Singular Shift Registers Over Residue Class Rings

by

MARIO MAGIDIN
Departamento de Matemáticas
Universidad Autónoma Metropolitana, Iztapalapa
México 13, D.F.
Mexico

and

ARTHUR GILL
Electronics Research Laboratory
Dept. of Electrical Engineering and
Computer Sciences
University of California, Berkeley, California

ABSTRACT

The study of shift registers over the ring \( Z_p \) (\( p \) a prime, \( r \geq 1 \)), in particular the singular case, is carried out, giving necessary and sufficient conditions to make a shift register singular. Its state graph is characterized as a tree, whose form depends on the characteristic polynomial of the shift register. The relationships with singular shift register over \( Z_p \) are explored and a proof of their equivalence is presented.

1. Introduction. In a recent paper [4], the authors showed that every Linear Sequential Circuit (LSC) defined over a residue class ring \( Z_m \) where \( m = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} \) (the \( p_i \) being distinct primes) is isomorphic to a parallel connection of \( k \) LSC's over \( Z_{p_i^{r_i}} \) \((i = 1, 2, \cdots, k)\) and each LSC over \( Z_{p_i^{r_i}} \) is in turn isomorphic to a cascade connection of \( r_i \) LSC's over \( Z_{p_i} \) (that is, the Galois field \( GF(p_i) \)), where the cascaded stages are separated by a (generally nonlinear) delay-free logic. In this paper, we specialize the study of LSC's to the important case of the shift register, in particular the singular shift register (SSR). We show its characterization, derive its properties and end up proving that any \( n \)-dimensional SSR over \( Z_{p^r} \) is equivalent to a \((n \times r)\)-dimensional LSC over \( Z_p \).

2. Definitions and Basic Results. The required results of the theory of LSC’s are introduced in this section. For more detail, the reader is referred to [1] or [2].
Definition 2.1. A finite sequential machine (or finite automaton) $M$ is a quintuple $\langle Q, \Sigma, \Delta, \delta, \lambda \rangle$, where

- $Q$ is a finite nonempty set of states.
- $\Sigma$ is a finite nonempty set of input symbols.
- $\Delta$ is a finite nonempty set of output symbols.
- $\delta$ is a function from $Q \times \Sigma$ into $Q$ called the transition function.
- $\lambda$ is a function from $Q \times \Sigma$ into $\Delta$ called the output function.

Definition 2.2. A Linear Sequential Circuit (LSC) over a ring $R$, is a sequential machine, such that there is a ring $R$ and non-negative integers $\ell, m, n$, such that $Q = R^n$, $\Sigma = R^\ell$, $\Delta = R^m$, and furthermore there exist matrices over $R$, $A_{n \times n}$, $B_{n \times \ell}$, $C_{m \times n}$, $D_{m \times \ell}$, such that:

$\delta(q, a) = Aq + Ba$

$\lambda(q, a) = Cq + Da$

for all $(q, a) \in Q \times \Sigma$.

Such a machine will sometimes be denoted by $\langle R, n, \ell, m, A, B, C, D \rangle$, or $\langle R, A, B, C, D \rangle$, or $\langle R, A, n, \varphi \rangle$ where $\varphi$ is the characteristic polynomial of $A$. Then $M$ is said to be of dimension $n$. We call $A$, $B$, $C$, $D$ the characterizing matrices, $A$ is called the characteristic matrix of the LSC.

An LSC as specified above can be realized by means of a finite number of primitive elements: adders, constant multipliers (both over the ring $R$) and $n$ unit delay elements. Conversely, any interconnection of such elements can be characterized as an LSC provided every closed loop contains at least one delay element, to avoid indeterminacy [1]. Figure 1 shows the customary representation for these primitive elements.

An LSC of the form $\langle R, n, 0, 0, A, 0, 0, 0 \rangle$ is called an Internal Circuit (IC).

$\text{Figure 1. Primitive elements}$

---

3 For any ring $R$ and any non-negative integer, $n$, $R^n$ is the module of $n$-tuples over $R$. 