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 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 $A \rightarrow \theta_S(A) \rightarrow \cdots \rightarrow \theta_S^q(A) = A$ 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 $S = E_k + \cdots + E_{k+p}$ 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: $\mathscr{M} \rightarrow \{1, 2, \cdots\}$ and $\psi: \mathscr{M} \rightarrow \mathscr{M}$ in the following way:

Let $i > 0$ be the least integer such that $\theta_S^i(A) \in \mathscr{M}$, then we define 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 deter-