DOI: 10.15415/mjis.2012.11008

Monomial Dynamical Systems in # P-complete

Jang-Woo Park
School of Arts & Sciences, University of Houston - Victoria,
Victoria, TX 77901, USA
Email: parkj1@uhv.edu

Shuhong Gao
Department of Mathematical Sciences, Clemson University,
Clemson, SC 29634-0975, USA
Email: sgao@math.clemson.edu

Abstract

In this paper, we study boolean monomial dynamical systems. Colón-Reyes, Jarrah, Laubenbacher, and Sturmfels(2006) studied fixed point structure of boolean monomial dynamical systems of f by associating the dynamical systems of f with its dependency graph χ_f and Jarrah, Laubenbacher, and Veliz-Cuba(2010) extended it and presented lower and upper bound for the number of cycles of a given length for general boolean monomial dynamics. But, it is even difficult to determine the exact number of fixed points of boolean monomial dynamics. We show that the problem of counting fixed points of a boolean monomial dynamical systems is #P-complete, for which no efficient algorithm is known. This is proved by a 1-1 correspondence between fixed points of f sand antichains of the poset of strongly connected components of χf..

1 INTRODUCTION

A dynamical system consists of a set V and a map $f : V \to V$. For any point $v \in V$, we can iterate f by defining $f^0(v) = v.$ and $f^i(v) = f(f^{i-1}(v))$ for $i \geq 1$. The **orbit of** v under f is the set of $f^i(v)$'s for all $i \geq 0$. A point $v \in V$ is called **periodic** or **cyclic** if there exists $m \geq 1$ such that $f^m(v) = v$, and such a minimum is called the **cycle length** of v under f. A point v is called **preperiodic** if the orbit of v is finite. In this case, the orbit of v contains a cycle, and the tail length of v is the smallest n such that $f^n(v)$ is cyclic.

In a classical dynamical system, V is a topological and metric space. A point $v \in V$ is called stable if, whenever $u \in V$ is "close" to v, the orbit of u stays "close" to that of v. The Fatou set of f consists of all the stable points of V and the Julia set of f is the complement of the Fatou set. So points in Julia set tend to move away from each other under iteration of f and they behave chaotically. In a classical dynamical system, it is important to understand the limiting behaviors of orbits and to characterize the Julia set. For more on classical dynamical system, we recommend (Devaney, 2003) and (Robinson, 1998).

Understanding dynamical systems on finite sets requires different techniques. When V is finite, every point is preperiodic. So the "stability" and "chaos" in classical dynamical systems are irrelevant in finite dynamical

Mathematical Journal of
Interdisciplinary Sciences
Vol. 1, No. 1,
July 2012
pp. 87–94

systems. We view a discrete dynamical system of f on a finite set V as a directed graph. The graph has V as a vertex set and, for any pair of $v, w \in V$, there is an edge from v to w if and only if $f(v) = w$. Then the graph consists of a collection of cycles with each node on the cycles having a tree. We are interested in understanding the distribution of the cycle lengths and the tree structures.

Although one can get answers for all the questions above by enumerating all points, we are interested in the underlying mathematical theory. The goal is to analyze the dynamics without actually enumerating all state transitions, since enumerating has exponential complexity in the number of model variables. For dynamical systems over finite fields, there are only a few cases that have been studied completely so far. For linear dynamical systems, Elspas (1959) examined the dynamics of linear systems over prime fields and showed that cycle structure can be determined by the elementary divisor of the matrix, and Hernandez (2005) generalized Elspas' results to arbitrary finite fields and also showed that tree structure can be determined by the nilpotent part of the map. Based on these results, Jarrah, Laubenbacher, and Vera-Licona (2006) presented an algorithms which describes the phase spaces. Xua and Zoub (2009) have presented an efficient algorithm to analyze cycle structure of the dynamics of linear systems over finite commutative rings. Studying dynamics of nonlinear maps is very challenging task. Only a few cases have been well understood. Barta and Morton (1994) studied the dynamics of certain types of polynomials over algebraic closure of finite fields. Zieve (1996) investigated the cycle lengths of polynomial maps over various rings. Even dynamics of quadratic polynomials over finite fields are still open except $f(x) = x^2$ and $f(x) = x^2 - 2$. The square map over prime fields was studied in (Roger, 1996) and the dynamics of $f(x) = x^2 - 2$ over prime fields was analyzed in (Gilbert, Kolesar, Reiter, and Stroey, 2001), (Park, 2003), and (Vasiga and Shallit, 2004). For monomial dynamics, Jarrah, Laubenbacher, and Veliz-Cuba (2010) provided an analysis of boolean monomial dynamical systems and Colón-Reyes, Jarrah, Laubenbacher, and Sturmfels (2006) showed that the structure of fixed points of monomial dynamics over general finite fields can be reduced to boolean monomial dynamics. They also provided a polynomial-time algorithm for determining if every cycle in a boolean monomial dynamical system is a steady state. Just (2003) showed that the corresponding problem is NP-hard if functions in a boolean dynamical system are quadratic monotone functions.

In this paper, we study boolean monomial dynamical systems. Colón-Reyes, Jarrah, Laubennacher, and Sturmfels (2006) studied fixed point structure of f over $\mathbf{F}_2$ by associating the dynamics of f with its dependency graph χ_f and Jarrah, Laubenbacher, and Veliz-Cuba (2010) extended it and presented lower and upper bound for the number of cycles of a given length for general boolean monomial dynamics. But, it is even difficult to determine the exact number of fixed points of boolean monomial dynamics. We show that the problem of counting fixed points of a monomial dynamics over $\mathbf{F}_2$ is #P-complete, for which no efficient algorithm is known.

2 MONOMIAL DYNAMICAL SYSTEMS

Let $V = \mathbf{F}_q^n$ and the map $f : \mathbf{F}_q^n \to \mathbf{F}_q^n$ is defined by

$$f = (f_1, f_2, \ldots, f_n)$$

where

$$f_i = c_i \cdot x_1^{m_{i1}} x_2^{m_{i2}} \cdots x_n^{m_{in}}, \quad 1 \le i \le n,$$

with $c_i \in \mathbf{F}_q$ and $m_{ij} \in \mathbf{N}$. Then f is called a monomial map over $\mathbf{F}_q$ and the dynamics f a **monomial dynamics**.

Since our work extends that of (Colón-Reyes, Jarrah, Laubennacher, and Sturmfels, 2006) and (Jarrah, Laubenbacher, and Veliz-Cuba, 2010), we will use their definitions and basic setup in most of cases. We associate f with a digraph χ_f, called the **dependency graph of** f which has vertex set $\{1, 2, \ldots, n\}$, and there is a directed edge from j to i if and only if $c_i \neq 0$ and $x_j \mid f_i$. Note that j is adjacent to i if and only if the value of χ_j affects f_i and we allow self-loops in χ_f.

Example 2.1 Let f be defined over $\mathbf{F}_2$ as

$$f = (x_2, x_3 x_4, x_2, x_5 x_{12}, x_6, c, x_8 x_{11}, x_3 x_9, x_{10}, x_6, x_9, x_{12})$$

where c in $\mathbf{F}_2$. The dependency graph χ_f of f is as follows:

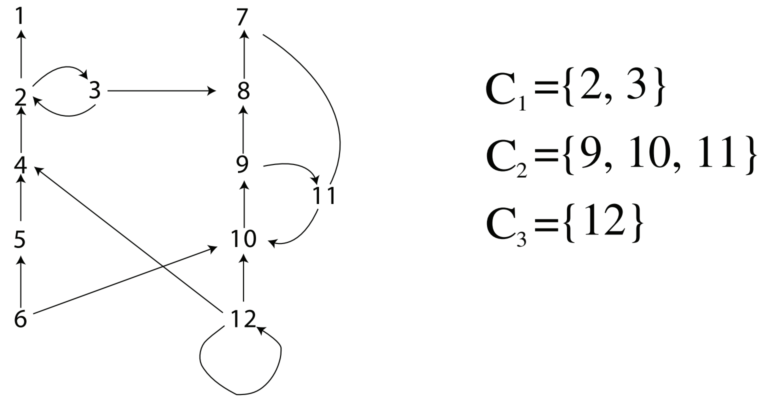

Figure 1: Dependency Graph χ_f of f and its Strongly Connected Components

When $c = 1$, the fixed points of f are :

$$(1,1,1,1,1,1,1,1,1,1,1,1),$$
$$(0,0,0,1,1,1,0,0,1,1,1,1),$$
$$(1,1,1,1,1,1,0,0,0,0,0,1),$$
$$(0,0,0,0,1,1,0,0,0,0,0,0),$$
$$(0,0,0,1,1,1,0,0,0,0,0,1).$$

When $c = 0$, the fixed points of f are :

$$(0,0,0,0,0,0,0,0,0,0,0,0),$$
$$(0,0,0,0,0,0,0,0,0,0,0,1).$$

Let χ be any digraph. For any two vertices $i, j \in \chi$, if there is a **directed path**, or **dipath** for short, from i to j and a dipath from j to i then we say i and j are **strongly connected**. A subset of vertices is called strongly connected if each pair of vertices in the subset is strongly connected. Any maximal strongly connected subset of vertices of χ is called a **strongly connected component** of χ, or simply a **component** of χ. Note that a vertex itself is a component if and only if it has a self-loop.

Note that different components of χ have disjoint vertices, and there may be vertices in χ that do not lie on any component. For any vertex i not on any component, either there is a dipath from i to some component or there is a dipath from some component to i, but not both. Similary, for any two components, if there are paths for one component to the other, then there is no path going to the opposite direction. We say a component C_1 is above, or greater than, another component C_2 if there is a dipath from C_2 to C_1. This makes the set of all the components of χ into a **partially ordered set**, i.e., a **poset**.

Example 2.1.(revisited) *Suppose that we have the dependency graph χ_f as in Figure. Then, for ,c = 1 the poset is as in Figure.*

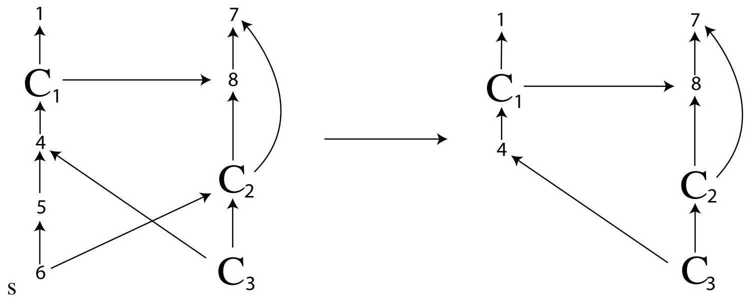

Figure 2: Poset of the Dependency Graph χ_f

Let G be a set. A partial order is a binary relation ‘‘$\leq$" over G which satisfies reflexive, antisymmetric, and transitive. With a partial order, G is called a partially ordered set. A pair of elements x and y in G are comparable if $x \leq y$ or $y \leq x$. A subset A of G is called an **antichain** if no two elements in A are comparable. Note that the empty subset is an antichain and any singleton subset is an antichain as well.

Example 2.2 Suppose that G is as below:

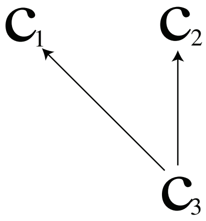

Figure 3: Poset of the Strongly Connected Components of χ_f

Then all the possible antichains of G are:

$$\varnothing, \{C_1\}, \{C_2\}, \{C_3\}, \text{and } \{C_1, C_2\}.$$

Note that G in Figure 2.2 is obtained from the poset of the dependency graph χ_f in Figure 2 by considering only components. For a given dependency graph χ_f of f, we define G_f as the poset of strongly connected components in χ_f and we call G_f the **component poset** of χ_f. Let A be a subset of a partially ordered set G. A is **upper closed** if for any $x \in A$ and $y \in G$, $x \leq y$ implies that $y \in A$ too. Similarly, A is **lower closed** if for any $x \in A$ and $y \in G$, $x \geq y$ implies that $y \in A$ too. Let k be an arbitrary field. For any point $P = (a_1, a_2, \ldots, a_n) \in k^n$, we define subsets $S_0(P)$ and $S_1(P)$ of χ_f as

$$S_0(P) = \{1 \leq i \leq n : a_i = 0\},\ \ {}_1(P) = \{1 \leq i \leq n : a_i \neq 0\}.$$

Then fixed points of monomial dynamics have the following unique property.

Proposition 2.1 *Let k be an arbitrary field and $f : k^n \rightarrow k^n$ be a monomial map. Suppose $P = (a_1, a_2, \ldots, a_n) \in k^n$ is a fixed point of f. Then $S_0(P)$ is upper closed and $S_1(P)$ is lower closed.*

Proof. Since $P = f(P)$, for each j in the dependency graph χ_f, we have $a_j = f_j(P)$. For any vertex i that has an edge to j, if $a_i = 0$ then $a_j = 0$. Also, if $a_j \neq 0$

then $a_i \neq 0$ for all vertices i adjacent to j. The proposition follows by chasing the dipaths in χ_f.

This property gives us a different way to recognize fixed points of monomial dynamics and we will investigate the structure of fixed points using this property.

3 FIXED POINTS

In this section, we study how to find all fixed points of the dynamics of a given map *f* over $\mathbf{F}_2$ and delve into the related combinatorial problems.

Theorem 3.1 *Let $f = (f_1, f_2, \ldots, f_n) : \mathbf{F}_2^n \to \mathbf{F}_2^n$ and let χ_f be the dependency graph of f. Assume that no f_i's are constant. Then there exists a correspondence between the set of fixed points of f and the set of antichains of the component poset G_f of χ_f.*

Proof. Suppose *P* is a fixed point of *f*. Then, by Proposition 2.1, $S_1(P)$ is lower closed. So the set of maximal strongly connected components among the strongly connected components contained in $S_1(P)$ forms an antichain. Now, suppose *A* is an antichain of the component poset. Then, for all $1 \leq i \leq n$, set $j_i = 0$ if $j_i \geq C$ for some $C \in A$ and set $j_i = 1$ otherwise. Let $P_A = (j_1, j_2, \ldots, j_n)$. Note that if *j* = 0, then since *j* = 0 for all $j \geq j_i$, $f_i(P_A) = 0$. Also, if $j_i = 1$, then since *j* = 1 for all $j \leq j_i$, $f_i(P_A) = 1$. This implies that $f(P_A) = P_A$, i.e. P_A is a fixed point.

Example 2.1.(revisited) *Suppose that f is defined in Example. Recall that we have already seen the component poset G_f of χ_f in Figure and the corresponding antichains. From this, we can find all the fixed points of f:*

$$\begin{array}{ccc}
\varnothing & \leftrightarrow & (1,1,1,1,1,1,1,1,1,1,1,1), \\
\{C_1\} & \leftrightarrow & (0,0,0,1,1,1,0,0,1,1,1,1), \\
\{C_2\} & \leftrightarrow & (1,1,1,1,1,1,0,0,0,0,0,1), \\
\{C_3\} & \leftrightarrow & (0,0,0,0,1,1,0,0,0,0,0,0), \\
\{C_1, C_2\} & \leftrightarrow & (0,0,0,1,1,1,0,0,0,0,0,1).
\end{array}$$

So, if we can compute the number of antichains of the component poset, then we know the number of fixed points of given boolean monomial dynamics.

Definition 3.1 (Valiant, 1979) *#P is the class of functions that can be computed by counting Turing machines of polynomial time complexity.*

A problem is #P-complete if and only if it is in #P, and every problem in #P can be reduced to it by a polynomial-time counting reduction. There is no known algorithms to solve #P-complete problem efficiently. Provan and Ball (1983) showed that computing the number of antichains of given poset is a #P-complete problem and Knuth and Rusky (2003) studied some special cases where the counting can be done efficiently. In the following, we present a simple algorithm to count the number of antichains of a given poset. Thus Theorem 3.1 gives us the following consequence.

Corollary 3.2 *The problem of counting fixed points of a boolean monomial dynamical systems is #P-complete.*

4 CONCLUSIONS

In this paper, we have focused on boolean monomial dynamical systems. We have shown that counting the number of fixed points of boolean monomial dynamics is a #P-complete problem. This implies that it is inherently difficult to study the structure of cycles of monomial dynamical systems over finite fields. For boolean dynamical systems with more than one term, which have not been covered in this paper, there is still difficulty in studying cycle structure of such dynamical systems.

REFERENCES

[1] Barta, A. and Morton, P., 1994. Algebraic dynamics of polynomial maps on the algebraic closure of a finite field,I. *Rocky Mountain Journal of Mathematics*, **24(2)**, pp.453-481. http://dx.doi.org/10.1216/rmjm/1181072411

[2] Barta, A. and Morton, P., 1994.Algebraic dynamics of polynomial maps on the algebraic closure of a finite field,II. *Rocky Mountain Journal of Mathematics*, **24(3)**, pp.905-932. http://dx.doi.org/10.1216/rmjm/1181072380

[3] Colón-Reyes, O., Jarrah, A.S., Laubenbacher, R., and Sturmfels, B., 2006.Monomial dynamical systems over finite fields. *Journal of Complex Systems*, **16(4)**, pp.333-342.

[4] Devaney, R.L., 2003.*An Introduction to Chaotic Dynamical System*. 2nd ed. Westview Press.

[5] Elspas, B., 1959. The theory of autonomous linear sequential networks. *IRE Transactions on Circuit Theory*, 6(1), pp.45-60.

[6] Gilbert, C.L., Kolesar, J.D., Reiter, C.A., and Stroey, J.D., 2001. Function digraphs of quadratic maps modulo *p*. *The Fibonacci Quarterly*, **39**, pp.32-49.

[7] Hernandez-Toledo, R.A., 2005. Linear finite dynamical systems. *Communications in Algebra*, **33(9)**, pp.2977-2989. http://dx.doi.org/10.1081/AGB-200066211

[8] Jarrah, A.S., Laubenbacher, R., and Vera-Licona. P., 2006.An efficient algorithm for finding the phase space structure of linear finite dynamical systems. preprint.

[9] Jarrah, A.S., Laubenbacher, R., and Veliz-Cuba,A., 2010. The dynamics of conjunctive and disjunctive boolean networks. *Bulletin of Mathematical Biology*, **72(6)**, pp.1425-1447. http://dx.doi.org/10.1007/s11538-010-9501-z

[10] Just, W.,2006. The steady state system problem is NP-hard even for monotone quadratic Boolean dynamical systems.preprints available at http://www.ohio.edu/people/just/PAPERS/monNPh14.

[11] Knuth, D.E. and Rusky, F., 2003. Efficient Coroutine Generation of Constrained Gray Sequences. *Lecture Notes in Computer Science*, **2635**, pp.183-208. http://dx.doi.org/10.1007/978-3-540-39993-3_11

[12] Park, J.W., 2003. Algebraic properties of the digraph generated by the iteration of quadratic mapping $x \mapsto x^2 - 2(\mathrm{mod}\, p)$. *manuscript.*

[13] Provan, J.S. and Ball, M.O., 1983. Complexity of Counting Cuts, *Siam Journal of Computing* ***12*** pp.777-788. http://dx.doi.org/10.1137/0212053

[14] Robinson, C., 1998.*Dynamical Systems - Stability, Symbolic Dynamics, and Chaos*. CRC.

[15] Rogers, T.D., 1996, The graph of the square mapping on the prime fields,*Discrete Mathematics*, **148**, pp.317-324. http://dx.doi.org/10.1016/0012-365X(94)00250-M

[16] Vasiga, T. and Shallit, J., 2004, On the iteration of certain quadratic maps over *GF*(*p*), *Discrete Mathematics*, **277**, pp.219-240. http://dx.doi.org/10.1016/S0012-365X(03)00158-4

[17] Xua, G.and Zoub, Y.M., 2009, Linear dynamical systems over finite rings.*Journal of Algebra*, **321(8)**, pp.2149-2155. http://dx.doi.org/10.1016/j.jalgebra.2008.09.029

[18] Valiant, L.G., 1979, The Complexity of Computing the Permanent.*Theoretical Computer Science*, **8**, pp.189-201 http://dx.doi.org/10.1016/0304-3975(79)90044-6

[19] Zieve, M.E., 1996.*Cycles of polynomial mappings*. PhD thesis, University of California at Berkeley.

Jang-Woo Park, is Professor in School of Arts & Sciences, University of Houston-Victoria, Victoria, USA

Shuhong Gao, is Professor in Department of Mathematical Sciences, Clemson University, Clemson, USA