COMMUNICATIONS IN INFORMATION AND SYSTEMS
Vol. 8, No. 1, pp. 39-54, 2008

003

# INVARIANTS OF PSEUDO-RANDOM NUMBER GENERATORS

CLYDE F. MARTIN* AND MARA D. NEUSEL*

**Abstract.** Pseudo-random number generators of the form $x_{n+1} = P(x_n)$, $y_n = h(x_n)$ are ubiquitous in applications ranging from cryptology to statistics. Such systems have been studied extensively in the control theory literature when $x_n \in \mathbb{R}$. In this paper we make a detailed study of the invariants of such systems when the underlying field is the Galois field of two elements. We consider various groups that act on such system.

**1. Introduction.** Repeatable pseudo-random number generators are ubiquitous in the technical world. Most such generators can be reduced to the following setting. Let $V$ be the vector space of dimension $n$ over the field with two elements $\mathbb{F}_2 = \{0, 1\}$. A **dynamical system with observation** consists of two mappings

$$P = (P_1, \ldots, P_n) : V \longrightarrow V \in \mathrm{map}(V, V), \text{ and}$$
$$h : V \longrightarrow \mathbb{F}_2 \in \mathrm{map}(V, \mathbb{F}_2).$$

We denote the set of all such systems by $\mathcal{A}$, i.e.,

$$(P, h) \in \mathcal{A} = \mathrm{map}(V, V) \times \mathrm{map}(V, \mathbb{F}_2).$$

We call $P$ the **generator of the system** $(P, h)$. Let $(P, h) \in \mathcal{A}$ and $\mathsf{v}_1 \in V$ some initial value. Set

$$\mathsf{v}_{i+1} = P(\mathsf{v}_i), \text{ and } y_i = h(\mathsf{v}_i) \quad \forall i = 1,\ 2, \cdots.$$

Thus we obtain a sequence of elements in $V$

$$\mathsf{v}_1,\ \mathsf{v}_2 = P(\mathsf{v}_1),\ \mathsf{v}_3 = P(\mathsf{v}_2), \cdots$$

generated by the map $P$. We call it the $P$**-sequence** and denote it by $\{P(\mathsf{v}_i)\}_{i \in \mathbb{N}}$. Furthermore we obtain a sequence of field elements

$$y_i(\mathsf{v}_1) = h(\mathsf{v}_i) \quad \forall i \in \mathbb{N}$$

denoted by

$$\{y_i(\mathsf{v}_1)\}_{i \in \mathbb{N}}.$$

This sequence is called a **system of pseudo-random numbers**.

Once an initial point $\mathsf{v}_1$ is chosen the output sequence is a string of zeros and ones uniquely determined by $P$ and $h$. These systems have been extensively studied, see, e.g., [9] and [11]. We follow the developments found in [13], [14], and [15].

*Department of Mathematics and Statistics, MS 1042, Texas Tech University, Lubbock, Texas 79409. E-mail: Clyde.F.Martin@ttu.edu and Mara.D.Neusel@ttu.edu