Monomial Dynamical Systems over Finite Fields

Omar Colón-Reyes[*]
Mathematics Department,
University of Puerto Rico at Mayagüez,
Mayagüez, PR 00681

Abdul Salam Jarrah[†]
Reinhard Laubenbacher[‡]
Virginia Bioinformatics Institute,
Virginia Tech,
Blacksburg, VA 24061-0477, USA

Bernd Sturmfels[§]
Department of Mathematics,
University of California at Berkeley,
Berkeley, CA 94720, USA

An important problem in the theory of finite dynamical systems is to link the structure of a system with its dynamics. This paper contains such a link for a family of nonlinear systems over an arbitrary finite field. For systems that can be described by monomials, information about the limit cycle structure can be obtained from the structure of the monomials. In particular, the paper contains a sufficient condition for a monomial system to have only fixed points as limit cycles. The condition is derived by reducing the problem to the study of a boolean monomial system and a linear system over a finite ring.

1. Introduction

Finite dynamical systems are time-discrete dynamical systems on finite state sets. Well-known examples include cellular automata and boolean networks, which have found broad applications in engineering, computer science, and, more recently, computational biology. (See, e.g., [1–4] for biological applications.) More general multistate systems have been used in control theory [5–8] and in the design and analysis of computer simulations [9–12]. One underlying mathematical question that is common to many of these applications is: How can we analyze

Electronic mail addresses: [*]ocolon@math.uprm.edu, [†]ajarrah@vbi.vt.edu, [‡]reinhard@vbi.vt.edu, [§]bernd@math.berkeley.edu.

the dynamics of the models without actually enumerating all state transitions, since enumeration has exponential complexity in the number of model variables? The present paper is a contribution toward an answer to this question.

For our purposes, a finite dynamical system is a function $f : X \longrightarrow X$, where X is a finite set [13]. The dynamics of f are generated by iteration of f and are encoded in its *phase space* $\mathcal{S}(f)$, which is a directed graph defined as follows. The vertices of $\mathcal{S}(f)$ are the elements of X. There is a directed edge $a \to b$ in $\mathcal{S}(f)$ if $f(a) = b$. In particular, a directed edge from a vertex to itself is admissible. That is, $\mathcal{S}(f)$ encodes all state transitions of f, and has the property that every vertex has out-degree exactly equal to 1. Each connected graph component of $\mathcal{S}(f)$ consists of a directed cycle, a so-called *limit cycle*, with a directed tree attached to each vertex in the cycle, consisting of the so-called *transients*.

Any boolean network can be viewed as a finite dynamical system $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$, where $\mathbb{F}_2$ is the finite field on two elements and $n \geq 1$. In this paper, we study finite dynamical systems $f : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$, where $\mathbb{F}_q$ is any finite field and $|\mathbb{F}_q| = q$. To be precise, we present a family of nonlinear finite systems for which the above question can be answered, that is, we can obtain information about the dynamics from the structure of the function.

Let $f : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$, $n \geq 1$ be a finite dynamical system. Observe that f can be described in terms of its coordinate functions $f_i : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$, that is, $f = (f_1, \ldots, f_n)$. It is well known that any set-theoretic function $g : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ can be represented by a polynomial in $\mathbb{F}_q[x_1, \ldots, x_n]$, see [14, pp. 369]. This polynomial can be chosen uniquely so that any variable in it appears to a degree less than q. That is, for any g there is a unique $\bar{h} \in \mathbb{F}_q[x_1, \ldots, x_n]/\langle x_i^q - x_i | i = 1, \ldots, n\rangle$, such that $g(a) = h(a)$ for all $a \in \mathbb{F}_q^n$. Consequently, any finite dynamical system over a finite field can be represented as a polynomial system. This is the point of view we take in this paper.

In the case that all the f_i are linear polynomials without a constant term, the dynamics of the *linear system* f can completely be determined from its matrix representation [15]. Let A be a matrix representation of a linear system $f : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$. Then the number of limit cycles and their length, as well as the structure of the transients, can be determined from the factorization of the characteristic polynomial of the matrix A. The structure of the limit cycles had been determined earlier by Elspas [16], and for affine systems by Milligan and Wilson [17].

In this paper we focus on the class of nonlinear systems described by special types of polynomials, namely *monomials*. That is, we consider systems $f = (f_i)$, so that each f_i is a polynomial of the form $x_{i_1}^{a_{i1}} x_{i_2}^{a_{i2}} \ldots x_{i_r}^{a_{ir}}$, or a constant. Without loss of generality we can assume that no coordinate function is constant, since the general case is easily reduced to this.

Some classes of monomial systems and their dynamic behavior have been studied before: monomial cellular automata [18, 19], boolean monomial systems [20], monomial systems over the p-adic numbers [21, 22], and monomial systems over finite fields [23, 24].

In [20] a special class of boolean monomial systems was studied, namely those which have only fixed points as limit cycles, so-called *fixed point systems*. The motivation for considering this class is the use of polynomial systems as models for biochemical networks. Depending on the experimental system considered, such networks often exhibit steady state dynamics. That is, their dynamic models have phase spaces whose limit cycles are fixed points. For the purpose of model selection it would be useful to have a structural criterion to recognize fixed point systems. The main result of the present paper is to reduce this question for monomial systems over a general finite field $\mathbb{F}_q$ to the same question for an associated boolean monomial system and a linear system over a ring of the form $\mathbb{Z}/(q-1)$.

2. Reduction of monomial systems

Let $f = (f_1, \ldots, f_n) : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ be a polynomial system, with each f_i a monomial, that is, $f_i = x_1^{a_{i1}} x_2^{a_{i2}} \ldots x_n^{a_{in}}$, with a_{ij} a nonnegative integer. That is, f can be described by the exponent matrix $A = (a_{ij})$. We first associate with f a boolean monomial system $T(f)$ and a linear system $L(f)$ over the ring $R = \mathbb{Z}/(q-1)$. Recall from [20] that f is called a fixed point system if all limit cycles of f consist of a fixed point. We will show that f is a fixed point system if and only if $T(f)$ and $L(f)$ are fixed point systems.

Definition 1. For $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$, we define support $\mathbf{u}$, denoted by $\mathrm{supp}(\mathbf{u})$, to be $\mathbf{v} = (v_1, \ldots, v_n)$, where

$$v_i = \begin{cases} 1 & \text{if } u_i \neq 0; \\ 0 & \text{if } u_i = 0. \end{cases}$$

The monomial system $f = (f_1, \ldots, f_n)$ induces a boolean monomial system $T(f) = (g_1, \ldots, g_n)$ on $\mathbb{F}_2^n$ by setting $g_i = x_1^{v_{i1}} \ldots x_n^{v_{in}}$, where $f_i = x_1^{u_{i1}} \ldots x_n^{u_{in}}$ and $\mathbf{v} = \mathrm{supp}(\mathbf{u})$.

Lemma 1. There is a commutative diagram

$$\begin{array}{ccc} \mathbb{F}_q^n & \xrightarrow{f} & \mathbb{F}_q^n \\ \downarrow & & \downarrow \\ \mathbb{F}_2^n & \xrightarrow{T(f)} & \mathbb{F}_2^n \end{array}$$

Proof. The proof is a straightforward verification, since

$$\mathrm{supp}(f(\mathbf{u})) = f(\mathrm{supp}(\mathbf{u})). \blacksquare$$

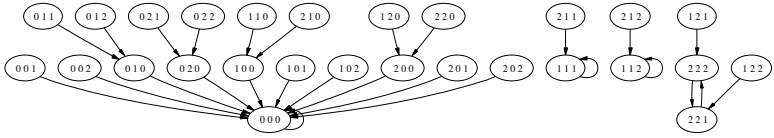

Figure 1. The phase space of f.

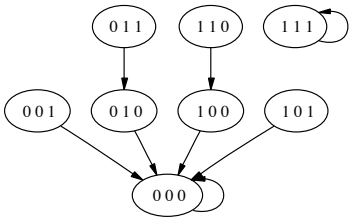

Figure 2. The phase space of $T(f)$.

Since $f = T(f)$ on the set of all $\mathbf{u}$ such that $\mathrm{supp}(\mathbf{u}) = \mathbf{u}$, the following corollaries are straightforward.

Corollary 1. The phase space of $T(f)$ is a subgraph of the phase space of f.

Corollary 2. Suppose that $T(f)$ is a fixed-point system. If $\{\mathbf{u}, f(\mathbf{u}), \ldots, f^t(\mathbf{u}) = \mathbf{u}\}$ is a cycle in the phase space of f, then $\mathrm{supp}(\mathbf{u}) = \mathrm{supp}(f^i(\mathbf{u}))$ for all $1 \leq i \leq t$.

For more results in this direction, see [23].

Example 1. Let

$$f = (x_1^2x_2, x_2x_3^2, x_1^2x_2x_3) : \mathbb{F}_3^3 \longrightarrow \mathbb{F}_3^3.$$

Figures 1 and 2 display the phase spaces of the system f and its "booleanization" $T(f)$, respectively.

Next we associate to f an n-dimensional linear system over a finite ring. Observe first that $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$ is isomorphic, as an abelian group, to $\mathbb{Z}/(q-1)$ *via* an isomorphism

$$\log : \mathbb{F}_q^* \longrightarrow \mathbb{Z}/(q-1),$$

given by the choice of a generator for the cyclic group $\mathbb{F}_q^*$. Note first that the set of vectors $\mathbf{u} \in \mathbb{F}_q^n$ with all nonzero entries is invariant under f.

Let α be a generator for the cyclic group $\mathbb{F}_q^* \cong \mathbb{Z}/(q-1)$, and let

$$\mathbf{u} = (u_1, \ldots, u_n) = (\alpha^{s_1}, \ldots, \alpha^{s_n}) = \alpha^{\mathbf{s}}.$$

Then $f(\mathbf{u}) = f(\alpha^{\mathbf{s}}) = \alpha^{A \cdot \mathbf{s}}$.

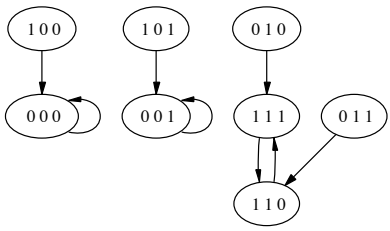

Figure 3. The phase space of $L(f)$.

Definition 2. Define $L(f) : (\mathbb{Z}/(q-1))^n \longrightarrow (\mathbb{Z}/(q-1))^n$ by

$$L(f)(\alpha^{\mathbf{s}}) = \alpha^{A\cdot\mathbf{s}}.$$

As defined, $L(f)$ is a linear transformation of $\mathbb{Z}$-modules. But we can consider it as a linear transformation of $\mathbb{Z}/(q-1)$-modules, viewing $\mathbb{Z}/(q-1)$ as a (finite) ring, which we denote by R. That is, we have the linear transformation

$$L(f) = A : R^n \longrightarrow R^n.$$

The proof of the following lemma is a straightforward verification.

Lemma 2. There is a commutative diagram

$$\begin{array}{ccc} (\mathbb{F}_q^*)^n & \xrightarrow{f} & (\mathbb{F}_q^*)^n \\ \downarrow & & \downarrow \\ R^n & \xrightarrow{L(f)} & R^n \end{array}$$

Note that the vertical arrows are isomorphisms. This implies that they preserve the phase space structure, including the length of limit cycles [13]. In particular, we have the following corollary.

Corollary 3. The phase space of $L(f)$ is isomorphic to the subgraph of the phase space of f consisting of all states with support vector $(1, 1, \ldots, 1)$.

Example 2. For the monomial system f in Example 1, $L(f) : (\mathbb{Z}/2)^3 \longrightarrow (\mathbb{Z}/2)^3$ is defined by $L(f)(\mathbf{s}) = A \cdot \mathbf{s}$, where

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

The phase space of $L(f)$ is given in Figure 3.

We now come to the main result of this section.

Theorem 1. Let $f : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ be a monomial dynamical system. Then f is a fixed point system if and only if $T(f)$ and $L(f)$ are fixed point systems.

Proof. From Corollaries 1 and 3, if f is a fixed point system, then so are $T(f)$ and $L(f)$. For the converse, we assume that $L(f)$ and $T(f)$ are fixed point systems, but f is not. For each limit cycle of f, either all states involved have all coordinates nonzero, or all states involved have at least one zero coordinate. In the first case it follows that $L(f)$ has a limit cycle of the same length. Hence, if f has a limit cycle of length greater than 1, then it can involve only states with at least one zero coordinate.

Let $\mathbf{a}_1, \ldots, \mathbf{a}_t$ be the states in the limit cycle. Since this limit cycle has to project to a fixed point of $T(f)$ it follows that the $\mathbf{a}_i$ have the same support vector, that is, the same pattern of zero entries, and differ only in the nonzero coordinates. Furthermore, the monomials in the nonzero coordinates do not involve any variables corresponding to zero coordinates. Thus, if we construct new states $\mathbf{b}_i$ by replacing each 0 in $\mathbf{a}_i$ by a 1, the $\mathbf{b}_i$ will be part of a limit cycle of length at least t, which is a contradiction. This completes the proof of the theorem. ■

3. Linear systems over finite commutative rings

Theorem 1 shows that to decide if a given monomial system f, over a finite field $\mathbb{F}_q$, is a fixed point system it is sufficient to decide this question for an associated boolean system, for which a criterion has been developed in [20], and a certain linear system over a finite ring $\mathbb{Z}/m$. It therefore remains to develop a criterion for linear systems over finite commutative rings that helps decide if the system is a fixed point system. Here we reduce the case of a general $\mathbb{Z}/m$ to that of m being a prime power.

Let $m = st$ for relatively prime integers s and t, and let f be a linear system over $\mathbb{Z}/m$ of dimension n. Choosing an isomorphism $\mathbb{Z}/m \cong \mathbb{Z}/s \times \mathbb{Z}/t$ we see that f is isomorphic to a product

$$g \times h : (\mathbb{Z}/s)^n \times (\mathbb{Z}/t)^n \longrightarrow (\mathbb{Z}/s)^n \times (\mathbb{Z}/t)^n,$$

where g and h are linear systems over $\mathbb{Z}/s$ and $\mathbb{Z}/t$, respectively. Using the fact that the phase space of f is then the direct product, as directed graphs, of the phase spaces of g and h (e.g., [15] or [25]), we obtain the following result.

Proposition 1. Let $m = st$ for relatively prime integers s and t, and let f be a linear system over $\mathbb{Z}/m$ of dimension n. Let g and h be the induced linear transformations over $\mathbb{Z}/s$ and $\mathbb{Z}/t$, respectively. Then f is a fixed point system if and only if g and h are fixed point systems.

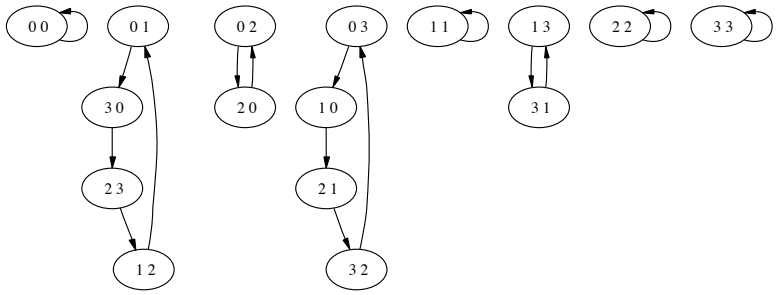

Figure 4. The phase space of f.

For the purpose of developing a criterion to recognize fixed point systems it is therefore sufficient to study linear systems over rings of the form $\mathbb{Z}/p^r$ for primes p. The following theorem provides a criterion for a further reduction of the problem to a linear system over the prime field $\mathbb{Z}/p$.

Theorem 2. Let $f = (f_1, \ldots, f_n) : (\mathbb{Z}/p^r)^n \longrightarrow (\mathbb{Z}/p^r)^n$ be a linear map, and let g be the projection map of f on $\mathbb{Z}/p$. That is $g = (g_1, \ldots, g_n) : (\mathbb{Z}/p)^n \longrightarrow (\mathbb{Z}/p)^n$, where $g_i = f_i \bmod p$. Then the phase space of g is isomorphic to a subgraph of the phase space of f.

Proof. Let $\sigma : (\mathbb{Z}/p)^n \longrightarrow (\mathbb{Z}/p^r)^n$ be given by

$$\sigma(\mathbf{a}) = \sigma(a_1, \ldots, a_n) = (a_1 p^{r-1}, \ldots, a_n p^{r-1}) = \mathbf{a}p^{r-1}.$$

Then it is easy to check that $\sigma \circ g = f \circ \sigma$, since the f_i are linear maps for all i. Therefore, it is straightforward to check that $g(\mathbf{a}) = \mathbf{b}$ if and only if $f(\mathbf{a}p^{r-1}) = \mathbf{b}p^{r-1}$, and hence the phase space of g is isomorphic to a subgraph of the phase space of f. ■

Corollary 4. Let f and g be as given in Theorem 2. If g is not a fixed point system, then f is not a fixed point system.

The dynamics of projection maps have been studied in [23].

Example 3. Let $f : (\mathbb{Z}/4)^2 \longrightarrow (\mathbb{Z}/4)^2$ be given by $f = (2x_1 + 3x_2, x_1)$. Then $g = (x_2, x_1) : (\mathbb{Z}/2)^2 \longrightarrow (\mathbb{Z}/2)^2$. The phase spaces of f and g are in Figures 4 and 5, respectively.

It remains to study the dynamics of linear systems over finite rings, in particular to find a criterion for a linear system to be a fixed point system. Together with the results in this paper, such a criterion would provide an algorithm for deciding if a monomial system over an arbitrary finite field is a fixed point system. However, it appears to be a difficult problem to understand the dynamics of linear systems even over rings of

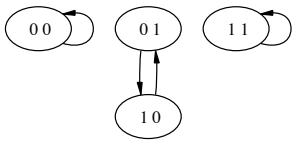

Figure 5. The phase space of g.

the form $\mathbb{Z}/p^r$, due to the lack of unique factorization in the polynomial ring $\mathbb{Z}/p^r[x]$. See, for example, [26].

Acknowledgments

The second and third authors were supported in part by NSF Grant Nr. DMS-0511441. The third author was also partially supported by NIH Grant Nr. RO1 GM068947-04.

References

[1] S. Kauffman, "Metabolic Stability and Epigenesis in Randomly Constructed Genetic Nets," *Journal of Theoretical Biology*, **22** (1969) 437–467.

[2] R. Albert and H. Othmer, "The Topology of the Regulatory Interactions Predicts the Expression Pattern of the Segment Polarity Genes in *Drosophila melanogaster*," *Journal of Theoretical Biology*, **223** (2003) 1–18.

[3] F. Celada and P. Seiden, "A Computer Model of Cellular Interactions in the Immune System," *Immunology Today*, **13** (1992) 56–62.

[4] R. Laubenbacher and B. Stigler, "A Computational Algebra Approach to the Reverse-Engineering of Gene Regulatory Networks," *Journal of Theoretical Biology*, **229** (2004) 523–537.

[5] R. Germundsson, J. Gunnarsson, and J. Plantin, "Symbolic Algebraic Discrete Systems—Applied to the JAS39 Fighter Aircraft," Technical Report, Linköping University, Linköping, Sweden, December 1994.

[6] M. LeBorgne, A. Benveniste, and P. LeGuernic, "Polynomial Dynamical Systems over Finite Fields," in *Algebraic Computing in Control*, edited by G. Jacob and F. Lamnabhi-Lagarrigue, Volume 165 of *Lecture Notes in Control and Information Sciences* (Springer, New York, 1991).

[7] H. Marchand and M. LeBorgne, "On the Optimal Control of Polynomial Dynamical Systems over $\mathbb{Z}/p\mathbb{Z}$," in *Proceedings of the Fourth Workshop on Discrete Event Systems*, IEEE, Cagliari, Italy, 1998.

[8] ———, "Partial Order Control of Discrete Event Systems Modeled as Polynomial Dynamical Systems," in *IEEE International Conference on Control Applications*, Trieste, Italy, 1998.

[9] C. Barrett and C. Reidys, "Elements of a Theory of Computer Simulation, I: Sequential CA over Random Graphs," *Applied Mathematics and Computation*, **98** (1999) 241–259.

[10] C. Barrett, H. Mortveit, and C. Reidys, "Elements of a Theory of Computer Simulation, II: Sequential Dynamical Systems," *Applied Mathematics and Computation*, **107** (2000) 121–136.

[11] ———, "Elements of a Theory of Computer Simulation, III: Equivalence of SDS," *Applied Mathematics and Computation*, **122** (2001) 325–340.

[12] R. Laubenbacher and B. Pareigis, "Decomposition and Simulation of Sequential Dynamical Systems," *Advances in Applied Mathematics*, **30** (2003) 655–678.

[13] ———, "Equivalence Relations on Finite Dynamical Systems," *Advances in Applied Mathematics*, **26** (2001) 237–251.

[14] R. Lidl and H. Niederreiter, *Finite Fields* (Cambridge University Press, New York, 1997).

[15] A. Hernández-Toledo, "Linear Finite Dynamical Systems," *Communications in Algebra*, **33** (2005) 2977–2989.

[16] B. Elspas, "The Theory of Autonomous Linear Sequential Networks," *IRE Transactions on Circuit Theory*, **6**(1) (1959) 45–60.

[17] D. Milligan and M. Wilson, "The Behavior of Affine Boolean Sequential Networks," *Connection Science*, **5** (1993) 153–167.

[18] R. Bartlett and M. Garzon, "Monomial Cellular Automata," *Complex Systems*, **7** (1993) 367–388.

[19] J. Kari, "Theory of Cellular Automata: A Survey," *Theoretical Computer Science*, **334** (2005) 3–33.

[20] O. Colón-Reyes, R. Laubenbacher, and B. Pareigis, "Boolean Monomial Dynamical Systems," *Annals of Combinatorics*, **8** (2004) 425–439.

[21] A. Khrennikov and M. Nilsson, "On the Number of Cycles of p-adic Dynamical Systems," *Journal of Number Theory*, **90** (2001) 255–264.

[22] M. Nilsson, "Fuzzy Cycles in Monomial Dynamical Systems," *Far East Journal of Dynamical Systems*, **5** (2003) 149–173.

[23] O. Colón-Reyes, "Monomial Dyanmical Systems over Finite Fields," Ph.D. Thesis, Virginia Tech, 2005.

[24] T. Vasiga and J. Shallit, "On the Iteration of Certain Quadratic Maps over GF(p)," *Discrete Mathematics*, **277** (2004) 219–240.

[25] A. Jarrah, R. Laubenbacher, and P. Vera-Licona, "An Efficient Algorithm for the Phase Space Structure of Linear Dynamical Systems over Finite Fields," Preprint, 2006.

[26] W. Brown, *Matrices over Commutative Rings* (M. Dekker, New York, 1993).