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

SYMMETRIC SHIFT REGISTERS

JAN SØRENG

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

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

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

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

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

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

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

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

2. Preliminaries.

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