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

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

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 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

Background
Systems of the form $x_{n+1} = P(x_n),\ y_n = h(x_n)$ and $\dot{x} = P(x),\ y = h(x)$ have been studied extensively in the control theory and statistical literature. The literature of hidden Markov chains, see [7], studies these systems when the underlying process is stochastic. In the case that the mappings are linear is well understood. When the mappings are nonlinear there is much that is unknown and this case is an active area of research. The study of nonlinear observability has touched on issues that are related to the goals of this paper. The papers [2], [4], [6], and [8] are relevant in that they are studying systems evolving on groups. In the papers [3] and [12] observability properties are used to study the underlying dynamics of the system. There the duality between control and observation is an important feature. There is a rich literature that studies properties of observable systems including invariants but almost all of the literature assumes an underlying topology of the state space. In this paper, since the state space is finite, we concentrate on the algebraic aspects.

If the map $P : V \longrightarrow V$ is bijective then the vector space V can be written as a disjoint union of subsets stabilized by P

$$V = V_1 \sqcup \cdots \sqcup V_l,$$

where

$$V_i = \{\mathsf{v}_{i,1},\ P(\mathsf{v}_{i,1}),\ P^2(\mathsf{v}_{i,1}),\ \cdots\}.$$

Thus the V_i's constitute the orbits of the P-action on V. Moreover, the orbits of P are periodic, since for some $k_i \in \mathbb{N}$

$$\mathsf{v}_{i,1} = P^{k_i}(\mathsf{v}_{i,1}).$$

Thus we obtain a set of l periodic systems of pseudo-random numbers $\{y_j(\mathsf{v}_{i,j})\}_{j\in\mathbb{N}}$ for $i = 1, \ldots, l$. We note that the period of a system of pseudo-random numbers is a divisor of the period of the respective P-orbits.

If P is not bijective, then the situation is a bit more complicated, because the orbits of P for different starting values can intersect nontrivially. This means that in the case of nonbijective maps P we obtain sequences in V, and hence in $\mathbb{F}_2$, that are *eventually* periodic. We illustrate this with the next example.

Example 1.1. *Enumerate the elements of the vector space V by*

$$\mathsf{v}_1, \ldots, \mathsf{v}_{2^n-1}, 0.$$

Define $P : V \longrightarrow V$ by

$$P(\mathsf{v}_i) = \mathsf{v}_{i+1}, i \mod 2^n - 1 \quad \text{and} \quad P(0) = \mathsf{v}_1.$$

If we choose v_i *as initial value, we obtain the periodic orbit*

$$\mathsf{v}_i,\ \mathsf{v}_{i+1}, \dots, \mathsf{v}_{2^n-1},\ \mathsf{v}_1, \dots, \mathsf{v}_{i-1}.$$

However, if we choose 0 *as initial value we obtain the sequence*

$$0,\ \mathsf{v}_1, \dots, \mathsf{v}_{2^n-1},\ \mathsf{v}_1, \dots, \mathsf{v}_{2^n-1}, \dots .$$

Thus this orbit is periodic starting with the second value.

For practical reason it is desired to have a generator P that generates a sequence of fundamental *prime* period p that is as large as possible. To accomplish this we assume that $p = 2^n - 1$ is a prime number. Such a prime is a Mersenne prime. The first few are given by $n = 2, n = 3, n = 5, n = 7, n = 13, n = 17, n = 19, n = 31, n = 61$, and $n = 89$.

To achieve this P has to cyclicly permute $2^n - 1$ elements in the vector space V. As the example above shows the map P still could be noninvertible. In this case, the period might start at the second value. However, in either case, we obtain a system of pseudo-random numbers with *a* periodic orbit of length $2^n - 1$.

In this paper we primarily study systems with a periodic orbit of length $2^n - 1$ in general and leave the detailed study of the other cases to the subsequent paper [16]. In Section 2 we present a short proof of the classical result that systems with fundamental period $2^n - 1$ can be linearized. This proof can be easily generalized to the general case of systems (P, h) with invertible generator P but possibly smaller orbits. We note that linear recurring systems have been extensively studied in [11].

In particular we are interested in systems with **observable output sequences**: We denote the **set of output sequences of the system** (P, h) by

$$D(P, h) = \{\{y_i(\mathsf{v}_1)\}_{i\in\mathbb{N}} :\ \mathsf{v}_1 \in V\}$$

where v_1 is the chosen initial data. A system (P, h) is called **observable** if the set $D(P, h)$ is in one-to-one correspondence to V. We will see in Section 3 that systems with fundamental P-orbit of length $2^n - 1$ are observable if and only if the map h is not periodic. This has several generalizations to systems with smaller P-orbits or with invertible generators P.

In Section 4 we see that for a map $g : V \longrightarrow V$ preserving the P-orbits the systems (P, h) and (gPg^{-1}, hg^{-1}) have upto cyclic shift the same output sequences. Thus they are simultaneously observable. In Sections 5 and 6 we show that *every* system (P, h) can be generated by polynomial functions.

2. Systems with Period $2^n - 1$. We call two systems $(P, h), (Q, k) \in \mathcal{A}$ **equivalent** if they have the same *periodic* output sequences of length at least two (with possibly different starting values). We denote by $\mathcal{A}/\sim$ the associated set of equivalence classes.

In this section we show that for a system (P, h) with a maximal periodic orbit of length $2^n - 1$ there exists an equivalent system with invertible linear generator.

Let (P, h) be a system with a maximal periodic P-orbit of length $2^n - 1$

$$\mathsf{v}_1,\ \mathsf{v}_2 = P(\mathsf{v}_1), \ldots, \mathsf{v}_{2^n-1} = P(\mathsf{v}_{2^n-2}) = P^{2^n-2}(\mathsf{v}_1), P(\mathsf{v}_{2^n-1}) = \mathsf{v}_1,$$

for $\mathsf{v}_i \in V$. Since the output mapping $h : V \longrightarrow \mathbb{F}_2$ is defined by setting values of

$$h(\mathsf{v}) \in \mathbb{F}_2,$$

there are 2^{2^n} distinct output functions h.

THEOREM 2.1. *Let (P, h) have a periodic P-orbit of length $2^n - 1$. Then there exists a system $(\overline{P}, \overline{h})$ such that*

- *$\overline{P}$ is invertible.*
- *$\overline{P}(0) = 0$.*
- *$V = V \setminus 0 \sqcup \{0\}$ is a subdivision of V into irreducible orbits.*
- *$(\overline{P}, \overline{h})$ is equivalent to (P, h).*

Proof. The orbit of P is an ordered set which we denote by $[\mathsf{v}_1, \ldots, \mathsf{v}_{2^n-1}]$. Assume it does not contain zero, then we define

$$\overline{P}(\mathsf{v}) = \begin{cases} 0 & \text{if } \mathsf{v} = 0, \\ P(\mathsf{v}) & \text{otherwise.} \end{cases}$$

Furthermore, setting $\overline{h}(\mathsf{v}) = h(\mathsf{v})$. leads to a system $(\overline{P},\ \overline{h})$ with the same output sequence of period $2^n - 1$, but invertible generator.

If the orbit $[\mathsf{v}_1, \ldots, \mathsf{v}_{2^n-1}]$ of P does contain $0 \in V$, say $\mathsf{v}_{i_0} = 0$, we can reduce to the preceding case in the following way: Let $\mathsf{v}_0 \in V$ be the element not contained in the periodic orbit of P above. Then set

$$\overline{P}(\mathsf{v}) = \begin{cases} 0 & \text{if } \mathsf{v} = 0, \\ P(0) & \text{if } \mathsf{v} = \mathsf{v}_0, \\ \mathsf{v}_0 & \text{if } \mathsf{v} = \mathsf{v}_{i_0-1}, \\ P(\mathsf{v}) & \text{otherwise.} \end{cases}$$

Thus we obtain the system $(\overline{P}, \overline{h})$, so that $\overline{P}$ has orbits $V \setminus \{0\}$ and $\{0\}$ as desired and

$$\overline{h}(\mathsf{v}) = \begin{cases} h(0) & \text{if } \mathsf{v} = \mathsf{v}_0, \\ h(\mathsf{v}_0) & \text{if } \mathsf{v} = 0, \\ h(\mathsf{v}) & \text{otherwise.} \end{cases}$$

Thus the System $(\overline{P}, \overline{h})$ has the same periodic output sequence. Moreover, by construction the map $\overline{P}$ is invertible. □

Thus we can assume without loss of generality that a system with maximal period $2^n - 1$ is generated by an invertible map $P : V \longrightarrow V$. The next result shows that we even can assume that P is linear[1]. We give a proof for the sake of completeness.

Theorem 2.2. *Let (P, h) be a system such that its generator P has fundamental period $2^n - 1$. Then there is an equivalent system $(\mathsf{L}, h_{\mathsf{L}})$ with an invertible linear generator L.*

Proof. If the generator P has maximal period $2^n - 1$ then by the preceding Theorem 2.1 we can assume that P cyclicly permutes the nonzero elements of the vector space V and $P(\mathsf{0}) = \mathsf{0}$.

The general linear group $\mathsf{GL}(n,\ \mathbb{F}_2)$ has order

$$(2^n - 1)(2^n - 2) \cdots (2^n - 2^{n-1}).$$

It is a doubly transitive permutation group on $V \setminus 0$ containing an element $\mathsf{L} \in \mathsf{GL}(n,\ \mathbb{F}_2)$ of cycle length (and hence order) $2^n - 1$. Such an element is called a *Singer cycle*. See Satz 7.3 in Section II.7 of [10].

Thus by adjusting the map $h : V \longrightarrow \mathbb{F}_2$ we obtain a System $(\mathsf{L}, h_{\mathsf{L}})$ with the same output sequence. □

The following generalization for individual periodic orbits of length p is straightforward:

Corollary 2.3. *Let (P, h) be a system such that P has a periodic orbit of period p, $[\mathsf{v}_1, \ldots, \mathsf{v}_p]$, with output sequence of period $[y_1, \ldots, y_p]$. Then there is a system $(\mathsf{L}, h_{\mathsf{L}})$ with an invertible linear generator L and with a periodic output sequence of the same period $[y_1, \ldots, y_p]$ if and only if the general linear group $\mathsf{GL}(n,\ \mathbb{F}_2)$ contains an element of order kp for some $k \in \mathbb{N}$.*

On the other hand, if P is invertible then we can generalize the above result as follows:

Corollary 2.4. *Let (P, h) be a system such that P is invertible. Let*

$$V = V_1 \sqcup \cdots \sqcup V_l$$

be a subdivision of the vector space V into disjoint periodic P-orbits. Then there is an equivalent system $(\mathsf{L}, h_{\mathsf{L}})$ with an invertible linear generator L if and only if there exists an element $\mathsf{L} \in \mathsf{GL}(n,\ \mathbb{F}_2)$ such that V decomposes into periodic L-orbits

$$V = V_1' \sqcup \cdots \sqcup V_l'$$

with $|V_i'| = |V_i|$.

Remark 2.5. *Since any linear form fixes the origin we obtain in the setting of the preceding corollary that necessarily one of the orbits V_i has length one.*

[1] The first author was made aware of this result by J. Rosenthal.

We note that the advantage of linear maps L, in contrast to arbitrary maps P, is that they are predictable, in the sense that if the values $\mathsf{L}(\mathsf{v}_1), \dots, \mathsf{L}(\mathsf{v}_k)$ are known and the set $\{\mathsf{v}_1, \dots, \mathsf{v}_k\}$ contains a basis of V, then L is known, and hence its entire orbits.

3. Observability. A system (P, h) is said to be **observable** if there is a one-to-one mapping from initial data to output sequences. Let

$$D(P, h) = \{\{y_i(\mathsf{v}_1); \mathsf{v}_1\}_{i=1}^{\infty} : \ \mathsf{v}_1 \in V\}$$

be the set of output sequences. Thus observability is the condition that the vector space V is in one-to-one correspondence with D.

In this section we present criteria for observability of systems (P, h) such that either P is invertible or the fundamental period of P has length $2^n - 1$.

In general the question of which systems are observable is quite complex. However, for linear systems there is a direct answer which is classic.

Theorem 3.1. *Let $\mathsf{A} : V \longrightarrow V$ be a linear map and let $h : V \longrightarrow \mathbb{F}$, $h(\mathsf{v}) = \mathsf{cv}$ for some $\mathsf{c} \in \mathbb{F}^n$. The system (A, h) is observable if and only if*

$$\det \begin{bmatrix} \mathsf{c} \\ \mathsf{cA} \\ \vdots \\ \mathsf{cA}^n \end{bmatrix} \neq 0.$$

For polynomial systems there is no general characterization of observability, see for example [5]. Indeed, in this case the answer depends on the ground field as the next example shows.

Example 3.2. *Let $V = \mathbb{F}$. Define a system (P, h) by*

$$P : V \longrightarrow V, \ \mathsf{v} \mapsto \mathsf{v}$$

and

$$h : V \longrightarrow \mathbb{F}, \mathsf{v} \mapsto \mathsf{v}^3 - 1.$$

If the ground field $\mathbb{F} = \mathbb{R}$ is the real numbers then this system is observable, because cube roots are unique. However, if $\mathbb{F} = \mathbb{C}$ is the field of complex numbers, this is no longer true and the system is no longer observable.

For arbitrary systems with fundamental period of prime length $2^n - 1$ we obtain a similarly easily checked criteria.

Theorem 3.3. *Let (P, h) have a periodic P-orbit of length $p = 2^n - 1$. Further assume that $2^n - 1$ is prime. The system is observable if and only if h is not constant on $V \setminus \{0\}$.*

Proof. Since the period of P is a multiple of the period of the random number sequence, and since $p = 2^n - 1$ is prime, we have that the sequence of random numbers has either period one or period $2^n - 1$. In the first case h is constant while in the second case the system is observable. □

As a corollary we have the following.

Corollary 3.4. *Let (P, h) be a system with invertible P. Let $V = V_1 \sqcup \cdots \sqcup V_l$ be a subdivision into irreducible P-orbits. Assume that $|V_i| = 1$ or prime. Then the system is observable if and only if h discriminates between the orbits of P and is not constant on any of these.*

The corollary is reminiscent of the seminal result of D. Aeyels, [1].

We note that for observability mainly the output sequence matters. Thus we can drop the assumption on the primality of the orbit lengths, replace it by a suitable condition on the map h and obtain the following result.

Theorem 3.5. *Let (P, h) be a system with maximal periodic P-orbit of length $2^n - 1$. Then this system is observable if and only if the output sequence $\{h(v_i)\}_{i\in\mathbb{N}}$ has fundamental period $2^n - 1$.*

Proof. By Theorem 2.2 the system (P, h) is equivalent to a system $(\mathsf{L}, h_{\mathsf{L}})$ with $\mathsf{L} \in \mathsf{GL}(n, \mathbb{F}_2)$. Thus the $2^n - 1$ periodic sequences of P are in one-to-one correspondence to the sequences of period $2^n - 1$ of L. Furthermore, the additional orbit of P of period $2^n - 1$ (if P is not bijective), resp. of period one (if P is bijective), corresponds to the orbit $\{0\}$ of L. Thus the set of all output sequences of (P, h) is in one-to-one correspondence to the output sequences

$$D(\mathsf{L}, h_{\mathsf{L}})$$

where $\mathsf{L} \in \mathsf{GL}(n, \mathbb{F})$ is a Singer-cycle, and $h_{\mathsf{L}} : V \longrightarrow \mathbb{F}_2$ is a suitable map. Thus h_{L} is not periodic on the ordered set $[v_1, P(v_1), \ldots, P^{2^n-2}(v_1)]$ if and only if $|D(\mathsf{L}, h_{\mathsf{L}})| = 2^n = |V|$. □

Similarly to Corollaries 2.3 and 2.4 we have the following:

Corollary 3.6. *Let (P, h) be a system with invertible P. Let $V = V_1 \sqcup \cdots \sqcup V_l$ be a subdivision into irreducible P-orbits. Assume that there is an element $\mathsf{L} \in \mathsf{GL}(n, \mathbb{F})$ and a map h_{L} such that the system $(\mathsf{L}, h_{\mathsf{L}})$ is equivalent (P, h). Then the system is observable if and only if h discriminates between the orbits of P and is not periodic on any of these.*

4. G-Equivalent Systems. Let G be the group of all invertible mappings on V

$$G = \{g : V \longrightarrow V,\ \mathsf{v}_i \mapsto g(\mathsf{v}_i)\},$$

where the group composition is given by composition of maps. We note that since G consists of all permutations of elements in V, it is abstractly isomorphic to the symmetric group on 2^n letter, Σ_{2^n}.

In this section we study the action of G on set of all systems $\mathcal{A}$ given by

$$G \times \mathcal{A} \longrightarrow \mathcal{A},\ (P, h) \mapsto (gPg^{-1}, hg^{-1}).$$

Proposition 4.1. *Let $(P, h) \in \mathcal{A}$ with invertible P. Let*

$$V = V_1 \sqcup \cdots \sqcup V_l$$

be a subdivision of the vector space into disjoint P-orbits. If $g \in G$ preserves the orbits then the two systems (P, h) and (gPg^{-1}, hg^{-1}) are equivalent.

Proof. Let $\mathsf{v}_{i,1} \in V_i$. Set $|V_i| = d_i$. Thus the system (P, h) has output sequences with period

$$h(\mathsf{v}_{i,1}),\ h(\mathsf{v}_{i,2}), \ldots, h(\mathsf{v}_{i,d_i})$$

for any $i = 1, \ldots, l$. By assumption we have that

$$g\mathsf{v}_{i,1} \in V_i.$$

If we choose $g\mathsf{v}_{i,1}$ as the starting value then the system (gPg^{-1}, hg^{-1}) has gPg^{-1}-sequence

$$g\mathsf{v}_{i,1},\ g\mathsf{v}_{i,2},\ g\mathsf{v}_{i,3},\ \ldots, g\mathsf{v}_{i,d_i}$$

and output sequence

$$\begin{aligned} h(g^{-1}g\mathsf{v}_{i,1}) &= h(\mathsf{v}_{i,1}), \\ h(g^{-1}gPg^{-1}g\mathsf{v}_{i,1}) &= h(P(\mathsf{v}_{i,1})) = h(\mathsf{v}_{i,2}), \\ &\cdots \\ h(g^{-1}gPg^{-1}g\mathsf{v}_{i,d_{i-1}}) &= h(P(\mathsf{v}_{i,d_{i-1}})) = h(\mathsf{v}_{i,d_i}) \end{aligned}$$

as desired. □

Remark 4.2. *We cannot subdivide V into P-orbits if P is not bijective. However, in this case we can phrase the preceding result "orbitwise": Let $V_1 \subseteq V$ be a P-orbit, and let $g \in G$ act on V_1. Then the output sequences of (P, h) and (gPg^{-1}, hg^{-1}) associated to the orbit V_1 are identical upto a cyclic shift.*

The preceding result motivates the following definition.

Definition 4.3. *Let $V_\bullet = \{V_1, \ldots, V_l\}$ be a subdivision of the vector space V into l disjoint subsets. Denote by $G_{V_\bullet} \subseteq G$ the subset of all invertible maps $g : V \longrightarrow V$ that preserve $V_\bullet$, i.e.,*

$$g(V_i) = V_i \quad i = 1, \ldots, l.$$

It is easily seen that $G_{V_\bullet} \leq G$ forms a subgroup. It is the largest subgroup of G acting on the set $\mathcal{A}(V_\bullet)$ of all systems (P, h) such that $V_\bullet$ is a subdivision of V into periodic P-orbits.

Remark 4.4. *The group $G_{V_\bullet}$ acts also on the set of all systems (P, h) such that $V_\bullet$ is a subdivision of V into blocks fixed by P. In this case the V_i's might not be orbits, but unions of orbits. Furthermore, $G_{V_\bullet}$ might not be the largest subgroup of G acting on the set of these systems.*

Remark 4.5. *By definition the set $\mathcal{A}(V_\bullet)$ consists only of systems (P, h) with invertible P. If P is not invertible, then the union of the subsets in $V_\bullet$ might not be the entire space V. Conversely, if $V_1 \cup \cdots \cup V_l = V$ then $\mathcal{A}(V_\bullet)$ consists of systems with invertible generator.*

Theorem 4.6. *Consider the action of $G_{V_\bullet}$ on $\mathcal{A}(V_\bullet)$. Let $(P, h) \in \mathcal{A}(V_\bullet)$. Then the $G_{V_\bullet}$-orbit of (P, h) consists precisely of all systems $(Q, k) \in \mathcal{A}(V_\bullet)$ that have upto cyclic shift the same output sequences.*

Proof. The preceding Proposition 4.1 shows that any two elements in one $G_{V_\bullet}$-orbit have upto cyclic shift the same output sequence.

Conversely, let (P, h) and (Q, k) be systems in $\mathcal{A}(V_\bullet)$. Let (P, h) have an orbit with initial value v_1 and output sequence $\{y_i(\mathsf{v}_1)\}_i$ and let the system (Q, k) have an orbit with initial value w_1 with output sequence $\{\eta_i(\mathsf{w}_1)\}_i$. Assume that they differ by a cyclic shift:

$$y_i(\mathsf{v}_1) = \eta_{i+m}(\mathsf{w}_1)$$

for some fixed m. Then choose an element $g : V \longrightarrow V \in G$ such that

$$g(\mathsf{w}_{i+m}) = \mathsf{v}_i \quad \forall i.$$

We can do that simultaneouly for all orbits since they are disjoint and g is an arbitrary bijective function from V to itself.

We obtain

$$gQg^{-1}(\mathsf{v}_i) = gQ(\mathsf{w}_{i+m}) = g(\mathsf{w}_{i+m+1}) = \mathsf{v}_{i+1} = P(\mathsf{v}_i)$$

and

$$h(\mathsf{v}_i) = k(\mathsf{w}_{i+m}) = k(g^{-1}\mathsf{v}_i).$$

Thus (P, h) and (Q, k) lie in the same $G_{V_\bullet}$-orbit. □

The preceding result is not the converse to Proposition 4.1, because the $G_{V_\bullet}$-orbit of a system (P, h) in $\mathcal{A}(V_\bullet)$ consists of systems that have exactly the same output sequences of length one. Furthermore, we note that not all equivalent systems of (P, h) are in $\mathcal{A}(V_\bullet)$, since they might have different P-orbits. However, the preceding result tells us that $G_{V_\bullet}$ acts on $\mathcal{A}(V_\bullet)/\sim$ and there it acts trivially. In other words the equivalence classes of elements in $\mathcal{A}(V_\bullet)$ contain the $G_{V_\bullet}$-orbits on $\mathcal{A}(V_\bullet)$, to be precise an equivalence class contains all $G_{V_\bullet}$-orbits whose output sequences differ only on the orbits of length one. It thus allows us to count the number of systems equivalent to some given (P, h) as we illustrate with the next example.

EXAMPLE 4.7. *Let (P, h) be a system with fundamental period $2^n - 1$. Thus $V = V \setminus \{0\} \sqcup \{0\}$ is a decomposition of the vector space V into disjoint minimal orbits. By Theorem 2.2 (P, h) is linearizable. There are $(2^n - 2)!$ possible functions $P : V \longrightarrow V$ with the same fundamental orbits. Thus there are $(2^n - 2)!(2^{2^n} - 4)$ systems (P, h) with an output sequence of fundamental period $2^n - 1$, since we have to subtract the ones with a map h constant on $V \setminus 0$. Moreover each equivalence class of these contains $2(2^n - 1)!$ elements. Thus there are*

$$\frac{(2^n - 2)!(2^{2^n} - 4)}{2(2^n - 1)!} = \frac{2^{2^{n-1}} - 2}{2^n - 1}$$

equivalence classes. For, e.g., $n = 2$ this gives 2 classes represented by the two output sequences

$$0, 0, 1 \quad \text{and } 0, 1, 1.$$

For $n = 3$ we find 18 classes represented by

$$\begin{array}{lll}
0,0,0,0,0,0,1 & 0,0,0,0,0,1,1 & 0,0,0,0,1,0,1 \\
0,0,0,1,0,0,1 & 0,0,0,0,1,1,1 & 0,0,0,1,0,1,1 \\
0,0,1,0,0,1,1 & 0,1,0,0,0,1,1 & 0,0,1,0,1,0,1
\end{array}$$

and their negatives.

5. Normalization: P as a Polynomial Function. In this section we want to present what we want to call the normalization of the system (P, h).

Let (P, h) be a system of period $p = 2^n - 1$, and consider the output sequence

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

where

$$y_i(\mathsf{v}_1) = h(P^{i-1}(\mathsf{v}_1)).$$

Denote by $\widehat{V}$ the n-dimensional vector space over the field with 2^n elements, $\mathbb{F}_{2^n}$. In this section we show how to construct polynomial *functions* F_i

$$F = (F_1, \ldots, F_n) : \widehat{V} \longrightarrow \widehat{V}$$

such that for some some starting value $\mathsf{w}_1 \in \widehat{V}$

$$(*) \qquad y_i = x_n(F^{i-1}(\mathsf{w}_1)).$$

The new system (F, x_n) is called the **normalization** of the system (P, h).

REMARK 5.1. *We pause to explain the difference between polynomials and polynomial functions. A polynomial in n variables over $\mathbb{F}_2$ is of the form*

$$\gamma + \sum_{i=1}^{n} \alpha_i x_i + \sum_{j \neq k} \beta_{jk} x_j x_k,$$

(where $\gamma, \alpha_i,\ \beta_{jk} \in \mathbb{F}_2$) because $a^2 = a$ for any element $a \in \mathbb{F}_2$. In contrast, a polynomial function in n variables over any field $\mathbb{F}$

$$f \in \mathbb{F}[x_1, \dots, x_n],$$

is a polynomial in $\overline{\mathbb{F}}[x_1, \dots, x_n]$ (where $\overline{\mathbb{F}}$ denotes the algebraic closure of $\mathbb{F}$) such that $f(\mathsf{v}) \in V = \mathbb{F}_2^n$ for all $\mathsf{v} \in V$. In particular, if $\mathbb{F} = \mathbb{F}_2$ we have that

$$f(x_1, \dots, x_n)^2 \neq f(x_1, \dots, x_n)$$

as polynomial functions: they take the same values on any $\mathsf{v} \in V = \mathbb{F}_2^n$, but for values from, say, $\mathbb{F}_4^n$ they are different.

PROPOSITION 5.2. *Let (P, h) be a system with periodic output sequence of fundamental period $p = 2^n - 1$ with output sequence $\{y_i(\mathsf{v}_1)\}_{i=1}^{\infty}$. Let $\widehat{V} = \mathbb{F}_{2^n}^n$ be the n-dimensional vector space over the field $\mathbb{F}_{2^n}$. Then there exists a polynomial function*

$$F = (F_1, \dots, F_n) : \widehat{V} \longrightarrow \widehat{V}$$

together with an initial value $\mathsf{w}_1 \in \widehat{V}$ such that the system (F, x_n) has the same output sequence as (P, h).

Proof. Pick $2^n - 1$ pairwise distinct elements $\mathsf{w}'_1, \dots, \mathsf{w}'_{2^n-1}$ in the vector space $\mathbb{F}_{2^n}^{n-1}$. These exist since the order of the vector space is given by

$$|\mathbb{F}_{2^n}^{n-1}| = (2^n)^{n-1} = 2^{n(n-1)} \geq 2^n - 1.$$

Then set

$$\mathsf{w}_i = (\mathsf{w}'_i, y_i) \in \widehat{V}.$$

Then we need that

$$F_j(\mathsf{w}_i) = (\mathsf{w}_{i+1})_j \mod 2^n - 1, \quad \forall j = 1, \dots, n,\ i = 1, \dots, 2^n - 1.$$

These are $2^n - 1$ conditions on the function F_j, for $j = 1, \dots, n$. Thus we need (at least) this many parameters for each F_j. Since the vector space of homogeneous polynomial functions of degree d over any field $\mathbb{F}$ has dimension given by

$$\dim_{\mathbb{F}} \mathbb{F}[V]_{(d)} = \binom{n+d-1}{d},$$

a nonhomogeneous polynomial function of degree d has

$$1+\binom{n}{1}+\binom{n+1}{2}+\cdots+\binom{n+d-1}{d}$$

parameters. Let d_j be the degree of F_j. Thus if

$$(\circ)\qquad 1+\binom{n}{1}+\binom{n+1}{2}+\cdots+\binom{n+d_j-1}{d_j}\geq 2^n-1$$

for all j, there exists a function F as desired. Since two different polynomial functions of degree 2^n-1 have different values already in $\mathbb{F}_{2^n}$ we let $F_1,\ldots,F_n$ have degree

$$d_1=\cdots=d_n=2^n-1.$$

Then the inequality $(\circ)$ is satisfied. By construction the orbit length of F is 2^n-1.□

Remark 5.3. *In the preceding proof we could have chosen the degree d to be smaller. However, $d=2^n-1$ works even when the functions $F_1,\ldots,F_n$ are homogeneous since*

$$\binom{n+2^n-2}{2^n-1}\geq 2^n-1.$$

We illustrate this result with an example.

Example 5.4. *Let $V=\mathbb{F}_2^2$ be the two-dimensional vector space over the field of two elements. Let (P,h) be the system given by*

$$P(x_1,x_2)=(x_1+x_2,x_1)\quad\text{and}\quad h(x_1,x_2)=x_1+x_2.$$

Then the vector space V has two disjoint orbits

$$\{(0,0)\}\quad\text{and}\quad\{(0,1),(1,0),(1,1)\}.$$

The latter has output sequence $1,\ 1,\ 0$. In order to find a suitable F we extend the ground field to $\mathbb{F}_4=\{0,1,\alpha,\alpha^2\}$. Then we set

$$\mathsf{w}_1'=0,\ \mathsf{w}_2'=1,\ \text{and}\ \mathsf{w}_3'=\alpha.$$

Thus

$$\mathsf{w}_1=(0,1),\ \mathsf{w}_2=(1,1),\ \text{and}\ \mathsf{w}_3=(\alpha,0).$$

By our result it is enough to check homogeneous polynomial functions of degree two. We find that the two polynomials

$$F_1(x_1,x_2)=\alpha^2x_1x_2+x_2^2$$
$$F_2(x_1,x_2)=\alpha^2x_1^2+\alpha x_1x_2+x_2^2$$

have an orbit

$$\{(0,1),\ (1,1),\ (\alpha,0)\}$$

with the desired output sequence 1, 1, 0*. In this case we have that*

$$\binom{n+d-1}{d} = 3 = 2^n - 1,$$

i.e., the above solution is unique among homogeneous polynomial functions of degree two. However, if we would allow to use inhomogeneous polynomials of degree two, or polynomials of higher degree, then we would find more polynomial functions F with the required properties.

Thus the disadvantage of the normalization of a system (P, h) is that it is usually not unique, cf. Section 2 where we constructed an equivalent system $(\mathsf{L}, h_{\mathsf{L}})$ with linear invertible generator. However, the following result shows that we can find polynomial functions F for *any* periodic P-orbit structure, cf. Corollary 2.4 where this was not always possible.

THEOREM 5.5. *Let (P, h) be an arbitrary system with l fundamental periodic P-sequences. Then there exists a polynomial function*

$$F = (F_1, \dots, F_n) : \widehat{V} \longrightarrow \widehat{V}$$

together with initial values $\mathsf{w}_{i1} \in \widehat{V}$, $i = 1, \dots, l$, such that the system (F, x_n) has the same periodic output sequences as (P, h).

Proof. Let $\mathbb{F}_{2^n}$ be the field with 2^n elements. By assumption

$$V_1 \cup \cdots \cup V_l \subseteq V$$

Let $|V_i| = s_i$. Thus there are $s = s_1 + \cdots + s_l = |V_1| + \cdots + |V_l| \leq |V| = 2^n$ different elements in these orbits. Pick s pairwise distinct elements $\mathsf{w}'_{1,1}, \dots, \mathsf{w}'_{l,s_l}$ in the vector space $\mathbb{F}_{2^n}^{n-1}$. These exist since the order of the vector space is given by

$$|\mathbb{F}_{2^n}^{n-1}| = (2^n)^{n-1} = 2^{n(n-1)} \geq 2^n \geq s.$$

Then set

$$\mathsf{w}_{i,j_i} = (\mathsf{w}'_{i,j_i}, y_{i,j_i}) \in \widehat{V}.$$

Then we need that

$$F_k(\mathsf{w}_{i,j_i}) = (\mathsf{w}_{i,j_i+1})_k \mod 2^n - 1, \quad \forall k = 1, \dots, n,\ i = 1, \dots, l, j_i = 1, \dots, s_i.$$

These are s conditions on the functions F_k, for $k = 1, \dots, n$. Thus we need (at least) this many parameters for each F_k.

Let d_k be the degree of F_k. As in the preceding result we can find polynomial functions F_k if we choose suitably high degrees. □

6. More on Normalizations. In this section we want to introduce a second method to represent a system (P, h) by polynomial functions. This time we need just two polynomial functions (and not n), but we need to change the vector space once more. We start with an example.

EXAMPLE 6.1. *Assume that* $p = 2^n - 1$ *is prime and let* (P, h) *be a system with fundamental output period* $2^n - 1$. *Let* $\mathbb{F}_p$ *be the prime field with p elements. Let* $\mathbb{F}_p = \{\mathsf{w}'_1, \ldots, \mathsf{w}'_p\}$. *Set* $\mathsf{w}_i = (\mathsf{w}'_i, y_i) \in \mathbb{F}_p^2$ *for* $i = 1, \ldots, p$. *We need two polynomial functions* F_1 *and* F_2 *on* $\mathbb{F}_p^2$ *such that*

$$\begin{aligned} F_1(\mathsf{w}'_i, y_i) &= \mathsf{w}'_{i+1}, \text{ and} \\ F_2(\mathsf{w}'_i, y_i) &= y_{i+1}. \end{aligned}$$

This gives $2^n - 1$ *conditions for both functions. If we assume that* F_1 *and* F_2 *are homogeneous then there is exactly one solution to this problem if* $\deg(F_1) = \deg(F_2) = 2^n - 2$. *(If the degrees are larger there are of course more than one solution.)*

So, again we simulate the system (P, h) *by polynomial functions. The advantage here is that we need only two functions. The disadvantage is that even though the output is again a string of zeros and ones, the input is not a vector in* $\mathbb{F}_2^n$ *but in* $\mathbb{F}_p^2$.

Denote by $\widetilde{V} = \mathbb{F}_{2^n}^2$ the vector space of dimension two over $\mathbb{F}_{2^n}$.

THEOREM 6.2. *Let* (P, h) *be an arbitrary system with l fundamental periodic P-sequences. Then there exists a polynomial function*

$$F = (F_1, F_2) : \widetilde{V} \longrightarrow \widetilde{V}$$

together with initial values $\mathsf{w}_{i1} \in \widetilde{V}$, $i = 1, \ldots, l$, *such that the system* (F, x_n) *has the same periodic output sequences as* (P, h).

Proof. Let $V_1, \ldots, V_l \subseteq V$ be the periodic P-sequences of length s_i, $i = 1, \ldots, l$. Denote by $s = s_1 + \cdots + s_l$. Then choose s different elements $\mathsf{w}'_{i,j_i} \in \mathbb{F}_{2^n}$ for $i = 1, \ldots l$, $j_i = 1, \ldots, s_i$. (Note that $s \leq 2^n$.) Let y_{i,j_i} be the j_ith output of sequence i. Then set

$$\mathsf{w}_{i,j_i} = (\mathsf{w}'_{i,j_i}, y_{i,j_i}).$$

We obtain the following s conditions on the polynomial functions F_1 and F_2

$$\begin{aligned} F_1(\mathsf{w}'_{i,j_i}, y_{i,j_i}) &= \mathsf{w}'_{i,j_i+1}, \text{ and} \\ F_2(\mathsf{w}'_{i,j_i}, y_{i,j_i}) &= y_{i,j_i+1}. \end{aligned}$$

As in the example above there is a solution to this system of equations for suitably high degree polynomials F_1 and F_2.

□

REFERENCES

[1] D. Aeyels, *Global observability of Morse-Smale vector fields*, J. Differential Equations, 45:1(1982), pp. 1–15.

[2] Z. Balogh, H. Bennett, and C. F. Martin, *On the observability of ergodic flows on abelian groups with characteristic functions*, Proceedings of the Guilford College Sesquicentennial Topology Conference, 1988 (Greensboro, NC, 1988), 31–35, Guilford College, Greensboro, NC, 1988

[3] C. I. Byrnes and C. F. Martin, *An integral-invariance principle for nonlinear systems*, IEEE Trans. Automat. Control, 40:6(1995), pp. 983–994.

[4] D. Cheng, W. P. Dayawansa, and C. F. Martin, *Observability of systems on Lie groups and coset spaces*, SIAM J. Control Optim., 28:3(1990), pp. 570–581.

[5] W. P. Dayawansa and C. F. Martin, Observing linear dynamics with polynomial output functions. Systems Control Lett., 9:2(1987), pp. 141–148.

[6] L. Drager and C. F. Martin, *Global observability of a class of nonlinear discrete time systems*, Systems Control Lett., 6:1(1985), pp. 65–68.

[7] R. J. Elliott, L. Aggoun, and J. B. Moore, *Hidden Markov models. Estimation and control. Applications of Mathematics* (New York), 29. Springer-Verlag, New York, 1995. xii+361 pp. ISBN: 0-387-94364-1

[8] D. S. Gilliam and C. F. Martin, *Discrete observability and Dirichlet series*, Systems Control Lett., 9:4(1987), pp. 345–348.

[9] D. Jungnickel, *Finite Fields*, BI Wissenschaftsverlag, Mannheim Leipzig Wien 1993.

[10] B. Huppert, *Endliche Gruppen I*, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen Band 134, Springer Verlag, Berlin Heidelberg New York 1967.

[11] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, Cambridge 2000.

[12] C. F. Martin and J. Miller, *Discrete observability of nonlinear systems using continuation techniques*, Appl. Math. Comput., 44:3(1991), pp. 241–248.

[13] C. F. Martin and M. Stamp, *Classification and realization of pseudo-random number generators*, Systems Control Lett., 14:2(1990), pp. 169–175.

[14] C. F. Martin and M. Stamp, *Constructing polynomials over finite fields, Computation and control* (Bozeman, MT, 1988), pp. 233–252 in: Progr. Systems Control Theory, 1, Birkhäuser, Boston MA, 1989.

[15] C. F. Martin and M. Stamp, *An algorithm for the k-error linear complexity of binary sequences with period* 2^n, IEEE Trans. Inform. Theory, 39:4(1993), pp. 1398–1401.

[16] C. F. Martin and M. D. Neusel, *Invariants of Pseudo-Random Number Generators II*, in preparation.

[17] M. D. Neusel, *Invariant Theory*, AMS, Providence RI 2007.