

An Algebraic and Graph Theoretic Framework to Study Monomial Dynamical Systems over a Finite Field

Edgar Delgado-Eckert

*ETH Zürich, Department of Biosystems Science and Engineering (D-BSSE)
WRO-1058-8.46, Mattenstrasse 26, 4058 Basel, Switzerland
edgar.delgado-eckert@mytum.de*

A monomial dynamical system $f : K^n \rightarrow K^n$ over a finite field K is a nonlinear deterministic time discrete dynamical system with the property that each component function $f_i : K^n \rightarrow K$ is a monic nonzero monomial function. In this paper we provide an algebraic and graph theoretic framework to study the dynamic properties of monomial dynamical systems over a finite field. Within this framework, characterization theorems for fixed point systems, that is, systems in which all trajectories end in steady states, are proved. These characterizations are stated in terms of connectedness properties of the dependency graph. Our formalism allowed us to develop an algorithm of polynomial complexity for testing whether or not a given monomial dynamical system over an arbitrary finite field is a fixed point system. In addition, we were able to identify a class of monomial dynamical systems, namely, the $(q - 1)$ -fold redundant monomial systems. Within this class of systems a characterization of fixed point systems is proved that represents a generalization of previous work on Boolean monomial dynamical systems.

1. Introduction

Time discrete dynamical systems over a finite set X are an important subject of active mathematical research. One relevant example of such systems are cellular automata, first introduced in the late 1940s by John von Neumann [1]. More general examples are nondeterministic finite state automata [2] and sequential dynamical systems [3].

Deterministic time discrete dynamical systems over a *finite field* are mappings $f : K^n \rightarrow K^n$, where K is a finite field and $n \in \mathbb{N}$ is the dimension of the system. As opposed to deterministic time discrete dynamical systems over a finite set X , this type of system allows for a richer mathematical framework within which they can be studied. For instance, it can be shown that every component function $f_i : K^n \rightarrow K$ is a polynomial function of bounded degree in n variables [4, 5].

The study of dynamical systems generally addresses the question of the system's long-term behavior, in particular, the existence of *fixed*

points and (*limit*) *cyclic trajectories*. In this paper we provide an algebraic and graph theoretic framework for studying a specific class of nonlinear time discrete dynamical systems over a finite field, namely, *monomial dynamical systems over a finite field*. In such systems, every component function $f_i: K^n \rightarrow K$ is a *monic nonzero monomial function*.

Some types of monomial systems and their dynamic behavior have been studied before: monomial cellular automata [6, 7], Boolean monomial systems [8], monomial systems over the p -adic numbers [9, 10], and monomial systems over a finite field [11-13]. A necessary and sufficient condition for Boolean monomial systems to be fixed point systems, that is, systems in which all trajectories end in steady states, is proved in [8]. This condition could be algorithmically exploited. Indeed, the authors make some suggestive comments in that direction [8, Section 4.3]. Moreover, they describe the structure of the limit cycles of a special type of Boolean monomial systems.

In [13] the authors present a necessary and sufficient condition for monomial systems over a finite field to be fixed point systems. However, this condition is not easily verifiable and therefore the theorem does not yield a tractable algorithm in a straightforward way. In [13] it is explicitly stated that a tractable algorithm to determine whether or not a monomial dynamical system over an arbitrary finite field is a fixed point system has still to be developed [13, Section 3]. Nevertheless, while the present paper was being peer-reviewed, [14] was published, providing the missing computational-algebraic ingredient toward an algorithmic application of the approach in [13]. However, the concrete details of an algorithm exploiting the results in [13] and [14] still need to be developed.

Our work was influenced by [8, 13, 12]. However, we took a slightly different approach. The mathematical formalism we developed allows for a deeper understanding of monomial dynamical systems over a finite field. Indeed, we were able to circumvent the complicated Glueing-procedure developed in [8, Section 5]. Our formalism allows formulating a very simple algorithm of *polynomial complexity* for testing whether or not a given monomial dynamical system over an arbitrary finite field is a fixed point system. Additional theorems that complement the work in [8, 13] are obtained. Furthermore, we were able to identify a class of monomial dynamical systems, namely, the $(q - 1)$ -fold redundant monomial systems (to be defined later). Within this class of systems, a very satisfying characterization of fixed point systems can be reached. Boolean systems are trivial examples of $(q - 1)$ -fold redundant systems. As a consequence, many of our results about $(q - 1)$ -fold redundant monomial systems provide a generalization of theorems proved in [8] for Boolean systems. Last but not least, our formalism also constitutes a basis for the study of *monomial control systems* [15].

It is pertinent to mention the work of [16] regarding *linear* time discrete dynamical systems over a finite field, in which the number of limit cycles and their lengths is linked to the factorization (in so-called elementary divisor polynomials) of the characteristic polynomial of the matrix representing the system. (See also [17] for a more mathematical exposition and [2, 18] for applications of the Boolean case in control theory.) Furthermore, the affine case, that is, a linear map followed by a translation, was studied in [19]. An interesting contribution was made by Paul Cull in [20], who extended the considerations to nonlinear functions, and showed how to reduce them to the linear case. However, Cull's approach does not yield an algorithm of polynomial complexity to solve the steady state system problem. Moreover, according to [21], this might in general not be possible as a matter of principle.

This paper is organized as follows: Section 2 establishes an algebraic and graph theoretic framework within which monomial dynamical systems over a finite field are studied. It starts with some basic definitions and algebraic results (proofs can be found in [5, Section 2.2]) and leads the reader to the first important result, namely, that the monoid of n -dimensional monomial dynamical systems over a finite field K is isomorphic to a certain monoid of matrices. Section 2 finishes with propositions about the relationship between the matrix F corresponding to a monomial system f (via the isomorphism mentioned) and the adjacency matrix of the dependency graph of f . These findings allow us to link topological properties of the dependency graph with the dynamics of f , which is the fundamental insight underlying this work.

Section 3 is devoted to the characterization of fixed point systems. These characterizations are stated in terms of connectedness properties of the dependency graph. Theorem 4, for instance, presents necessary and sufficient connectedness conditions for a system to be a fixed point system. Furthermore, the class of $(q - 1)$ -fold redundant monomial systems is introduced and a characterization of fixed point systems within this class is provided. We finish Section 3 with several relatively easy to test sufficient conditions for a system to be a fixed point system.

Section 4 presents an algorithm of polynomial complexity to test whether or not a given monomial dynamical system over a finite field K is a fixed point system. A detailed complexity analysis of the algorithm is provided.

2. Algebraic and Graph Theoretic Formalism

In this section we introduce the monoid of n -dimensional monomial dynamical systems over a finite field \mathbb{F}_q . This monoid is isomorphic to a certain monoid of matrices; in other words, the composition $f \circ g$ of two monomial dynamical systems f, g is completely captured by the product $F \cdot G$ of their corresponding matrices. Furthermore, we provide our definition for the dependency graph of a monomial dynamical system f . The adjacency matrix of the dependency graph is precisely the matrix F associated with f via the isomorphism mentioned earlier. This finding allows us to link topological properties of the dependency graph with the dynamics of f , which is the fundamental insight underlying this work.

Definition 1. We denote a *finite field* with \mathbb{F}_q , where q stands for the number of elements in the field. It is understood that q is a power of the (prime) characteristic of the field.

Definition 2. Let \mathbb{F}_q be a finite field. The set $E_q := \{0, \dots, q-1\} \subset \mathbb{N}_0$ is called the *exponents set* of the field \mathbb{F}_q .

Definition 3. Let \mathbb{F}_q be a finite field and $n \in \mathbb{N}$. A map $f: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ is called a *monomial dynamical system* over \mathbb{F}_q if for every $i \in \{1, \dots, n\}$ there exists a tuple $(F_{i1}, \dots, F_{in}) \in E_q^n$ such that $f_i(x) = x_1^{F_{i1}} \cdots x_n^{F_{in}} \forall x \in \mathbb{F}_q^n$.

Remark 1. As opposed to [8], we exclude in the definition of a monomial dynamical system the possibility that one of the functions f_i is equal to the zero function. However, in contrast to [13], we do allow the case $f_i \equiv 1$ in our definition. This is not a loss of generality because of the following: If we were studying a dynamical system $f: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ where one of the functions, say f_j , was equal to zero, then, for every initial state $x \in \mathbb{F}_q^n$, after one iteration the system would be in a state $f(x)$ whose j^{th} entry is zero. In all subsequent iterations the value of the j^{th} entry would remain zero. As a consequence, the long-term dynamics of the system are reflected in the projection $\pi_j(y) := (y_1, \dots, y_{j-1}, y_{j+1}, \dots, y_n)^t$ and it is sufficient to study the system

$$\tilde{f} : \mathbb{F}_q^{n-1} \rightarrow \mathbb{F}_q^{n-1}$$

$$y \mapsto \begin{pmatrix} f_1(y_1, \dots, y_{j-1}, 0, y_{j+1}, \dots, y_n) \\ \vdots \\ f_{j-1}(y_1, \dots, y_{j-1}, 0, y_{j+1}, \dots, y_n) \\ f_{j+1}(y_1, \dots, y_{j-1}, 0, y_{j+1}, \dots, y_n) \\ \vdots \\ f_n(y_1, \dots, y_{j-1}, 0, y_{j+1}, \dots, y_n) \end{pmatrix}.$$

In general, the system \tilde{f} could contain component functions equal to the zero function, since every component f_i that depends on the variable x_j would become zero. As a consequence, the described procedure needs to be applied several times until the lower dimensional system obtained does not contain component functions equal to zero. It is also possible that this repeated procedure yields the one-dimensional zero function. In this case, we can conclude that the original system f is a fixed point system with $(0, \dots, 0) \in \mathbb{F}_q^n$ as its unique fixed point. The details about this procedure are described as the “preprocessing algorithm” in [5, Appendix B].

It is well known that every function $h : \mathbb{F}_q^n \rightarrow \mathbb{F}_q$ is a polynomial function in n variables where no variable appears to a power higher or equal to q (e.g., [4, pp. 368-369]; or [5, Section 1.2]). Calculating the composition of a dynamical system $f : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ with itself, we face the situation where some of the exponents exceed the value $q - 1$ and need to be reduced according to the well-known rule

$$a^q = a \quad \forall a \in \mathbb{F}_q. \tag{1}$$

This process can be accomplished systematically if we look at the power x_i^p (where $p > q$) as a polynomial in the ring $\mathbb{F}_q[\tau]$ and define the magnitude $\text{red}_q(p)$ as the degree of the (unique) remainder of the polynomial division $\tau^p \div (\tau^q - \tau)$ in the polynomial ring $\mathbb{F}_q[\tau]$. Then we can write

$$x_i^p = x_i^{\text{red}_q(p)} \quad \forall x_i \in \mathbb{F}_q, \tag{2}$$

which is a direct consequence of the following easily shown properties (e.g., [5, Lemma 39]) of the operator $\text{red}_q : \mathbb{N}_0 \rightarrow \mathbb{F}_q$:

$$\text{red}_q(\text{red}_q(c)) = \text{red}_q(c) \quad \forall c \in \mathbb{N}_0 \tag{3}$$

$$\text{red}_q(c) = 0 \Leftrightarrow c = 0 \tag{4}$$

$$\text{for } a, b \in \mathbb{N}_0, x^a = x^b \forall x \in \mathbb{F}_q \Leftrightarrow \text{red}_q(a) = \text{red}_q(b) \tag{5}$$

$$\begin{aligned} &\text{for } a, b \in \mathbb{N}, \\ &\text{red}_q(a) = \text{red}_q(b) \Leftrightarrow \exists \alpha \in \mathbb{Z} : a = b + \alpha(q - 1). \end{aligned} \tag{6}$$

In conclusion, the “exponents arithmetic” needed when calculating the composition of dynamical systems $f, g: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ can be formalized based on the reduction operator $\text{red}_q(p)$. Indeed, the set $E_q = \{0, 1, \dots, (q - 1)\} \subset \mathbb{Z}$ together with the operations of addition $a \oplus b := \text{red}_q(a + b)$ and multiplication $a \bullet b := \text{red}_q(ab)$ is a commutative semiring with identity 1. We call this commutative semiring the *exponents semiring* of the field \mathbb{F}_q . With this operation, it can be easily shown that the set $M(n \times n; E_q)$ of $n \times n$ quadratic matrices with entries in the semiring E_q together with the operation \cdot of matrix multiplication (which is defined in terms of the operations \oplus and \bullet on the matrix entries) over E_q is a monoid. Similarly, the set

$$\begin{aligned} MF_n^n(\mathbb{F}_q) := & \left\{ f: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n \mid \right. \\ & \left. \exists F \in M(n \times n; E_q) : f_i(x) = x_1^{F_{i1}} \dots x_n^{F_{in}} \forall x \in \mathbb{F}_q^n \right\} \end{aligned}$$

of all n -dimensional monomial dynamical systems over \mathbb{F}_q together with the composition \circ of mappings is a monoid. It is not hard to prove that these two monoids are isomorphic via the isomorphism

$$\begin{aligned} \Psi & : M(n \times n; E_q) \rightarrow MF_n^n(\mathbb{F}_q) \\ G & \mapsto \Psi(G) \end{aligned}$$

where

$$\Psi(G)_i(x) := x_1^{G_{i1}} \dots x_n^{G_{in}} \text{ for } i = 1, \dots, n.$$

The interested reader can find proofs for the previous results in [5, Section 2.2].

Remark 2. The operation $\text{red}_q: \mathbb{N}_0 \rightarrow E_q$ can be extended to matrices $M(n \times n; \mathbb{N}_0)$ by applying red_q to the entries of the matrix. We call this extension $\text{mred}_q: M(n \times n; \mathbb{N}_0) \rightarrow M(n \times n; E_q)$. See [5, Remark 47] for further details where one important property of mred_q shown is

$$\text{mred}_q(A) = 0 \Leftrightarrow A = 0. \tag{7}$$

Remark 3. For a given monomial dynamical system $f \in MF_n^n(\mathbb{F}_q)$, the matrix $F := \Psi^{-1}(f)$ is called the *corresponding matrix* of the system f . For a matrix power in the monoid $M(n \times n; E_q)$, we use the notation F^m . By induction it can be easily shown that $\Psi^{-1}(f^m) = F^m$.

As our investigations have shown, topological properties of the dependency graph of a monomial dynamical system (defined later) can reveal dynamic properties of the system. Therefore, in the rest of this section we turn our attention to some graph theoretic considerations. We now review some well-known graph theoretical objects and results while, at the same time, we introduce some useful notation.

Definition 4. A directed graph $G = (V_G, E_G, \pi_G : E_G \rightarrow V_G \times V_G)$ that allows self loops and parallel directed edges is called a *digraph*.

Definition 5. Let M be a nonempty finite set. Furthermore, let $n := |M|$ be the cardinality of M . An *enumeration* of the elements of M is a bijective mapping $f : M \rightarrow \{1, \dots, n\}$. Given an enumeration f of the set M , we write $M = \{f_1, \dots, f_n\}$ where the unique element $x \in M$ with the property $f(x) = i \in \{1, \dots, n\}$ is denoted as f_i .

Definition 6. Let $f \in MF_n^n(\mathbb{F}_q)$ be a monomial dynamical system and $G = (V_G, E_G, \pi_G)$ a digraph with vertex set V_G of cardinality $|V_G| = n$. Furthermore, let $F := \Psi^{-1}(f)$ be the corresponding matrix of f . The digraph G is called a *dependency graph* of f if and only if an enumeration $a : V_G \rightarrow \{1, \dots, n\}$ of the elements of V_G exists, such that $\forall i, j \in \{1, \dots, n\}$ there are *exactly* F_{ij} directed edges $a_i \rightarrow a_j$ in the set E_G , that is, $|\pi_f^{-1}((a_i, a_j))| = F_{ij}$.

Remark 4. It is easy to show that if G and H are dependency graphs of f , then G and H are isomorphic. In this sense we speak of *the* dependency graph of f and denote it by $G_f = (V_f, E_f, \pi_f)$. Note that our definition of a dependency graph differs slightly from the definition used in [8].

Definition 7. Let $G = (V_G, E_G, \pi_G)$ be a digraph. Two vertices $a, b \in V_G$ are called *connected* if there is a $t \in \mathbb{N}_0$ and (not necessarily different) vertices $v_1, \dots, v_t \in V_G$ such that $a \rightarrow v_1 \rightarrow v_2 \rightarrow \dots \rightarrow v_t \rightarrow b$. In this situation we write $a \rightarrow_s b$, where s is the number of directed edges involved in the sequence from a to b (in this case $s = t + 1$). Two sequences $a \rightarrow_s b$ of the same length are considered different if the directed edges involved are different or the order at which they appear is different, even if the visited vertices are the same. As a convention, a single vertex $a \in V_G$ is always connected to itself $a \rightarrow_0 a$ by an empty sequence of length 0.

Definition 8. Let $G = (V_G, E_G, \pi_G)$ be a digraph and $a, b \in V_G$ two vertices. A sequence $a \rightarrow_s b$

$$a \rightarrow v_1 \rightarrow v_2 \rightarrow \dots \rightarrow v_t \rightarrow b$$

is called a *path*, if no vertex v_i is visited more than once. If $a = b$, but no other vertex is visited more than once, $a \rightarrow_s b$ is called a *closed path*.

Definition 9. Let $G = (V_G, E_G, \pi_G)$ be a digraph. Two vertices $a, b \in V_G$ are called *strongly connected* if there are natural numbers $s, t \in \mathbb{N}$ such that $a \rightarrow_s b$ and $b \rightarrow_t a$. In this situation we write $a \rightleftharpoons b$.

Theorem 1. Let $G = (V_G, E_G, \pi_G)$ be a digraph. \rightleftharpoons is an equivalence relation on V_G called a *strong equivalence*. The equivalence class of any vertex $a \in V_G$ is called a *strongly connected component* and denoted by $\vec{a} \subseteq V_G$.

Proof. This is well known as shown, for instance, in [8, Definition 3.1]. ■

Definition 10. Let $G = (V_G, E_G, \pi_G)$ be a digraph and $a \in V_G$ one of its vertices. The strongly connected component $\vec{a} \subseteq V_G$ is called *trivial* if and only if $\vec{a} = \{a\}$ and there is no edge $a \rightarrow a$ in E_G .

Definition 11. Let $G = (V_G, E_G, \pi_G)$ be a digraph with vertex set V_G of cardinality $|V_G| = n$ and $V_G = \{a_1, \dots, a_n\}$ an enumeration of the elements of V_G . The matrix $A \in M(n \times n; \mathbb{N}_0)$ whose entries are defined as $A_{ij} :=$ number of edges $a_i \rightarrow a_j$ contained in E_G for $i, j = 1, \dots, n$ is called an *adjacency matrix* of G with the enumeration a .

Theorem 2. Let $G = (V_G, E_G, \pi_G)$ be a digraph with vertex set V_G of cardinality $|V_G| = n$ and $V_G = \{a_1, \dots, a_n\}$ an enumeration of the elements of V_G . Furthermore, let $A \in M(n \times n; \mathbb{N}_0)$ be its adjacency matrix (with the enumeration a), $m \in \mathbb{N}$ a natural number, and $B := A^m \in M(n \times n; \mathbb{N}_0)$ is the m^{th} power of A . Then $\forall i, j \in \{1, \dots, n\}$ the entry B_{ij} of B is equal to the number of different sequences $a_i \rightarrow_m a_j$ of length m .

Proof. The proof of this is a well-known result and can be found in [22]. ■

Remark 5. Let $f \in MF_n^n(\mathbb{F}_q)$ be a monomial dynamical system. Furthermore, let $G_f = (V_f, E_f, \pi_f)$ be the dependency graph of f and $V_f = \{a_1, \dots, a_n\}$ the associated enumeration of the elements of V_f . Then, according to the definition of a dependency graph, $F := \Psi^{-1}(f)$

(the corresponding matrix of f) is precisely the adjacency matrix of G_f with the enumeration a . Now, by Remarks 3 and 2 we can conclude

$$\Psi^{-1}(f^m) = \text{mred}_q(F^m). \tag{8}$$

3. Characterization of Fixed Point Systems

The results presented in Section 2 allow us to link topological properties of the dependency graph with the dynamics of f . We now exploit this feature to prove some characterizations of fixed point systems stated in terms of connectedness properties of the dependency graph. In the course of these investigations we will identify and define a class of monomial dynamical systems as the $(q - 1)$ -fold redundant monomial systems. Within this class of systems, a very satisfying characterization of fixed point systems can be reached. A trivial example of $(q - 1)$ -fold redundant systems are the Boolean systems, that is, monomial systems $f \in M F_n^n(F_2)$. As a consequence, many of the results shown in this section provide a generalization of results proved in [8] for Boolean systems.

Theorem 3. Let F_q be a finite field and $f \in M F_n^n(F_q)$ a monomial dynamical system. Then f is a fixed point system with $(1, \dots, 1)^t \in F_q^n$ as its only fixed point if and only if its dependency graph only contains trivial strongly connected components.

Proof. By Remark 5, $F := \Psi^{-1}(f)$ is the adjacency matrix of the dependency graph of f . If the dependency graph does not contain any nontrivial strongly connected components, every sequence $a \rightsquigarrow_s b$ between two arbitrary vertices can be at most of length $n - 1$. (A sequence that revisits a vertex would contain a closed sequence, which is strongly connected.) Therefore, by Theorem 2, $\exists m \in \mathbb{N}$ with $m \leq n$ such that $F^m = 0$ (the zero matrix in $M(n \times n; \mathbb{N}_0)$). Now, according to equation (8) we have $\Psi^{-1}(f^m) = \text{mred}_q(F^m) = \text{mred}_q(0) = 0$ and consequently $\Psi^{-1}(f^r) = 0 \forall r \geq m$. Thus, $f^r = 1 \forall r \geq m$.

If, on the other hand, there is an $m \in \mathbb{N}$ such that $f^{m+\lambda} = f^m = 1 \forall \lambda \in \mathbb{N}$ applying the isomorphism Ψ^{-1} (see Remark 3) we obtain $F^{(m+\lambda)} = F^m = 0 \forall \lambda \in \mathbb{N}$ and (see equation (8)) $\text{mred}_q(F^{m+\lambda}) = \text{mred}_q(F^m) = 0 \forall \lambda \in \mathbb{N}$. It follows from equation (7) (see also [5, Remark 47]) that $F^{m+\alpha} = 0 \forall \alpha \in \mathbb{N}_0$.

Now, by Theorem 2, there are no sequences $a \rightsquigarrow_s b$ between any two arbitrary vertices a, b of length larger than $m - 1$. As a conse-

quence, there cannot be any nontrivial strongly connected components in the dependency graph of f . ■

Definition 12. A monomial dynamical system $f \in MF_n^n(\mathbb{F}_q)$ whose dependency graph contains nontrivial strongly connected components is called a *coupled monomial dynamical system*.

Definition 13. Let $G = (V_G, E_G, \pi_G)$ be a digraph, $m \in \mathbb{N}$ a natural number, and $a, b \in V_G$ two vertices. The number of different sequences of length m from a to b is denoted by $s_m(a, b) \in \mathbb{N}_0$. By Theorem 2 it obviously holds that $s_m(a_i, a_j) = (A^m)_{ij}$.

Theorem 4. Let \mathbb{F}_q be a finite field, $f \in MF_n^n(\mathbb{F}_q)$ a coupled monomial dynamical system, and $G_f = (V_f, E_f, \pi_f)$ its dependency graph. Then f is a fixed point system if and only if there is an $m \in \mathbb{N}$ such that the following two conditions hold.

1. For every pair of nodes $a, b \in V_f$ with $a \rightarrow_m b$ there exists for every $\lambda \in \mathbb{N}$ an $a_\lambda \in \mathbb{Z}$ such that $s_{m+\lambda}(a, b) = s_m(a, b) + a_\lambda(q - 1) \neq 0$.
2. For every pair of nodes $a, b \in V_f$ with $s_m(a, b) = 0$ it holds that $s_{m+\lambda}(a, b) = 0 \forall \lambda \in \mathbb{N}$.

Proof. Let $V_f = \{a_1, \dots, a_n\}$ be the enumeration of the vertices. If f is a fixed point system, $\exists m \in \mathbb{N}$ such that $f^{m+\lambda} = f^m \forall \lambda \in \mathbb{N}$. By applying the homomorphism Ψ^{-1} we get (see Remark 3)

$$F^{(m+\lambda)} = F^m \forall \lambda \in \mathbb{N}. \tag{9}$$

By Remark 5 it follows that $\text{mred}_q(F^{m+\lambda}) = \text{mred}_q(F^m) \forall \lambda \in \mathbb{N}$. Let $i, j \in \{1, \dots, n\}$. If, on the one hand, $(F^m)_{ij} = 0$, then by equation (9) we would have $(F^{(m+\lambda)})_{ij} = 0 \forall \lambda \in \mathbb{N}$. Consequently, by equation (4) we have $(F^{m+\alpha})_{ij} = 0 \forall \alpha \in \mathbb{N}_0$.

Now, by Theorem 2, there are no sequences $a_i \rightarrow_s a_j$ of length larger than $m - 1$. In other words, Theorem 4 condition 2 follows. If, on the other hand, $(F^m)_{ij} \neq 0$ then by equation (9) we would have $(F^{(m+\lambda)})_{ij} = (F^m)_{ij} \neq 0 \forall \lambda \in \mathbb{N}$. Consequently, by equations (4) and (6) $\exists a_\lambda \in \mathbb{Z}$ such that $(F^{m+\lambda})_{ij} = (F^m)_{ij} + a_\lambda(q - 1) \forall \lambda \in \mathbb{N}$. In other words, Theorem 4 condition 1 follows.

We now show the converse: Given conditions 1 and 2 and in accordance with Theorem 2 and Remark 5, if $(F^m)_{ij} = 0$, then $(F^{m+\lambda})_{ij} = (F^m)_{ij} \forall \lambda \in \mathbb{N}$ and if $(F^m)_{ij} \neq 0$, then $\exists a_\lambda \in \mathbb{Z} : (F^{m+\lambda})_{ij} = (F^m)_{ij} + a_\lambda(q - 1) \neq 0 \forall \lambda \in \mathbb{N}$.

Now, by equations (4) and (6), we have $\text{mred}_q(F^{m+\lambda}) = \text{mred}_q(F^m) \forall \lambda \in \mathbb{N}$ and by Remark 5 $F^{(m+\lambda)} = F^m \forall \lambda \in \mathbb{N}$. Thus, after applying the isomorphism $\Psi: f^{m+\lambda} = f^m \forall \lambda \in \mathbb{N}$. ■

The following parameter for digraphs was introduced into the field of research on monomial dynamical systems over F_2 in [8] as the “loop number”. The loop number of a strongly connected graph is also known as the “index of imprimitivity” [23] or “period” [24] and has been used in the study of non-negative matrices [25, 26]. It is well known that this number quantizes the length of any closed sequence in a strongly connected digraph. It is also the biggest possible “quantum”.

Definition 14. Let $G = (V_G, E_G, \pi_G)$ be a digraph and $a \in V_G$ one of its vertices. The number

$$L(a) := \min_{\substack{a \rightarrow_u a \\ a \rightarrow_v a \\ u \neq v}} |u - v|$$

is called the *loop number* of a . If there is no sequence of positive length from a to a , then $L(a)$ is set to zero.

If \vec{a} is nontrivial, then for every $b \in \vec{a}$ it holds that $L(b) = L(a)$ (for a proof see [8, Lemma 4.2]). Therefore, we introduce the loop number of strongly connected components as $L(\vec{a}) := L(a)$.

In [25, Section 3.4], the index of imprimitivity is directly defined (i.e., without defining it for single nodes in the digraph) for strongly connected digraphs using an equivalent definition.

Remark 6. The loop number of any trivial strongly connected component is, due to the convention made in Definition 14, equal to zero.

Corollary 1. Let F_q be a finite field, $f \in MF_n^m(F_q)$ a coupled monomial dynamical system, and $G_f = (V_f, E_f, \pi_f)$ its dependency graph. If f is a fixed point system, then the loop number of each of its nontrivial strongly connected components is equal to one.

Proof. Let $m \in \mathbb{N}$ be as stated in Theorem 4. Let $\vec{a} \subseteq V_f$ be a nontrivial strongly connected component. For every $b \in \vec{a}$ we have that b is strongly connected with itself. Therefore, for every $s \in \mathbb{N}$ there is a $t \geq s$ such that $b \rightarrow_t b$. In particular, there must be a $u \in \mathbb{N}$ with $u > m$ such that $b \rightarrow_u b$, that is, $s_u(b, b) \geq 1$. By condition 2 of Theorem 4 we know that $s_m(b, b) \neq 0$, otherwise $s_u(b, b) = 0$. Now, from condition 1 we know that $\exists a_\lambda \in \mathbb{Z} : s_{m+\lambda}(b, b) = s_m(b, b) + a_\lambda(q - 1) \neq 0 \forall \lambda \in \mathbb{N}$ and, in particular,

$s_{m+\lambda}(b, b) \neq 0 \forall \lambda \in \mathbb{N}$. Therefore, $\forall \lambda \in \mathbb{N}$ there are sequences $b \rightarrow_{m+\lambda} b$. Thus, $\mathcal{L}(\vec{a}) = \mathcal{L}(b) = 1$. ■

Definition 15. Let $G = (V_G, E_G, \pi_G)$ be a digraph and $a, b \in V_G$ two vertices. The vertex a is called *recurrently connected* to b , if for every $s \in \mathbb{N}$ there is a $u \geq s$ such that $a \rightarrow_u b$.

Remark 7. Let $G = (V_G, E_G, \pi_G)$ be a digraph with vertex set V_G of cardinality $n := |V_G|$. Obviously, for any two vertices $a, b \in V_G$ either a is recurrently connected to b or there is an $m \in \mathbb{N}$ with $m \leq n$ such that no sequence $a \rightarrow_t b$ of length $t \geq m$ exists.

Lemma 1. Let $G = (V_G, E_G, \pi_G)$ be a digraph and $U \subseteq V_G$ a nontrivial strongly connected component. Furthermore, let $t := L(U)$ be the loop number of U . Then for each $a, b \in U$ there is an $m \in \mathbb{N}$ such that the graph G contains sequences $a \rightarrow_{m+\lambda t} b$ of length $m + \lambda t \forall \lambda \in \mathbb{N}$.

Proof. See [8, Proposition 4.5] or, alternatively, [25, Lemma 3.4.1]. ■

Theorem 5. Let $G = (V_G, E_G, \pi_G)$ be a digraph containing nontrivial strongly connected components. If the loop number of every nontrivial strongly connected component is equal to one, then there is an $m \in \mathbb{N}$ such that *any* pair of vertices $a_i, a_j \in V_G$ with a_i recurrently connected to a_j satisfies $s_{m+\lambda}(a_i, a_j) > 0 \forall \lambda \in \mathbb{N}_0$.

Proof. This follows easily from Lemma 1. Alternatively, see [25, Lemma 3.4.1]. ■

Definition 16. Let \mathbb{F}_q be a finite field, $f \in M F_n^n(\mathbb{F}_q)$ a monomial dynamical system, and $G_f = (V_f, E_f, \pi_f)$ its dependency graph. f is called a $(q - 1)$ -fold *redundant monomial system* if there is an $N \in \mathbb{N}$ such that for any pair $a, b \in V_f$ with a recurrently connected to b , the following holds:

$$\forall m \geq N \exists \alpha_{abm} \in \mathbb{N}_0 : s_m(a, b) = \alpha_{abm}(q - 1).$$

Remark 8. Note that any Boolean monomial dynamical system $f \in M F_n^n(\mathbb{F}_2)$ is $(2 - 1)$ -fold redundant.

Lemma 2. Let \mathbb{F}_q be a finite field, $f \in M F_n^n(\mathbb{F}_q)$ a coupled $(q - 1)$ -fold redundant monomial dynamical system, and $G_f = (V_f, E_f, \pi_f)$ its dependency graph. Then f is a fixed point system if the loop number of each nontrivial strongly connected component of G_f is equal to one.

Proof. Let $V_f = \{a_1, \dots, a_n\}$ be the enumeration of the vertices and $F := \Psi^{-1}(f)$ be the corresponding matrix of f . Consider two arbitrary

vertices $a_i, a_j \in V_f$. By Remark 7, either a_i is recurrently connected to a_j or there is an $m_0 \in \mathbb{N}$ with $m_0 \leq n$ such that no sequence $a \rightarrow_t b$ of length $t \geq m_0$ exists. If the latter is the case, then $(F^{m_0+\lambda})_{ij} = 0 \forall \lambda \in \mathbb{N}_0$.

On the other hand, if a_i is recurrently connected to a_j , then by Theorem 5 there is an $m_1 \in \mathbb{N}$ such that

$$s_{m_1+\gamma}(a_i, a_j) > 0 \forall \gamma \in \mathbb{N}_0. \tag{10}$$

Consider now $m_2 := \max(n, m_1)$. Due to the universality of m_1 in equation (10), for any pair of vertices $a_i, a_j \in V_G$ with a_i recurrently connected to a_j there is a sequence $a_i \rightarrow_{m_2+\gamma} a_j$ of length $m_2 + \gamma$, in particular $s_{(m_2+\gamma)}(a_i, a_j) > 0 \forall \gamma \in \mathbb{N}_0$. Now, let N be the constant in Definition 16 and $m_3 := \max(N, m_2)$. Now, by hypothesis, $\exists \alpha_{ij\gamma} \in \mathbb{N}$ such that $s_{(m_3+\gamma)}(a_i, a_j) = \alpha_{ij\gamma}(q-1) \forall \gamma \in \mathbb{N}_0$. Thus,

$$\begin{aligned} s_{(m_3+\gamma)}(a_i, a_j) &= \\ \alpha_{ij\gamma}(q-1) &= \alpha_{ij0}(q-1) + (\alpha_{ij\gamma} - \alpha_{ij0})(q-1) = \\ s_{m_3}(a_i, a_j) &+ (\alpha_{ij\gamma} - \alpha_{ij0})(q-1) \forall \gamma \in \mathbb{N}_0. \end{aligned}$$

Summarizing, since $m_0 \leq n \leq m_2 \leq m_3$, we can say that $\forall i, j \in \{1, \dots, n\}$, depending on whether a_i and a_j are recurrently connected or not, $(F^{m_3+\lambda})_{ij} = 0 \forall \lambda \in \mathbb{N}_0$ or $\exists a_\lambda \in \mathbb{Z} : (F^{m_3+\lambda})_{ij} = (F^{m_3})_{ij} + a_\lambda(q-1) \neq 0 \forall \lambda \in \mathbb{N}_0$. Now, by equations (4) and (6), it follows that $\text{mred}_q(F^{m_3+\lambda}) = \text{mred}_q(F^{m_3}) \forall \lambda \in \mathbb{N}$ and by Remark 5 $F^{(m_3+\lambda)} = F^{m_3} \forall \lambda \in \mathbb{N}$. Thus, after applying the isomorphism Ψ we have $f^{m_3+\lambda} = f^{m_3} \forall \lambda \in \mathbb{N}$. ■

Theorem 6. Let F_q be a finite field, $f \in MF_n^q(F_q)$ a coupled $(q-1)$ -fold redundant monomial dynamical system, and $G_f = (V_f, E_f, \pi_f)$ its dependency graph. Then f is a fixed point system if and only if the loop number of each nontrivial strongly connected component of G_f is equal to one.

Proof. The claim follows immediately from Lemma 2 and Corollary 1. ■

Theorem 7. Let F_q be a finite field, $f \in MF_n^q(F_q)$ a coupled monomial dynamical system, and $G_f = (V_f, E_f, \pi_f)$ its dependency graph. Then f is a fixed point system if the following properties hold.

1. The loop number of each nontrivial strongly connected component of G_f is equal to one.
2. For each nontrivial strongly connected component $\vec{a} \subseteq V_f$ and arbitrary $b, c \in \vec{a}$, $s_1(b, c) \neq 0 \Rightarrow s_1(b, c) = q - 1$.

Proof. Let $V_f = \{a_1, \dots, a_n\}$ be the enumeration of the vertices. Consider two vertices $a_i, a_j \in V_f$ such that a_i is recurrently connected to a_j . Then by Theorem 5 there is an $m_1 \in \mathbb{N}$ such that

$$s_{m_1+\gamma}(a_i, a_j) > 0 \forall \gamma \in \mathbb{N}_0. \tag{11}$$

Consider now $m_2 := \max(n, m_1)$. Due to the universality of m_1 in equation (11), for any pair of vertices $a_i, a_j \in V_G$ with a_i recurrently connected to a_j there is a sequence $a_i \rightarrow_{m_2+\gamma} a_j$ of length $m_2 + \gamma$. Since $m_2 + \gamma > n - 1$, necessarily $\exists a_{k_\gamma}, a_{l_\gamma} \in \vec{a}_{k_\gamma}$ such that \vec{a}_{k_γ} is nontrivial and

$$a_i \rightarrow_{(m_2+\gamma)} a_j = a_i \rightarrow \dots \rightarrow a_{k_\gamma} \rightarrow_t a_{l_\gamma} \rightarrow \dots \rightarrow a_j \tag{12}$$

(t depends on i, j , and γ). Now, by hypothesis, every two directly connected vertices $a, b \in \vec{a}_{k_\gamma}$ are directly connected by exactly $q - 1$ directed edges. Therefore, for any sequence $a_{k_\gamma} \rightarrow_t a_{l_\gamma}$ of length $t \in \mathbb{N}$ there are $(q - 1)^t$ different copies of it and we can conclude $\exists \alpha \in \mathbb{N}$ such that $s_t(a_{k_\gamma}, a_{l_\gamma}) = \alpha(q - 1)$. As a consequence, there are $\alpha(q - 1)$ different copies of the sequence in equation (12). Since we are dealing with an arbitrary sequence $a_i \rightarrow_{(m_2+\gamma)} a_j$ of fixed length $m_2 + \gamma$, $\gamma \in \mathbb{N}_0$ we can conclude that $\exists \alpha_{ij\gamma} \in \mathbb{N}$ such that $s_{(m_2+\gamma)}(a_i, a_j) = \alpha_{ij\gamma}(q - 1) \forall \gamma \in \mathbb{N}_0$. Thus, f is a coupled $(q - 1)$ -fold redundant monomial dynamical system and the claim follows from Lemma 2. ■

Corollary 2. Let F_2 be the finite field with two elements, $f \in MF_n^n(F_2)$ a Boolean monomial dynamical system, and $F := \Psi^{-1}(f) \in M(n \times n; E_2)$ its corresponding matrix. Furthermore, let F_q be a finite field and $g \in MF_n^n(F_q)$ the monomial dynamical system whose corresponding matrix $G := \Psi^{-1}(g) \in M(n \times n; E_q)$ satisfies $\forall i, j \in \{1, \dots, n\}$

$$G_{ij} = \begin{cases} q - 1 & \text{if } F_{ij} = 1 \\ 0 & \text{if } F_{ij} = 0. \end{cases}$$

If f is a fixed point system then g is a fixed point system too.

Proof. Let $G_f = (V_f, E_f, \pi_f)$ be the dependency graph of f . By the definition of g , one can easily see that the dependency graph $G_g = (V_g, E_g, \pi_g)$ of g can be generated from G_f by adding $q - 2$ identical parallel edges for every existing edge. Obviously G_f and G_g have the same strongly connected components. If G_f does not contain any nontrivial strongly connected components, then G_g would not contain any either and by Theorem 3 g would be a fixed point system. If, on the other hand, G_f does contain nontrivial strongly connected components, then by [8, Theorem 6.1] each of those components would have loop number 1. From the definition of g it also follows for any pair of vertices $a, b \in E_g$ that $s_1(a, b) \neq 0 \Rightarrow s_1(a, b) = q - 1$. By Theorem 7 g would be a fixed point system. ■

Example 1. Let F_2 be the Boolean finite field and $f \in MF_n^n(F_2)$ the Boolean coupled monomial dynamical system defined by

$$f_1(x) = x_1^{a_{11}}$$

$$f_i(x) = \left(\prod_{j=1}^i x_j^{a_{ij}} \right), \quad i = 2, \dots, n$$

where $a_{ij} \in \{0, 1\}$, $i = 1, \dots, n$, $j = 1, \dots, i$. According to [8, Corollary 6.3], such a system is always a fixed point system. Now, let F_q be a finite field and consider $g \in MF_n^n(F_q)$, the coupled monomial dynamical system defined by

$$g_1(x) = x_1^{\mu(a_{11})}$$

$$g_i(x) = \left(\prod_{j=1}^i x_j^{\mu(a_{ij})} \right), \quad i = 2, \dots, n$$

where

$$\mu(a) := \begin{cases} q - 1 & \text{if } a = 1 \\ 0 & \text{if } a = 0. \end{cases}$$

Such a system is called *triangular*. By Corollary 2, g must be a fixed point system.

Theorem 8. Let F_q be a finite field, $f \in MF_n^n(F_q)$ a coupled monomial dynamical system, and $G_f = (V_f, E_f, \pi_f)$ its dependency graph. Then f is a fixed point system if for every vertex $a \in V_f$ that is recurrently

connected to some other vertex $b \in V_f$ the edge $a \rightarrow a$ appears exactly $q - 1$ times in E_f , that is, $|\pi_f^{-1}((a, a))| = q - 1$.

Proof. Let $V_f = \{a_1, \dots, a_n\}$ be the enumeration of the vertices and $F := \Psi^{-1}(f)$ be the corresponding matrix of f . Consider two vertices $a_i, a_j \in V_f$ such that a_i is recurrently connected to a_j . Then by Theorem 5 there is an $m_1 \in \mathbb{N}$ such that

$$s_{m_1+\gamma}(a_i, a_j) > 0 \forall \gamma \in \mathbb{N}_0. \tag{13}$$

Consider now $m_2 := \max(n, m_1)$. Due to the universality of m_1 in equation (13), for any pair of vertices $a_i, a_j \in V_G$ with a_i recurrently connected to a_j there is a sequence $a_i \rightarrow_{m_2+\gamma} a_j$ of length $m_2 + \gamma$. Consider one particular sequence $a_i \rightarrow_{m_2+\gamma} a_j$ of length $m_2 + \gamma$ and call it $w_\gamma := a_i \rightarrow_{m_2+\gamma} a_j$. By hypothesis there are exactly $q - 1$ directed edges $a_i \rightarrow a_i$. Therefore, there are $q - 1$ copies of the sequence w_γ . Since we are dealing with an arbitrary sequence $a_i \rightarrow_{(m_2+\gamma)} a_j$ of fixed length $m_2 + \gamma$, $\gamma \in \mathbb{N}_0$ we can conclude that $\exists \alpha_{ij\gamma} \in \mathbb{N}$ such that $s_{(m_2+\gamma)}(a_i, a_j) = \alpha_{ij\gamma}(q - 1) \forall \gamma \in \mathbb{N}_0$. Thus, f is a coupled $(q - 1)$ -fold redundant monomial dynamical system and the claim follows from Lemma 2. ■

Example 2. Let F_q be a finite field and $f \in MF_n^n(F_q)$ a monomial dynamical system such that the diagonal entries of its corresponding matrix $F := \Psi^{-1}(f)$ satisfy $F_{ii} = q - 1 \forall i \in \{1, \dots, n\}$. Since every vertex satisfies the requirement of Theorem 8, f must be a fixed point system.

4. An Algorithm of Polynomial Complexity to Identify Fixed Point Systems

4.1 Some Basic Considerations

Definition 17. Let X be a nonempty finite set, $n \in \mathbb{N}$ a natural number, and $f : X^n \rightarrow X^n$ a time discrete finite dynamical system. The *phase space* of f is the digraph with node set X^n , arrow set E defined as $E := \{(x, y) \in X^n \times X^n \mid f(x) = y\}$, and vertex mapping

$$\begin{aligned} \pi & : E \rightarrow X^n \times X^n \\ (x, y) & \mapsto (x, y). \end{aligned}$$

According to our definition of monomial dynamical system $f \in MF_n^n(F_q)$, the possibility that one of the functions f_i is equal to

the zero function is excluded (see Definition 3 and Remark 1). Therefore, the following algorithm is designed for such systems. However, in this algorithmic framework it would be convenient to include the more general case (as defined in [8, 13]), that is, the case when some of the functions f_i can indeed be equal to the zero function. In the vein of Remark 1 this actually only requires some type of preprocessing. The preprocessing algorithm is described and analyzed in [5, Appendix B].

Our algorithm is based on the following observation made by Dr. Michael Shapiro about general time discrete finite dynamical systems: a chain of transient states in the phase space of a time discrete finite dynamical system $f : X^n \rightarrow X^n$ can contain at most $s := |X^n| - 1 = |X|^n - 1$ transient elements. Therefore, to determine whether a system is a fixed point system, it is sufficient to establish whether the mappings f^r and f^{r+1} are identical for any $r \geq s$. In the case of a monomial system $f \in M F_n^n(\mathbb{F}_q)$, due to the isomorphism of the monoids $M(n \times n; E_q)$ and $M F_n^n(\mathbb{F}_q)$ (see Section 2), we only need to look at the corresponding matrices $F^r, F^{r+1} \in M(n \times n; E_q)$ (see also [27] in the Boolean case). Computationally, it is more convenient to generate the following sequence of powers:

$$F^2, (F^2)^2 = F^4, (F^4)^2 = F^8, (F^8)^2 = F^{16}, \dots, F^{(2^t)}.$$

To achieve the “safe” number of iterations $|F_q^n| - 1 = q^n - 1$ we need to make sure $2^t \geq q^n - 1$. This is equivalent to $t \geq \log_2(q^n - 1)$. To obtain a natural number we use the ceil function:

$$t := \text{ceil}(\log_2(q^n - 1)). \tag{14}$$

Thus we have, due to the monotonicity of the log function, $t < \log_2(q^n - 1) + 1 \leq \log_2(q^n) + 1 = n \log_2(q) + 1$.

In the Boolean case, the studies performed in [27] on upper bounds for the length of the transient part of the sequence $(F^i)_{i \in \mathbb{N}}$ of consecutive powers of F could significantly improve our algorithm. Such bounds could provide us with a better (i.e., lower) lower bound than equation (14) for t . It would be beyond the scope of this article to elaborate on these aspects of the Boolean case.

4.2 The Algorithm and Its Complexity Analysis

The algorithm is fairly simple. Given a monomial system $f \in M F_n^n(\mathbb{F}_q)$ and its corresponding matrix $F := \Psi^{-1}(f) \in M(n \times n; E_q)$:

1. With t as defined by equation (14), calculate the matrices $A := F^{2^t}$ and $B := FA$. This step requires $t + 1$ matrix multiplications.

2. Compare the n^2 entries A_{ij} and B_{ij} . This step requires at most n^2 comparisons. (This maximal value is needed in the case that f is a fixed point system.)
3. f is a fixed point system if and only if the matrices A and B are equal.

It is well known that matrix multiplication requires $2n^3 - n^2$ addition or multiplication operations. Since $t + 1 < n \log_2(q) + 2$, the number of operations required in step 1 is bounded above by $(2n^3 - n^2)(n \log_2(q) + 2)$. Summarizing, we have the following upper bound $N(n, q)$ for the number of operations in steps 1 and 2:

$$N(n, q) := (2n^3 - n^2)(n \log_2(q) + 2) + n^2.$$

For a fixed size q of the finite field F_q used it holds that

$$\lim_{n \rightarrow \infty} \frac{N(n, q)}{n^4} = 2 \log_2(q)$$

and we can conclude $N(n, q) \in O(n^4)$ for a fixed q . The asymptotic behavior for a growing number of variables and growing number of field elements is described by

$$\lim_{\substack{n \rightarrow \infty \\ q \rightarrow \infty}} \frac{N(n, q)}{n^4 \log_2(q)} = 2.$$

Thus, $N(n, q) \in O(n^4 \log_2(q))$ for $n, q \rightarrow \infty$.

It is necessary to comment on the arithmetic operations performed during the matrix multiplications. Since the matrices are elements of the matrix monoid $M(n \times n; E_q)$, the arithmetic operations are operations in the monoid E_q . The addition (resp., multiplication) operation on E_q requires an integer number addition (resp., multiplication) and a reduction using red_q (see Section 2). For a detailed description of integer number representation and arithmetic in typical computer algebra systems see [28, Chapter 4].

The reduction $\text{red}_q(a)$ of an integer number $a \in \mathbb{N}_0$, $a \geq q$ is obtained as the degree of the remainder of the polynomial division $\tau^a \div (\tau^q - \tau)$. According to [28, Section 4.6.5] this division requires $O(2(\deg(\tau^a) - \deg(\tau^q - \tau))) = O(2(a - q))$ integer number operations. However, we know that the reductions $\text{red}_q(\cdot)$ are applied to the result of (regular integer) addition or multiplication of elements of E_q and therefore

$$a - q \leq \begin{cases} 2(q - 1) - q = q - 2 \\ (q - 1)^2 - q = q^2 - q + 1. \end{cases}$$

As a consequence, in the worst case scenario, one addition (resp., multiplication) in the monoid E_q requires $O(q)$ (resp., $O(q^2)$) regular integer number operations.

Since E_q is a finite set and only the results of n^2 pairwise additions and n^2 pairwise multiplications are needed, the numbers are stored in a table after the first time they are calculated while the algorithm is running. Since most of the commercial and freely available computer algebra systems provide implementations of finite field arithmetic and arithmetic of polynomials over a finite ring, the implementation of our algorithm is a very simple task. We have successfully implemented the algorithm in MapleTM. The code can be made available from the author upon request.

Since the matrix multiplications dominate the complexity of the algorithm, for very large systems more efficient matrix multiplication algorithms could be used. Indeed, using Strassen's algorithm [29, 30], a complexity of $O(n^{\omega+1} \log_2(q))$, where $\omega \leq \log_2(7) \approx 2.807$ could be reached. The performance could be substantially improved through the use of parallelization techniques [31, 32].

It is pertinent to mention that while this article was being peer-reviewed, the article [14] was published, in which an algorithm of complexity $O(n^3 \log_2(n \log_2(q)))$ is presented, that is used to determine whether an n -dimensional linear dynamical system $L : R^n \rightarrow R^n$ over a finite ring R of cardinality $q = |R|$ is a fixed point system. While the authors of [14] did perform a complexity analysis of their algorithm, they did not elaborate on the details of a concrete computer implementation of the arithmetic operations on the finite ring R and thus, did not provide information on the computational cost of such operations.

In [13] it is stated that in order to exploit their results algorithmically, an algorithm would be required to determine whether or not a linear dynamical system $L : R^n \rightarrow R^n$ over a finite ring R is a fixed point system. The algorithm presented in [14] provides this missing ingredient. Nevertheless, for a given $f \in M F_n^n(\mathbb{F}_q)$, prior to being able to apply the algorithm from [14], a linear dynamical system $L(f) : (\mathbb{Z} / (q - 1))^n \rightarrow (\mathbb{Z} / (q - 1))^n$ and a Boolean monomial dynamical system $T(f) \in M F_n^n(\mathbb{F}_2)$ need to be constructed (see [13] for the details). The overall computational complexity of an algorithm exploiting the results of [13] and [14] still remains to be investigated.

Acknowledgments

We would like to thank Dr. Omar Colón-Reyes for his hospitality and a very fruitful academic interaction at the University of Puerto Rico, Mayagüez. We are grateful to Dr. Bodo Pareigis for offering the opportunity to participate in a great seminar at the Ludwig-Maximilians-Universität in Munich, Germany. We also would like to express our gratitude to Dr. Michael Shapiro for very helpful comments. We are grateful to Dr. Karen Duca for her support and to Dr. David Thorley-Lawson for providing an excellent research environment at the Pathology Department of Tufts University, the institute where the material for this paper was conceived. Moreover, we thank Dr. Jill Roughan, Dr. Michael Shapiro and Dr. David Thorley-Lawson for proofreading the manuscript.

The author acknowledges support by a Public Health Research Grant (RO1 AI062989) to Dr. David Thorley-Lawson at Tufts University, Boston, MA, USA. The author was affiliated with Centre for Mathematical Sciences, Munich University of Technology, Boltzmannstr.3, 85747 Garching, Germany and also with Pathology Department, Tufts University, 150 Harrison Ave., Boston, MA 02111, USA during the development of the material presented here.

References

- [1] A. W. Burks, ed., *Essays on Cellular Automata*, Urbana, IL: University of Illinois Press, 1970.
- [2] J. Reger and K. Schmidt, "Modeling and Analyzing Finite State Automata in the Finite Field F_2 ," *Mathematics and Computers in Simulation*, 66(2-3), 2004 pp. 193-206. doi .1016/j.matcom.2003.11.005.
- [3] C. L. Barrett, H. S. Mortveit, and C. M. Reidys, "Elements of a Theory of Simulation II: Sequential Dynamical Systems," *Applied Mathematics and Computation*, 107(2-3), 2000 pp. 121-136. doi.10.1016/S0096-3003(98)10114-5.
- [4] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Vol. 20 (*Encyclopedia of Mathematics and Its Applications*), New York: Cambridge University Press, 1997 (foreword by P. M. Cohn).
- [5] E. Delgado-Eckert, "Monomial Dynamical and Control Systems over a Finite Field and Applications to Agent-Based Models in Immunology," Ph.D. thesis, Munich, Germany: Technische Universität München, 2008. <http://mediatum2.ub.tum.de/doc/645326/document.pdf>.
- [6] J. Kari, "Theory of Cellular Automata: A Survey," *Theoretical Computer Science*, 334(1-3), 2005 pp. 3-33. doi.10.1016/j.tcs.2004.11.021.
- [7] R. Bartlett and M. Garzon, "Monomial Cellular Automata," *Complex Systems*, 7(5), 1993 pp. 367-388.
- [8] O. Colón-Reyes, R. Laubenbacher, and B. Pareigis, "Boolean Monomial Dynamical Systems," *Annals of Combinatorics*, 8(4), 2004 pp. 425-439. doi.10.1007/s00026-004-0230-6.

- [9] A. Khrennikov and M. Nilsson, "On the Number of Cycles of p -adic Dynamical Systems," *Journal of Number Theory*, 90(2), 2001 pp. 255-264. doi.10.1006/jnth.2001.2665.
- [10] M. Nilsson, "Fuzzy Cycles of p -adic Monomial Dynamical Systems," *Far East Journal of Dynamical Systems*, 5(2), 2003 pp. 149-173.
- [11] T. Vasiga and J. Shallit, "On the Iteration of Certain Quadratic Maps over $GF(p)$," *Discrete Mathematics*, 277(1-3), 2004 pp. 219-240.
- [12] O. Colón-Reyes, *Monomial Dynamical Systems over Finite Fields*, Ph.D. thesis, Blacksburg, VA: Virginia Tech., 2005.
- [13] O. Colón-Reyes, A. S. Jarrah, R. Laubenbacher, and B. Sturmfels, "Monomial Dynamical Systems over Finite Fields," *Complex Systems*, 16(4), 2006 pp. 333-342.
- [14] G. Xu and Y. M. Zou, "Linear Dynamical Systems over Finite Rings," *Journal of Algebra*, 321(8), 2009 pp. 2149-2155.
- [15] E. Delgado-Eckert, "Boolean Monomial Control Systems," *Mathematical and Computer Modelling of Dynamical Systems*, 15(2), 2009 pp. 107-137. doi.10.1080/13873950902808594.
- [16] B. Elspas, "The Theory of Autonomous Linear Sequential Networks," *IRE Transactions on Circuit Theory*, 6(1), 1959 pp. 45-60.
- [17] R. A. Hernández Toledo, "Linear Finite Dynamical Systems," *Communications in Algebra*, 33(9), 2005 pp. 2977-2989. doi.10.1081/AGB-200066211.
- [18] J. Reger and K. Schmidt, "A Finite Field Framework for Modeling, Analysis and Control of Finite State Automata," *Mathematical and Computer Modelling of Dynamical Systems (MCMDS)*, 10(3-4), 2004 pp. 253-285. doi.10.1080/13873950412331300142.
- [19] D. K. Milligan and M. J. D. Wilson, "The Behavior of Affine Boolean Sequential Networks," *Connection Science*, 5(2), 1993 pp. 153-167.
- [20] P. Cull, "Linear Analysis of Switching Nets," *Biological Cybernetics*, 8(1), 1971 pp. 31-39. doi.10.1007/BF00270831.
- [21] W. Just, "The Steady State System Problem Is NP-Hard Even for Monotone Quadratic Boolean Dynamical Systems." (Jun 3, 2006) www.math.ohiou.edu/~just/PAPERS/monNPh14.pdf.
- [22] F. Harary, R. Z. Norman, and D. Cartwright, *Structural Models: An Introduction to the Theory of Directed Graphs*, New York: Wiley & Sons, 1965.
- [23] V. Pták and I. Sedláček, "On the Index of Imprimitivity of Nonnegative Matrices," *Czechoslovak Mathematical Journal*, 8(83), 1958 pp. 496-501.
- [24] E. V. Denardo, "Periods of Connected Networks and Powers of Nonnegative Matrices," *Mathematics of Operations Research*, 2(1), 1977 pp. 20-24. doi.10.1287/moor.2.1.20.
- [25] R. A. Brualdi and H. J. Ryser, *Combinatorial Matrix Theory*, Vol. 39 (*Encyclopedia of Mathematics and Its Applications*), New York: Cambridge University Press, 1991.
- [26] P. Lancaster and M. Tismenetsky, *The Theory of Matrices: With Applications*, 2nd ed., (*Computer Science and Applied Mathematics*). Orlando, FL: Academic Press Inc., 1985.

- [27] B. De Schutter and B. De Moor, "On the Sequence of Consecutive Powers of a Matrix in a Boolean Algebra," *SIAM Journal on Matrix Analysis and Applications*, 21(1), 1999 pp. 328-354. doi.10.1137/S0895479897326079.
- [28] M. Kaplan, *Computer algebra*, Berlin: Springer-Verlag, 2004.
- [29] V. Strassen, "Gaussian Elimination Is Not Optimal," *Numerische Mathematik*, 13(4), 1969 pp. 354-356.
- [30] D. H. Bailey, K. Lee, and H. Simon, "Using Strassen's Algorithm to Accelerate the Solution of Linear Systems," *The Journal of Supercomputing*, 4(4), 1991 pp. 357-371. doi .10.1007/BF00129836.
- [31] M. Ben-Ari, *Principles of Concurrent and Distributed Programming: Algorithms and Models*, 2nd ed., New York: Addison-Wesley, 2006.
- [32] A. Pollard, D. J. K. Mewhort, and D. F. Weaver, eds., *High Performance Computing Systems and Applications*, New York: Springer-Verlag, 2000.