} 
t_i & \text{if } i = 1 \\
t_i - t_{i-1} - s_{i-1} & \text{if } i \neq 1.
\end{cases}
\]
Then \( \rho_{p+1} \) is bijective.

Proof of Lemma 6.5: a) By Lemma 4.1 c) in [2]
\[
\{ D_1(A) : A \in \mathcal{M}(\gamma) \} = \{(t_1, \ldots, t_{p+1}) : 0 < t_1 \leq t_2 \leq \ldots \leq t_{p+1} = a_1(\gamma)\}
\]
and the proof is obvious.

b) By Lemma 4.1 c) in [2]
\[
\{ D_{p+1}(A) : A \in \mathcal{M}(\gamma) \} = \left\{ \left[ \begin{array}{c} t_1 \\ s_1 \end{array} \right], \ldots, \left[ \begin{array}{c} t_{p+1} \\ s_{p+1} \end{array} \right] : 0 \leq s_i, 0 \leq t_i, \\
\sum t_i \leq 1, \sum s_i \leq 1 \right\}
\]
\[
t_i + s_i \leq t_{i+1} (i = 1, \ldots, p+1), 
\sum t_i + s_i = a_{p+1}(\gamma) \text{ and }
\sum s_i = m(\gamma) \}.
\]
We observe that \( \rho_{p+1} \) is well defined.

Let \( D = [(d_1, \ldots, d_{p+1})] \in \mathcal{N}_{p+1}(\gamma) \). There exists one and only one \( E \) such that \( \rho_{p+1}(E) = D \). This \( E \) can be constructed in the following way:

Put \( E = [(t_1, \ldots)] \) where \( t_1 = d_1, t_2 = d_2 + t_1 + s_1, t_3 = d_3 + t_2 + s_2 \) etc.

Q.E.D.

Proof of Thm. 6.3: a) follows from Lemma 4.1 c) in [2].

b) We observe \( (i = 1, \ldots, p+1) \)

(6.3) \( \{ \text{the trivial period of } E : E \in \mathcal{N}_{i}(\gamma) = \Omega_i(\gamma) \} \).

Moreover,

(6.4) \( \gamma_i^*(A) \) is the trivial period of \( \rho_i(D_i(A)) \).
For \( i = 1, \ldots, p \) (6.4) follows directly from the definition.

Next we let \( i = p+1 \) and \( D_{p+1}(A) = [(t^1_s), \ldots, (t^{y_{p+1}}_s)] \). By definition \( \gamma^*_p(A) \) is the trivial period of \( [(d^1_s), \ldots] \)

where

\[
d'_i = \begin{cases} 
  t_1 - t_{y_{p+1}} + a_{p+1}(\gamma) & \text{if } i = 1 \\
  t_i - t_{i-1} & \text{if } i \neq 1.
\end{cases}
\]

We denote \( \rho_{p+1}(D_{p+1}(A)) = [(d^1_s), \ldots] \). Since \( s_{y_{p+1}} + t_{y_{p+1}} = a_{p+1}(\gamma) \)
(by Lemma 4.1 in [2]), we have \( d_i = d'_i - s_{i-1} \), for \( i = 1, \ldots, p+1 \) \( (s_0 = s_{y_{p+1}}) \)

Hence, \( \gamma^*_p(A) \) is the trivial period of \( \rho_{p+1}(D_{p+1}(A)) \).

Lemma 6.5, (6.3) and (6.4) imply

(6.5) \( \{\gamma^*_i(A) : A \in \mathbb{M}(\gamma)\} = \Omega_i(\gamma) \)

By Lemma 4.1 c) in [2]

(6.6) \( \{D_1(A), \ldots, D_{p+1}(A) : A \in \mathbb{M}(\gamma)\} = \bigvee_{i=1}^{p+1} \{D_i(A) : A \in \mathbb{M}(\gamma)\} \).

(6.5) and (6.6) imply that b) is true. Q.E.D.

7. The number of cycles

In this section we will count the number of cycles in

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

where \( \mathbb{M} \) is defined in Section 4. First we do the following observation.

**Observation 7.1:** Suppose \( \mathcal{C} \) is a cycle in \( \bar{\mathbb{M}} \). If \( A, B \in \mathcal{C} \cap \mathbb{M} \), then \( \mu(A) = \mu(B) \).

**Proof:** There exists \( i \) such that \( \psi^i(A) = B \). By Obs. 3.10, Lemma 4.2 and 4.3 the observation follows. Q.E.D.
Next we let

\[(7.1) \quad G(\mu) = \text{the number of cycles } \mathcal{C} \text{ in } \mathcal{M},\]

such that \( A \in \mathcal{C} \cap \mathcal{M} \Rightarrow \mu(A) = \mu. \)

**Theorem 7.2:** For each \( \mu \in \mathcal{P} \) we let \( \gamma_1(\mu), \alpha_1^*(\mu), \gamma_1^*(\mu), \chi_1(\mu), \)
\( MP(\mu) \) and \( m(\mu) \) be as in Section 6. Moreover, we let
\( m^*(\mu) = m(\mu) \cdot \frac{\gamma_{p+1}^*(\mu)}{\gamma_{p+1}(\mu)}. \)

a) The number of cycles in \( \mathcal{M} = \Sigma\{G(\mu); \mu \in \mathcal{P}\}. \)

b) The number of cycles in \( \mathcal{M} \) of length \( MP = \Sigma\{G(\mu); \mu \in \mathcal{P} \text{ and } MP(\mu) = MP\}. \)

c) We let \( \sigma(r,s,t) = \text{the number of elements in} \)
\( \mathcal{R}(r,s,t) = \{(d_1, \ldots, d_s): d_i \geq 0, d_1 = r, d_1 + \ldots + d_s = t \text{ and} \)
\( (d_1, \ldots, d_s) \text{ has trivial period } s \}. \)

Then \( \sigma(r,s,t) \) can be calculated inductively by the following formula:
\[\sigma(r,s,t) = \binom{t+s-r-2}{s-2} - \Sigma\{\sigma(r,\frac{s}{s'},\frac{t}{s'}); \frac{s}{s'} \text{ and } \frac{t}{s'} \text{ are integers}\}. \]

( ) is the binomial coefficient.

d) We let \( \sigma(s,t) = \text{the number of elements in} \)
\( \mathcal{R}(s,t) = \{(d_1, \ldots, d_s): d_i \geq 0, d_1 + \ldots + d_s = t \text{ and} \)
\( (d_1, \ldots, d_s) \text{ has trivial period } s \}. \)

Then \( \sigma(s,t) \) can be calculated inductively by the following formula:
\[\sigma(s,t) = \binom{t+s-1}{s-1} - \Sigma\{\sigma(\frac{s}{s'},\frac{t}{s'}); \frac{s}{s'} \text{ and } \frac{t}{s'} \text{ are integers}\}. \]

\[e) \quad G(\mu) = \left( \prod_{i=1}^{p+1} w_i(\mu) \right) (X_{p+1}(\mu) \gamma_{p+1}^*(\mu))^{-1} \]
where (we write $\alpha^*_i = \alpha^*_i(\mu)$, $\gamma^*_i = \gamma^*_i(\mu)$ and $m^* = m^*(\mu)$)

\[
\alpha^*_i
w_i(\mu) = \sum_{t=1}^T t \cdot \sigma(t, \gamma^*_i, \alpha^*_i) \quad \text{for } i = 1, \ldots, p
\]

and

\[
w_{p+1}(\mu) = \sigma(\gamma^*_{p+1}, \alpha^*_{p+1} - m^*) \cdot \left( \frac{m^* + \gamma^*_{p+1} - 1}{\gamma^*_{p+1} - 1} \right)
+ \left( \frac{\alpha^*_{p+1} - m^* + \gamma^*_{p+1} - 1}{\gamma^*_{p+1} - 1} \right) \cdot \sigma(\gamma^*_{p+1}, m^*) - \sigma(\gamma^*_{p+1}, \alpha^*_{p+1} - m^*) \cdot \sigma(\gamma^*_{p+1}, m^*).
\]

**Proof:** In the proof we let $\# \text{ denote } "the number of elements in"$. 

a) and b) follows from Thm. 6.2 and Obs. 7.1.

c) $\{(d_1, \ldots, d_s): d_i \geq 0, d_1 = r \text{ and } d_1 + \ldots + d_s = t\}^{\#}$

$= \{(d_2, \ldots, d_s): d_i \geq 0 \text{ and } d_2 + \ldots + d_s = t-r\}^{\#}$

$= \text{the number of ways to divide } (t-r) \text{'s into } (s-1) \text{ groups}$

$= \text{the number of ways to put } s-2 \text{ O's into } (t+s-r-2) \text{ positions}$

$= \binom{t+s-r-2}{s-2}$.

We subtract those $(d_1, \ldots, d_s)$ with trivial period less than $s$.

For each $s'$ such that $\frac{s}{s'}$ and $\frac{t}{s'}$ are integers, $(d_1, \ldots, d_s)$

$+ (d_1, \ldots, d_{s/s'})$ is a bijective correspondence between

\[
\{(d_1, \ldots, d_s): 0 \leq d_i, d_1 = r, d_1 + \ldots + d_s = t \text{ and}
\]

$(d_1, \ldots, d_s) \text{ has trivial period } \frac{s}{s'}\}
\]

and $\mathcal{P}_{s/r}(r, s/s', t/s')$.

By using these correspondences c) follows.

d) The proof of d) is analogous with the proof of c).

e) We let $\mathcal{P}_i(\gamma)$ and $\rho_i$ be as in Section 6. First we introduce some notation and observations. If $\mu = \gamma \times \gamma^*$

$(\gamma_1, \ldots, \gamma_{p+1}) \times (\gamma^*_1, \ldots, \gamma^*_{p+1})$ we let for $i = 1, \ldots, p$
\[ \mathcal{N}_i(\mu) = \{(d_1, \ldots, d_{\gamma_1}) \in \mathcal{N}_i(\gamma) : (d_1, \ldots, d_{\gamma_1}) \text{ has trivial period } \gamma_1^* \}. \]

Moreover,

\[ \mathcal{N}_{p+1}(\mu) = \{(s_1, \ldots, s_{\gamma_{p+1}}) \in \mathcal{N}_{p+1}(\gamma) \text{ with trivial period } \gamma_{p+1}^* \}. \]

By Lemma 6.5 we prove easily

\[ (7.2) \{ \rho_i : \{D_i(A) : \mu(A) = \mu \} \rightarrow \mathcal{N}_i(\mu) \text{ is surjective} \]

for \( i = 1, \ldots, p \) and bijective for \( i = p+1 \).

Suppose \( i \in \{1, \ldots, p\} \). If \( (d_1, \ldots, d_{\gamma_1}) \in \mathcal{N}_i(\mu) \), then

\[
\begin{align*}
&d_1 + \ldots + d_{\gamma_1} = d_{\gamma_1}^* + \ldots + d_{2\gamma_1}^* = \ldots = d_{(r-1)\gamma_1}^* + \ldots + d_{r\gamma_1}^* \\
&= \frac{\alpha_i(\gamma)}{r} = \frac{\gamma_1}{\gamma_{\gamma_i}} \text{ since } r = \frac{\gamma_1}{\gamma_{\gamma_i}}.
\end{align*}
\]

Specially we have

\[ (7.3) \quad d_1 \leq \frac{\alpha_i(\mu)}{\gamma_1} \text{ for } (d_1, \ldots, d_{\gamma_1}) \in \mathcal{N}_i(\mu). \]

Next we do the following observation \( i = 1, \ldots, p \):

\[ (7.4) \quad \text{To each } (d_1, \ldots, d_{\gamma_1}) \in \mathcal{N}_i(\mu) \text{ there exists exactly one element } D \in \{D_i(A) : \mu(A) = \mu\} \text{ such that } \rho_i(D) = (d_1, \ldots, d_{\gamma_1}). \]

These elements are

\[ (s, s+d_2, s+d_2+d_3, \ldots, s+ \sum_{j=2}^{\gamma_1} d_j) \text{ where } s = 1, \ldots, d_1. \]

Now we start the proof. (5.9) in the proof of Thm. 5.1 implies that for each \( A \in \mathcal{M} \) such that \( \mu(A) = \mu \) we have:

There are \( X_{p+1}(\mu)\gamma_{p+1}^*(\mu) \) elements in \( \mathcal{M} \) on the same cycle as \( A \).
Hence, we must prove \( \{ A \in \mathcal{M} : \mu(A) = \mu \}^{**} = \prod_{i=1}^{p+1} w_i(\mu) \).

By Lemma 4.1 c) in [2] we have
\[
\prod_{i=1}^{p+1} \{ D_i(A) : \mu(A) = \mu \} = \{ (D_1(A), \ldots, D_{p+1}(A)) : \mu(A) = \mu \}
\]
and
\[
\{ (D_1(A), \ldots, D_{p+1}(A)) : \mu(A) = \mu \}^{**} = \{ A \in \mathcal{M} : \mu(A) = \mu \}^{**}.
\]

Hence, the proof is complete if we can prove
\[
(7.5) \quad \{ D_i(A) : \mu(A) = \mu \}^{**} = w_i(\mu) \text{ for } i = \ldots, p+1.
\]

We suppose first \( 1 \leq i \leq p \). By (7.2), (7.3) and (7.4) we get
\[
\{ D_i(A) : \mu(A) = \mu \}^{**} = \prod_{r=1}^{\alpha_i} \{ t : (d_1, \ldots, d_{\gamma_i}) \in \mathcal{P}_i(\mu) : d_1 = t \}^{*}.
\]

Hence, we must prove
\[
\{ (d_1, \ldots, d_{\gamma_i}) \in \mathcal{P}_i(\mu) : d_1 = t \}^{**} = \sigma(t, \gamma_i^*, \alpha_i^*).
\]

This follows by c) since \( \{ (d_1, \ldots, d_{\gamma_i}) \in \mathcal{P}_i(\mu) : d_1 = t \} \) is in bijective correspondence with \( \mathcal{R}(t, \gamma_i^*, \alpha_i^*) \) by the map
\[
(d_1, \ldots, d_{\gamma_i}) \to (d_1, \ldots, d_{\gamma_i^*}).
\]

Hence, (7.5) is proved in the case \( 1 \leq i \leq p \).

Next we prove (7.5) in the case \( i = p+1 \). By (7.2)
\[
(7.6) \quad \{ D_{p+1}(A) : \mu(A) = \mu \}^{*} = \mathcal{P}_{p+1}(\mu)^{*}
\]

We let
\[
Q(s,t) = \{ (d_1, \ldots, d_s) : d_1 \geq 0 \text{ and } d_1 + \ldots + d_s = t \}.
\]

We get
\[
(7.7) \quad Q(s,t)^{**} = \binom{s+t-1}{s-1}.
\]
We define
\[ \phi\left( \left[ \begin{array}{c} d_1 \\ \vdots \\ d_{p+1} \\ s_1 \\ \vdots \\ s_{p+1} \end{array} \right] \right) = (d_1, \ldots, d_{p+1}) \times (s_1, \ldots, s_{p+1}) \]
for elements in \( \mathcal{P}_{p+1}(\mu) \).
\( \phi \) is injective and \( \phi(\mathcal{P}_{p+1}(\mu)) = \mathcal{R}(\gamma_{p+1}, \alpha_{p+1}-m*) \times Q(\gamma_{p+1}, m*) \cup Q(\gamma_{p+1}, \alpha_{p+1}-m*) \times \mathcal{R}(\gamma_{p+1}, m*) \)

Hence, by d) and (7.7) we get
(7.8) \( \mathcal{P}_{p+1}(\mu)^* = w_{p+1}(\mu) \).

In the proof of (7.8) we use the formula
\[ (A \cup B)^* = A^* + B^* - (A \cap B)^* \]
(7.6) and (7.8) imply \( \{D_{p+1}(A) : \mu(A) = \mu\}^* = w_{p+1}(\mu) \).

Q.E.D.

8. The reduction

We will reduce the cycle structure problem to the set studied in the Sections 4 - 7. First we need two lemmas. C \( \subset \) D means C contained in D and C \( \not\subset \) D. If D = a_1 \cdots a_s, we define
\( t \in D \iff r \leq t \leq s \) and \( f_D(t) = f(a_r \cdots a_t) \).

Lemma 8.1: 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 \( f(C_i) = -\text{type}(B_i) \) and 0 > \( f_{C_i}(t) \) \( \geq \) -\( \text{type}(B_i) \) for \( t \in C_i \).

Then we have
\[ n + \text{type}(B_f) = \left( \sum_{i=1}^{p+1} 2i \gamma_i \right) + m_A + (i_1 + \ldots + i_f) \],
and
\[ \alpha_{\text{type}(B_f)}(A) = m_A \iff i_1 + \ldots + i_f = 0 \].
Proof: We let $C_f = 0_{\text{type}(B_f)}$ and consider
\[ A^* = AC_f = 0_1 B_1 C_1 \ldots 0_f B_f C_f. \]

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

- the length of $B_i = m(B_i) + \Sigma\{2 \cdot \text{type}(B^*) : B^* < B_i\}$,
- the length of $C_i = \text{type}(B_i) + \Sigma\{2 \cdot \text{type}(B^*) : B^* < C_i\}$.

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

- the length of $B_i C_i = [m(B_i) - (p+1)] + \Sigma\{2 \cdot \text{type}(B^*) : B^* < B_i C_i\}$.

Otherwise,

- the length of $B_i C_i = \Sigma\{2 \cdot \text{type}(B^*) : B^* < B_i C_i\}$.

Hence,

- the length of $A^* = [m(B_i) - (p+1)] : \text{type}(B_i) = p+1$
  + $\Sigma\{2 \cdot \text{type}(B^*) : B^* \text{ a block}\} + (i_1 + \ldots + i_f)$
  \[= m_A + (\Sigma 2 i \gamma_i) + (i_1 + \ldots + i_f).\]

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

Q.E.D.

We write

\[(8.1) \quad \theta_{k,p} = \theta_{E_{k+\ldots+E_{k+p}}}.\]

Lemma 8.2: 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

\[(\gamma_{p+1}(A) \neq 0 \text{ and } a_{p+1}(A) = m_A \text{ or } \{z = \sup\{i : \gamma_i(A) \neq 0\} < p+1 \text{ and } a_z(A) = 0\}) \iff \theta_{j,k,p}(A) = \theta_{j,k,p}'(A) \text{ for } p' > p \text{ and every } j.\]
Proof: We suppose first $\gamma_{p+1}(A) \neq 0$. By Lemma 4.4 in [2] there exists $q$ such that $\bar{A} = \theta_{k,p}^q(A)$ satisfies

$$\gamma_i(A) = \gamma_i(\bar{A}), a_i(A) = a_i(\bar{A}), m_A = m_{\bar{A}},$$

$\bar{A}$ 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

$$\bar{A} = 0_{i_1} B_1 C_1 0_{i_2} B_2 C_2 \ldots 0_{i_f} B_f$$

as in Lemma 8.1.

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

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

$$w(\theta_{k,p}(\bar{A})) = k+p+1$$

where $s$ = length of $B_1 C_1$.

In the same way we prove $i_1 = \ldots = i_f = 0$. By Lemma 8.1

$$a_{p+1}(\bar{A}) = m_{\bar{A}}.$$ Hence, $a_{p+1}(A) = m_A$.

Next we suppose $a_{p+1}(A) = m_A$. Hence, $a_{p+1}(\bar{A}) = m_{\bar{A}}$. By Lemma 8.1 we have $i_1 + \ldots + i_f = 0$. Hence, type($B_1$) = $p+1$. Moreover, let $j = \inf\{i > 1 : \text{type}(B_i) = p+1\}$. Put $C_1^j = C_1 B_2 C_2 \ldots B_{j-1} C_{j-1}$ and $B_2^j = B_j$. By continuing in this way we can suppose

$$\text{type}(B_1) = \ldots = \text{type}(B_f) = p+1.$$ Hence, by Lemma 5.6 c) we get

$$\theta_{j,k,p}^p(\bar{A}) = \theta_{j,k,p}^p(\bar{A})$$

for $p' > p$.

Finally we treat the case $z = \sup \gamma_i(A) < p+1$. By Lemma 5.6 a) we have $\theta_{j,k,p}^p(A) = \theta_{j,k_1,p_1}^p(A)$ where $k_1 = p+1 - z$ and $p_1 = z-1$.

By Lemma 4.4 in [2] there exists $q$ such that $\bar{A} = \theta_{k,p}^q(A)$ satisfies:

$$\gamma_i(A) = \gamma_i(\bar{A}), a_i(A) = a_i(\bar{A}), m_A = m_{\bar{A}} = 0,$$

$\bar{A}$ 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

$$\bar{A} = 0_{i_1} B_1 C_1 0_{i_2} B_2 C_2 \ldots 0_{i_f} B_f$$

as in Lemma 8.1.
We suppose $\theta^j_{k,p}(A) = \theta^j_{k,p'}(A)$ for $p' > p$. As in the case $\gamma_p(A) \neq 0$ we prove $i_1 = \ldots = i_f = 0$. By Lemma 8.1 $a_z(A) = m_A = 0$.

Next we suppose $a_z(A) = 0$. Hence, $a_z(\bar{A}) = m_{\bar{A}} = 0$. By Lemma 8.1 we have $i_1 + \ldots + i_f = 0$. As before we can suppose $\text{type}(B_p) = \ldots = \text{type}(B_f) = z$. Hence, by Lemma 5.6 c) we get $\theta^j_{k,p}(\bar{A}) = \theta^j_{k,p'}(\bar{A})$ for $p' > p$.

Q.E.D.

Now we start the reduction process. We need very precise notation:

If we determine the block structure of $A$ with respect to $p$, we write $\gamma^p_1(A) = \gamma^p_i(A)$, $a^p_i(A) = a_i(A)$ and $m^p_A = m_A$.

For $\mathcal{F} \subset \{0,1\}^n$ we define $\mathcal{F}[k,p] = \{ \theta^i_{k,p}(A) : A \in \mathcal{F} \text{ and } i \text{ is an integer} \}$.

Reduction 1: We define

$$\mathcal{M}_{k,p} = \{ A : w(A) = \sup_i w(\theta^i_{k,p}(A)) \in \{ k, \ldots, k+p+1 \} \}.$$ 

If $A = a_1 \ldots a_n \notin \mathcal{M}_{k,p}$, then we have $\theta_{k,p}(A) = a_2 \ldots a_n a_1$ and $\theta_{k,p}(A) \notin \mathcal{M}_{k,p}$.

Proof: For $A = a_1 \ldots a_n \notin \mathcal{M}_{k,p}$ we have $w(a_2 \ldots a_n) \notin \{ k, \ldots, k+p \}$.

Hence, $(E_k + \ldots + E_{k+p})(a_2 \ldots a_n) = 0$.

Q.E.D.

Reduction 2: We define

$$\mathcal{M}_{k,p}(i) = \{ A \in \mathcal{M}_{k,p} : w(A) = i \}.$$ 

a) $\mathcal{M}_{k,p} = \bigcup_{s=0}^{p} \mathcal{M}_{k,p}(k+s+1)$ is a disjoint union.
b) We define

\[ \mathcal{M}_{k,p}^{*}(k+p+1) = \{ A \in \mathcal{M}_{k,p}^{*}(k+p+1) : \gamma_{p+1}^p(A) \neq 0 \quad \text{and} \quad \sigma_{p+1}^p(A) = \mathcal{M}^p(A) \text{ or } (z = \sup\{ i : \gamma_i^p(A) \neq 0 \} < p+1 \quad \text{and} \quad \sigma_{p+1}^p(A) = 0) \}. \]

For \( s < p \) we have

\[ \mathcal{M}_{k,p}^{*}(k+s+1)[k,p] = \mathcal{M}_{k,s}^{*}(k+s+1)[k,s] \quad \text{and} \quad \theta_{k,p} = \theta_{k,s} \text{ on this set}. \]

**Proof:** a) is obvious.

b) By Lemma 5.6 c) in [2] we have \( \theta_{k,p}^i(A) = \theta_{k,s}^i(A) \) for all \( i \) and \( A \in \mathcal{M}_{k,p}^{*}(k+s+1) \). Moreover, by Lemma 8.2 we have

\[ A \in \mathcal{M}_{k,p}^{*}(k+s+1) \iff A \in \mathcal{M}_{k,s}^{*}(k+s+1). \]

Q.E.D.

By Reduction 2 it is sufficient to determine the cycle-structure of the sets

\[ \mathcal{M}_{k,p}(k+p+1)[k,p] \quad \text{and} \quad \mathcal{M}_{k,p}^{*}(k+p+1)[k,p] \]

with respect to \( \theta_{k,p} \).

**Reduction 3:** We define

\[ \mathcal{M}_{k,p}(k+p+1,j) = \{ A \in \mathcal{M}_{k,p}(k+p+1) : \sup\{ i : \gamma_i^p(A) \neq 0 \} = j \}, \]

\[ \mathcal{M}_{k,p}^{*}(k+p+1,j) = \{ A \in \mathcal{M}_{k,p}^{*}(k+p+1) : \sup\{ i : \gamma_i^p(A) \neq 0 \} = j \}. \]

a) \( \mathcal{M}_{k,p}(k+p+1)[k,p] = \bigcup_{j=1}^{p+1} \mathcal{M}_{k,p}(k+p+1,j)[k,p] \) is a disjoint union.

b) Suppose \( j < p+1 \). Put \( k' = k+p+1 - j \) and \( p' = j-1 \).
Then
\[ M_{k,p}(k+p+1,j)_{[k,p]} = \{ A \in M_{k',p'}(k'+p'+1,p'+1) : m_{A}^{p'} = 0 \} \]
and \( \theta_{i}^{i} k',p'(A) = \theta_{i}^{i} k',p'(A) \) for \( A \in M_{k,p}(k+p+1,j) \).

c) \( M_{k,p}^{*}(k+p+1)_{[k,p]} = \bigcup_{j=1}^{p+1} M_{k,p}^{*}(k+p+1,j)_{[k,p]} \) is a disjoint union.

d) Suppose \( j < p+1 \). Put \( k' = k+p+1 - j \) and \( p' = j-1 \).
Then
\[ M_{k,p}^{*}(k+p+1,j)_{[k,p]} = \{ A \in M_{k',p'}(k'+p'+1) : \alpha_{p'+1}^{p}(A) = 0 \} \]
and \( \theta_{i}^{i} k',p'(A) = \theta_{i}^{i} k',p'(A) \) for \( A \in M_{k,p}^{*}(k+p+1,j) \).

e) \( M_{k,p}^{*}(k+p+1,p+1)_{[k,p]} = \{ A \in M_{k,p}(k+p+1,p+1) : \alpha_{p+1}^{p}(A) = m_{A} \} \).

**Proof:** By Lemma 4.12 in [2] we have for \( A \in M_{k,p} \):
If \( w(\theta_{i}^{i} k',p'(A)) = k+p+1 \), then \( \gamma_{i}(A) = \gamma_{i}(\bar{A}) \), \( \alpha_{i}(A) = \alpha_{i}(\bar{A}) \)
and \( m_{A} = m_{\bar{A}} \) where \( \bar{A} = \theta_{k,p}^{i}(A) \).

a) and c) follows from this observation. e) follows by the definition of \( M_{k,p}^{*}(k+p+1) \).

b) By the definitions of blocks
\[ A \in M_{k,p}(k+p+1,j) \iff A \in M_{k',p'}(k'+p'+1,p'+1) \text{ and } m_{A}^{p'} = 0 \]
Moreover, by Lemma 5.6 a) in [2] we have
\[ (8.2) \quad \theta_{i}^{i} k',p'(A) = \theta_{i}^{i} k',p'(A) \text{ for all } i \text{ and } A \in M_{k,p}(k+p+1,j) \].

d) By the definition of \( M_{k,p}^{*}(k+p+1,j) \)
\[ A \in M_{k,p}^{*}(k+p+1,j) \iff A \in M_{k',p'}(k'+p'+1,p'+1) \text{ and } m_{A}^{p'} = 0 \text{ and } d) \text{ follows.} \]
Put $\mathcal{N} = \mathcal{M}_{k,p}(k+p+1,p+1)$. By the Reduction 3 there is sufficient to determine the cycle structure with respect to $\theta_{k,p}$ of the following 4 sets

$$
\mathcal{N}_{[k,p]},
$$

$$
\mathcal{S}_1 = \{A \in \mathcal{N} : m_A^p = 0\}_{[k,p]},
$$

$$
\mathcal{S}_2 = \{A \in \mathcal{N} : \sigma_{p+1}(A) = 0\}_{[k,p]},
$$

$$
\mathcal{S}_3 = \{A \in \mathcal{N} : \sigma_{p+1}(A) = m_A\}_{[k,p]}.
$$

By Lemma 4.4 in [2] $\mathcal{N}_{[k,p]} = \mathcal{M}_{[k,p]}$ where $\mathcal{M}$ is as in Section 4. Hence, the cycle structure of $\mathcal{N}_{[k,p]}$ is completely determined in the Sections 4 - 7. The other 3 sets are subsets of $\mathcal{N}_{[k,p]}$ and we find the cycle structure of these sets by modifying the Theorems 6.2, 6.3 and 7.2. More precisely, let $\mathcal{P}_1$ be as in Thm. 6.3 and define.

$$
\mathcal{P}_1^1 = \{(y_1,\ldots,y_{p+1}) \in \mathcal{P}_1 : \sum_{i=1}^{p+1} i \cdot y_i = k+p+1 \text{ and } \sum_{i=1}^{p+1} i \cdot y_i \leq n+p+1\}
$$

$$
\mathcal{P}_1^2 = \{(y_1,\ldots,y_{p+1}) \in \mathcal{P}_1 : \sum_{i=1}^{p+1} i \cdot y_i = k+p+1 \text{ and } \sum_{i=1}^{p+1} i \cdot y_i = n+p+1\}
$$

$$
\mathcal{P}_1^3 = \{y = (y_1,\ldots,y_{p+1}) \in \mathcal{P}_1 : m(y) + \sum_{i=1}^{p+1} i \cdot y_i = n+p+1 \text{ and } m(y) + \sum_{i=1}^{p+1} i \cdot y_i = k+p+1\}
$$

If we will determine the cycle structure of $\mathcal{S}_i$, the only change in the Theorems 6.2, 6.3 and 6.4 is that we replace $\mathcal{P}_1$ in Thm. 6.3 a) by $\mathcal{P}_1^i$ ($i = 1,2,3$).

Next we do the following observations.

**Observation 8.3:** Thm. 5.1 is true for $A \in \{0,1\}^n$ such that $w(A) = k+p+1$ and $\gamma_{p+1}^p(A) \neq 0$. 
Proof: By Lemma 4.4 and 4.12 in [2] there exists $j$ such that $A^* = \theta_k^j(A) \in M$ and integers $r_q, x_q$ $(q = 1,...,p+1)$ such that:

\[
\begin{cases}
\text{If } q \in \{1, ..., p\} \text{ and } D_q(A) = (t_1, ..., t_{\gamma_q}), \text{ then } \\
D_q(A^*) = (t_{r_q+1} - x_q, ..., t_{\gamma_q} - x_q, t_1 - x_q + a_q(A), ..., t_{r_q} - x_q + a_q(A)).
\end{cases}
\]

Moreover, the analogous statement is true for $q = p+1$.

It is very easy to see that the trivial periods of the difference vectors of $D_q(A)$ and $D_q(A^*)$ are equal. Hence, $\gamma_q^*(A) = \gamma_q^*(A^*)$ and $a_q^*(A) = a_q^*(A^*)$ for $q = 1,...,p+1$.

The observation follows easily.

Q.E.D.

Observation 8.4: Suppose $w(A) \in \{k,...,k+p+1\}$. Then

\[
\sup_{1 \leq i \leq 2n} w(\theta_{k,p}^i(A)) = \sup_i w(\theta_{k,p}^i(A)).
\]

Proof: We choose $j$ such that $A^* = \theta_k^j(A)$ satisfies $w(A^*) = \sup w(\theta_{k,p}^i(A))$. As in Step 3 and 4 in the forthcoming procedure where we determine the minimal periods, we can suppose $w(A^*) = k+p+1$ and $\gamma_p^{p+1}(A) \neq 0$. By Lemma 4.4 in [2] there exists $i$ such that $A^{**} = \theta_k^i(A^*) \in M$ where $M$ is as in Section 4.

By Lemma 4.2 and 4.3 we have

\[
w(A^{**}) = w(\psi(A^{**})) = ... = w(\psi^j(A^{**})) = ... = k+p+1
\]

and $\psi^j(A^{**}) = \theta_{k,p}^q(\psi^{j-1}(A^{**}))$ for some $q \leq 2n$.

Hence, the observation follows.

Q.E.D.

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 $w(A) \notin \{k, \ldots, k+p+1\}$, then $\theta_{k,p}(A) = \xi(A)$ where 

$$\xi(a_1 \ldots a_n) = (a_2 \ldots a_n a_1)$$

and the problem is trivial.

We therefore suppose $w(A) \in \{k, \ldots, k+p+1\}$.

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

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

(The last equality follows from Obs. 8.4.)

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]). Moreover, we have $w(A^*) = k''+p''+1$ and $\gamma_{p''+1}^{p''+1}(A^*) \neq 0$. Hence, we can use Thm. 5.1 (Obs. 8.3).
Index of notation:

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
<th>Lemma/Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\theta_S$</td>
<td>the introduction</td>
<td>Lemma 4.2, 4.3</td>
</tr>
<tr>
<td>$E_i$</td>
<td></td>
<td>Lemma 4.3</td>
</tr>
<tr>
<td>$i, i'$</td>
<td>Section 2</td>
<td></td>
</tr>
<tr>
<td>$f(\cdot)$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$a \land b$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$B$</td>
<td>denotes a block</td>
<td></td>
</tr>
<tr>
<td>$d(B)$</td>
<td>Section 2</td>
<td></td>
</tr>
<tr>
<td>$w(\cdot)$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\theta$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\Lambda(\cdot)$, $\mathcal{D}(\cdot)$</td>
<td>Def. 3.1</td>
<td></td>
</tr>
<tr>
<td>$D_i(A)$</td>
<td>Def. 3.2</td>
<td></td>
</tr>
<tr>
<td>$p(\beta, \hat{t})$, $a^*(\alpha, \hat{t})$</td>
<td>Lemma 3.5, 3.6</td>
<td></td>
</tr>
<tr>
<td>$r(\beta, \hat{t})$</td>
<td>Def. 3.7</td>
<td></td>
</tr>
<tr>
<td>$\mathcal{M}$</td>
<td>Section 4</td>
<td></td>
</tr>
<tr>
<td>$\psi$, $\text{Index}(\cdot)$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\gamma_i(A), a_i(A)$</td>
<td>(4.1)</td>
<td></td>
</tr>
</tbody>
</table>

References:


2. J. Søreng, Symmetric Shift Registers.
   (This is a revised version of "The difference equation $x_{n+1} = x_1 + S(x_2, \ldots, x_n)\ldots"", Preprint No. 19, 1977 University of Oslo.)
Appendix

In this appendix we will formulate the results in [2] which is not contained in "The difference equation ... ". First we mention that the definition of \( d(B) \) is changed: If we denote \( d(B) \) in "The difference equation ... " by \( d'(B) \), then \( d(B) = d'(B)-1 \) where \( d(B) \) is as in the revised version. Now we will formulate Lemma 4.1 c), 4.4, 4.11, 4.12, 4.13, 5.6 and 5.7 in [2]. The lemmas are reformulated slightly by using the notation of this paper. We refer to the index of notation.

**Lemma 4.1 c):** Suppose \( \gamma = (\gamma_1, \ldots, \gamma_{p+1}) \in P_1 \) (\( P_1 \) is as in Thm. 6.3 a)). Then

\[
\{(D_1(A), \ldots, D_{p+1}(A)) : A \in M(\gamma) = \bigcup_{i=1}^{p+1} \mathcal{F}_i \}
\]

where

\[
\mathcal{F}_i = \{(t_1, \ldots, t_{\gamma_i}) : 0 < t_1 \leq t_2 \leq \ldots \leq t_{\gamma_i} \leq a_i(\gamma)\} \quad \text{for } i = 1, \ldots, p,
\]

and

\[
\mathcal{F}_{p+1} = \{(s_1, \ldots, s_{\gamma_{p+1}}) : t_1 \geq 0, s_1 \geq 0, s_1 + \ldots + s_{\gamma_{p+1}} = m(\gamma),
\]

\[
t_1 + s_i \leq t_{i+1} \quad (i = 1, \ldots, \gamma_{p+1} - 1) \text{ and } t_{\gamma_{p+1}} + s_{\gamma_{p+1}} = a_{p+1}(\gamma)\}.
\]

Moreover, \( A \) is uniquely determined by \( D_1(A), \ldots, D_{p+1}(A) \).

Finally, we have

\[
M = \bigcup_{\gamma \in P_1} M(\gamma).
\]

**Lemma 4.4:** Suppose \( w(A) = k+p+1 \) and \( A \in \{0,1\}^n \). Then there exists \( j \) such that \( A^* = \delta_{k+p}^j(A) \in M \) and \( \gamma_j(A) = \gamma_j(A^*) \) \((i = 1, \ldots, p+1)\) and \( m_A = m_{A^*} \).

**Lemma 4.11** is almost equal to Lemma 4.2 in this paper.
Lemma 4.12: Suppose \( w(A) = w(\theta_{k+p}^i(A)) = k+p+1 \). Put \( A^* = \theta_{k+p}^i(A) \). Then there exists \( r_q, x_q \) \((q = 1, \ldots, p+1)\) such that:

If \( 1 \leq q \leq p \) and \( D_q(A) = (t_1, \ldots, t_{\gamma_q}) \), then

\[
D_q(A^*) = (t_{r_q+1} - x_q, \ldots, t_{\gamma_q} - x_q, t_1 + a(q - x_q), \ldots, t_{r_q} + a(q - x_q)).
\]

Moreover, if \( D_{p+1}(A) = \left[ \left( \frac{t_1}{s_1}, \ldots, \frac{t_{\gamma_{p+1}}}{s_{\gamma_{p+1}}} \right) \right] \), then

\[
D_{p+1}(A) = \left[ \frac{t_{r_{q+1}} - x_q}{s_{r_{q+1}}}, \ldots, \frac{t_{\gamma_q} - x_q}{s_{\gamma_q}}, \frac{t_1 + a_{\gamma(q - x_q)}}{s_1}, \ldots, \frac{t_{r_q + a_{\gamma(q - x_q)}}}{s_{r_q}} \right]
\]

where \( q = p+1 \).

Lemma 4.13 is almost equal to Lemma 4.3 in this paper.

Lemma 5.6: a) We suppose \( A \in \{0,1\}^n \) and \( w(A) = k+p+1 \).

We determine the block structure of \( A \) with respect to \( p \). If \( j = \sup \{\text{type}(B): B \text{ block in } A\} \), then

\[
w(\theta_{S}^i(A)) \leq k+p+1-j \text{ and } \theta_{S}^i(A) = \theta_{S'}^i(A) \text{ for every } i,
\]

where \( S = E_k + \ldots + E_{k+p} \), \( S' = E_{k'} + \ldots + E_{k'+p'} \), \( p' = j-1 \)

and \( k' = k+p+1-j \).

b) We suppose \( A \in \{0,1\}^n \). \( S = E_k + \ldots + E_{k+p} \) and \( w(A) = \sup_i w(\theta_{S}^i(A)) = k+p'+1 \). Then \( \theta_{S}^i(A) = \theta_{S'}^i(A) \) for every \( i \),

where \( S' = E_{k'} + \ldots + E_{k+p'} \).

c) We suppose \( A = a_1 \ldots a_n \in \{0,1\}^n \) and \( w(A) = k+p+1 \).

Suppose \( 1 \leq z \leq p+1 \). Suppose \( A = B \) is a \( z \)-block or

\[
A = B_1T_1B_2T_2 \ldots B_f \text{ where } \text{type}(B) = z \text{ and } T_i = a_r \ldots a_s \{ \text{satisfies}
\]

\[
0 > f(a_r, \ldots a_j) \geq -z = f(T_i) \text{ for } j = r, \ldots, s \text{ (i = 1, \ldots, r-1)}.
\]

Then for \( p' > p \) we have \( \theta_{S}^i(A) = \theta_{S'}^i(A) \) for every \( i \),

where \( S' = E_k + \ldots + E_{k+p'} \) and \( S = E_k + \ldots + E_{k+p} \).
Lemma 5.7: Suppose $A \in \{0,1\}^n$ and $w(A) = k+p+1$ and $S = E_k + \ldots + E_{k+p}$. Suppose $A = BTD$ where $B$ is a block and $T = a_r \ldots a_s$ satisfies

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

Then $w(S^z(A)) = k+p+1$ where $z = \text{the length of ET}$.