DYNAMICS OF LINEAR SYSTEMS
OVER FINITE COMMUTATIVE RINGS

YANGJJIANG WEI, GUANGWU XU, AND YI MING ZOU

Abstract. The dynamics of a linear dynamical system over a finite field can be described by using the elementary divisors of the corresponding matrix. It is natural to extend the investigation to a general finite commutative ring. In a previous publication, the last two authors developed an efficient algorithm to determine whether a linear dynamical system over a finite commutative ring is a fixed point system or not. The algorithm can also be used to reduce the problem of finding the cycles of such a system to the case where the system is given by an automorphism. Here, we further analyze the cycle structure of such a system and develop a method to determine its cycles.

1. Introduction

Let $R$ be a commutative ring with 1, let $M$ be an $R$-module, and let $f : M \rightarrow M$ be an $R$-module endomorphism. We may consider $f$ as a dynamical system via iteration:

\[ f, \ f^2 = f \circ f, \ \cdots, \ f^m = f \circ \cdots \circ f, \ \cdots, \]

and investigate the behaviors of the system. For our convenience, we set $f^0 = id$. By studying the dynamics of the system, we mean to investigate its possible cycles (including fixed points) generated by the elements of $M$. It is clear that if the cardinality of $M$ is infinite, then there may not be any cycle except the obvious fixed point 0. But if $M$ is finite, then for any initial input $a \in M$, the sequence $f^m(a)$, $m \geq 0$, will eventually either stabilize or enter a cycle. We should restrict our attention to the case where both $R$ and $M$ are finite in this paper, and we call such a system a linear dynamical system over the finite ring $R$.

If $R = F$ is a finite field, then $M$ is a finite dimensional vector space over $F$, and the dynamics of $f$ can be described by using the elementary
divisors of the $F$-linear map $f$. Suppose the elementary divisors of $f$ are (see [7], pp. 356-357):

$$p_i^{m_{ij}}, \ 1 \leq i \leq s, \ 1 \leq j \leq k_i,$$

where each $p_i$ is an irreducible polynomial in $F[x]$, and the $m_{ij}$ are integers such that for each $i$,

$$m_{i1} \geq m_{i2} \geq \cdots \geq m_{ik_i} > 0.$$

Then there are $f$-cyclic subspaces $M_{ij}$ (i.e. there exists a vector $v \in M_{ij}$ and an integer $k \geq 0$ such that $(v, f(v), \ldots, f^k(v))$ is a basis of $M_{ij}$) with minimal polynomial $p_i^{m_{ij}}, \ 1 \leq i \leq s, \ 1 \leq j \leq k_i$, such that $M$ is a direct sum of the $M_{ij}$’s.

It is easy to see (over any ring $R$) that if $M = M_1 \oplus M_2$ is a direct sum decomposition of $f$-invariant submodules (we will just call them $f$-submodules), and $C_i$ is a cycle in $M_i$ of length $c_i$ ($i = 1, 2$), then the direct product

$$C_1 \times C_2 := \{(a, b) \mid a \in M_1, \ b \in M_2\}$$

offers $\text{GCD}(c_1, c_2)$ cycles of length $\text{LCM}(c_1, c_2)$ for the module $M$. So we can just work with each direct summand independently.

Therefore, the problem of finding the cycles (including fixed points) of $f$ (over a field $F$) reduces to the problem of finding the cycles of the restricted linear maps

$$f_{ij} = f|_{M_{ij}} : M_{ij} \to M_{ij}, \ 1 \leq i \leq s, \ 1 \leq j \leq k_i.$$

If $p_i = x$, the corresponding linear maps $f_{ij}, \ 1 \leq j \leq k_i$, are nilpotent and thus all have just one fixed point 0 and have no cycle of length $> 1$. So the question is to find the cycle structures of those $f_{ij}$ such that the corresponding $p_i$ are not $x$ (these $f_{ij}$ are automorphisms of the $M_{ij}$). For these cases, since the characteristic polynomial of each $f_{ij}$ is equal to its minimal polynomial, Elspas’ formula describes its cycle structure [4][6] (we use $g_{ij}^k$ instead of $p_i^{m_{ij}}$ to simplify the notation in the formula):

$$G_{ij} = 1 + \sum_{k=1}^{s} \frac{q^{mk} - q^{m(k-1)}}{c_k} C_k,$$

where $q = |F|$, 1 corresponds to the fixed point 0, $C_k$ is a cycle of length $c_k$, and $c_k = \text{ord}(g_{ij}^k)$ (i.e. $c_k$ is the least positive integer $t$ such that $g_{ij}^k$ divides $x^t - 1$). This formula gives a nice description of the cycle structure, though the actual computation is more involved: one first computes the normal form of the matrix $xI - A$, where $A$ is the matrix of $f$ with respect to a basis of $M$, or computes its minimum polynomial.
m(f), then factors the polynomials that appear in the normal form of 
$I - A$ (or $m(f)$) to get the $g_{ij}^k$, and then computes the order of each 
g_{ij}^k.

Note that if $g_{ij}^k$ divides $x^t - 1$, then all $g_{ij}^s$, $0 \leq s \leq k$, divide $x^t - 1$. So by the comment about the cycles of a direct sum of $f$-modules, we have:

**Lemma 1.1.** The $F$-module endomorphism $f$ possesses a cycle of maximum length, say $c$, such that all other cycle lengths are divisors of $c$.

For a general finite commutative ring $R$, since the factorization in $R[x]$ may not be unique, different approaches are needed. The study of linear dynamical systems over rings of the form $\mathbb{Z}_q$ was suggested in [2] due to its relation with monomial dynamical systems over finite fields. In [1] an approach by using Fitting’s lemma [7]: there is a positive integer $k$ such that $M = \ker f^k \oplus \text{Im} f^k$ was suggested. However, the key to the success of the proposed approach, which is to find a proper $k$ and compute $f^k$ efficiently, was not treated. In [9], an upper bound for $k$ was determined, and an algorithm that runs in time $O(n^3 \log(n \log(q)))$, where $n$ is given by $M = \mathbb{Z}^n$ and $q = |R|$, to compute $f^k$ was developed. The results of [9] provide a solution to the problem of determining whether or not such a system is a fixed point system, and also reduce the problem of finding the cycle structure of such a system to that of an automorphism (since $f : \text{Im} f^k \rightarrow \text{Im} f^k$ is bijective).

The main idea of [9] is, to determine the cycles of $f$, we can just consider the $f$-module $M$ as an abelian group ($\mathbb{Z}$-module) and determine the lengths of the cycles. After obtaining the information on the lengths of the cycles, we can find the cycles by solving linear systems of the form $(f^c - I)X = 0$, where $I$ is the identity map and $c$ is a cycle length. By the structure theorem of finitely generated abelian groups [7], we can assume that

\[ \text{Im} f^k = \mathbb{Z}_{p_1^{a_1}} \oplus \mathbb{Z}_{p_2^{a_2}} \oplus \cdots \oplus \mathbb{Z}_{p_m^{a_m}}, \]

where $p_1, \ldots, p_m$ are (not necessarily distinct) primes, and $a_1, \ldots, a_m$ are (not necessarily distinct) positive integers.

We further note that an $f$-module as in (1.1) can be written as a direct sum of $f$-submodules such that each of these submodules is formed by grouping those $\mathbb{Z}_{p_i^{a_i}}$’s with the same prime $p_i$ together. As discussed before, whenever we have a direct sum of $f$-submodules, we can just work with each direct summand independently. Therefore, our goal here is to analyze the cycle structure of an automorphism of an
abelian group of the form ($p$ is a prime):

\begin{equation}
M = \mathbb{Z}_{p^{a_1}} \times \mathbb{Z}_{p^{a_2}} \times \cdots \times \mathbb{Z}_{p^{a_m}}, 1 \leq a_1 \leq a_2 \leq \ldots \leq a_m.
\end{equation}

(1.2)

Since abelian groups are $\mathbb{Z}$-modules, an endomorphism of $M$ can be represented by an integer matrix $A$; and if all $a_i$’s are $1$, i.e. $M = \mathbb{Z}_p^m$, it is an endomorphism of the vector space $M$ over the field $\mathbb{Z}_p$. In the case where all $a_i$’s are the same, i.e. $M = \mathbb{Z}_p^{a}$, an approach was developed in [3] for an arbitrary endomorphism of $M$ using number theory techniques based on congruence of integers.

In this paper, we consider the general case where $M$ is defined by (1.2) such that the $a_i$’s are not necessary the same. Our emphasis is on the computation of the cycles; and for that, we need to be able to compute the possible cycle lengths efficiently. In Section 2, we give an upper bound for the cycle lengths such that all possible cycle lengths are factors of the given upper bound. The factors of the given upper bound are obtained from the induced linear systems over the finite field $\mathbb{Z}_p$, and thus there is no extra work needed to factor the upper bound. The results of this paper and the results in [9] together provide an algorithm to determine the cycles structure of a linear dynamical system over a finite commutative ring. The algorithm is given in Section 3. We consider three examples in Section 4. The first example shows that the given upper bound for the cycle lengths is sharp, and the third example is a linear system derived from a real world cancer regulatory network.

2. Result

We begin by collecting some general facts. The following lemma holds for any ring $R$.

**Lemma 2.1.** Let $M, N$ be $R$-modules, let $\varphi : M \to N$ be an onto $R$-module homomorphism, and let $K = \ker \varphi$. If $f : M \to M$ is an $R$-module endomorphism such that $f(K) \subseteq K$, then $f$ induces an $R$-module endomorphism $\bar{f}$ of $N$ by $\bar{f}(\varphi(m)) = \varphi(f(m)), m \in M$.

**Proof.** The proof is a straightforward verification of the definition. □

Recall that we work with a finite commutative ring $R$ and a finite $R$-module, so it is possible to use a reduction approach to find the cycles of an $R$-module endomorphism $f$. For this purpose, we investigate the relationships among the cycles of the $f$-modules $M$, $N$, and $K$ (notation as in Lemma 2). For any $m \in M$, we denote by $\ell(m)$ the length of the cycle generated by $m$ (if $m$ lies on a cycle). We have the following simple fact about fixed points:
Proof. We have that $u_1 = u + w$ is a fixed point $\iff f(u + w) = u + f(w) = u + w \iff f(w) = w$. \hfill \Box

From now on, we assume that $f$ is an automorphism. Then every element of $M$ lies in a cycle. Note that by our assumption on $M$, $p^a_m(M) = 0$ (see (1.2)), thus $p^a_m(K) = 0$. Suppose that $a$ is the least positive integer $i$ such that $p^i(K) = 0$. For $u \in M$, let $\varphi(u) = v \in N$, and let $\ell(v) = s$. With these assumptions, we have $f^s(u) = u + w$ for some $w \in K$. Let $\ell(w) = k$. We will write $[s, k]$ (respectively, $(s, k)$) for the least common multiple (respectively, the greatest common divisor) of $s$ and $k$.

Lemma 2.2. There exists $0 \leq b \leq a$ such that $\ell(u) = p^b[s, k]$.

Proof. Let $\ell(u) = c$. Since $f^c(u) = u$, $\bar{f}^c(v) = v$ in $N$. So $c$ is a multiple of $s$. Let $c = ts$, then from $f^s(u) = u + w$ we have $w = f^s(u) - u$ and $u = f^{ts}(u) = f^{(t-1)s}(u) + f^{(t-1)s}(w)$.

Applying $f^s$ to this equation we have $f^c(w) = w$, which implies that $c$ is also a multiple of $k$. Thus $c$ is a common multiple of $s$ and $k$, say $c = c_0[s, k]$ for some positive integer $c_0$. This holds without the assumption that $p^a(K) = 0$. If $p^a(K) = 0$, we will have $c_0 = p^b$ for some $0 \leq b \leq a$.

To see that, let $[s, k] = ns$, where $n = \frac{k}{(s, k)}$. Start with $f^s(u) = u + w$ and compute inductively, we have

$$f^{ns}(u) = u + w + f^s(w) + \cdots + f^{(n-1)s}(w). \tag{2.1}$$

Note that since $ns$ is a multiple of $k$, $(f^{ns} - I)(w) = 0$, which implies $$(f^s - I)(w + f^s(w) + \cdots + f^{(n-1)s}(w)) = 0,$$

that is

$$w_1 := w + f^s(w) + \cdots + f^{(n-1)s}(w)$$

is a fixed point of $f^s$. If $w_1 = 0$, then $c = [s, k]$. However, we do not know if $w_1 = 0$ or not, so we use the assumption that $p^a(K) = 0$. Start from (2.1): $f^{ns}(u) = u + w_1$, note that $w_1$ is a fixed point of $f^{ns}$, we have

$$f^{p^a ns}(u) = (f^{ns})^{p^a}(u) = u + p^a w_1 = u. \quad \text{ (since } w_1 \in K)$$
Thus \( \ell(u) \) is a factor of \( p^n a \), which implies \( c_0 = p^b \) for some \( 0 \leq b \leq a \). \( \square \)

We now assume that \( f : M \rightarrow M \) is a \( \mathbb{Z} \)-module automorphism, where \( M \) is defined by (1.2). Note that \( p^{m_i}(M) = 0 \). For each \( 0 \leq i \leq a_m \), we define

\[
M_i = \{ v \in M \mid p^i v = 0 \}.
\]

Then each \( M_i \) is an \( f \)-submodule of \( M \). Consider the \( f \)-submodule filtration

\[
(2.2) \quad M_0 = (0) \subset M_1 \subset \cdots \subset M_{a_m-1} \subset M_{a_m} = M.
\]

There are positive integers \( k_i \leq m \), \( 1 \leq i \leq a_m \), such that the quotients

\[
M_i / M_{i-1} \cong \mathbb{Z}_p^{k_i}, \quad 1 \leq i \leq a_m.
\]

The automorphism \( f \) induces automorphisms

\[
\bar{f}_i : M_i / M_{i-1} \cong \mathbb{Z}_p^{k_i} \rightarrow M_i / M_{i-1} \cong \mathbb{Z}_p^{k_i}, \quad 1 \leq i \leq a_m.
\]

Since \( \mathbb{Z}_p \) is a field, the dynamics of these automorphisms can be determined as discussed in the introduction section. For each \( 1 \leq i \leq a_m \), let the set of cycle lengths of \( \bar{f}_i \) be \( L_{ij} = \{ c_{ij} : 1 \leq j \leq \ell_i \} \), where \( \ell_i \) is a positive integer depending on \( i \). We assume that \( c_{i1} > c_{ij}, \quad 1 \leq i \leq a_m, \quad 1 < j \leq \ell_i \). Then by Lemma [1.1] for any \( 1 \leq i \leq a_m, \quad c_{ij} | c_{i1} \) for all \( 1 \leq j \leq \ell_i \).

**Theorem 2.1.** Assume that \( f : M \rightarrow M \) is a \( \mathbb{Z} \)-module automorphism, where \( M \) is defined by (1.2), and keep the notation introduced above.

1. For each integer \( c_{i1} \) \( (1 \leq i \leq a_m) \), the dynamical system \( f : M \rightarrow M \) possesses a cycle whose length is a multiple of \( c_{i1} \).

2. All cycle lengths of \( f \) are factors of

\[
(2.4) \quad p^{a_m-1} \cdot \text{LCM}(c_{11}, c_{21}, \ldots, c_{a_m1}),
\]

where \( \text{LCM} \) stands for the least common multiple.

**Proof.** (1) For a fixed \( 1 \leq i \leq a_m \), choose \( u \in M_i \) such that its image \( \bar{u} \in M_i / M_{i-1} \) belongs to a cycle of length \( c_{i1} \). If the cycle to which \( u \) belongs has length \( c \), then \( f^c(u) = u \) and hence \( f^c(\bar{u}) = \bar{f}^c(u) = \bar{u} \) in \( M_i / M_{i-1} \), which implies that \( c_{i1} | c \).

(2) We use induction on \( a_m \). There is nothing to prove if \( a_m = 1 \) since \( f \) is just an automorphism of the vector space \( M = \mathbb{Z}_p^m \). Let \( a_m \geq 2 \). Then since \( f \) induces an automorphism of each \( f \)-submodule \( M_i \) in (2.2), it induces an automorphism of

\[
M / M_1 \cong \mathbb{Z}_{p^{a_1-1}} \times \mathbb{Z}_{p^{a_2-1}} \times \cdots \times \mathbb{Z}_{p^{a_m-1}}.
\]
The filtration of (2.2) induces the following filtration:

\((0) = M_1/M_1 \subset M_2/M_1 \subset \cdots \subset M_{a_m-1}/M_1 \subset M/M_1.\)

Since for \(2 \leq i \leq a_m\)

\((2.6) \quad (M_i/M_1)/(M_{i-1}/M_1) \cong M_i/M_{i-1},\)

by the induction assumption, we have that the possible cycle lengths of \(M/M_1\) are factors of \(r = p^{a_m-2} \text{LCM}(c_{21}, \ldots, c_{a_m}).\) Now the theorem follows by noticing \(p(M_1) = 0\) and applying Lemma 1.1 to \(M_1\) and Lemma 2.1 to the projection \(M \to M/M_1.\)

\(\square\)

**Corollary 2.1.** If \(M = \mathbb{Z}_p^m\) (i.e. the case where all \(a_i\) are equal), the cycle lengths are factors of \(p^{a-1}c\), where \(c\) is the maximum cycle length of \(M/M_{a-1} \cong \mathbb{Z}_p\) with the module structure induced by \(f\).

*Proof.* Consider the onto \(f\)-module homomorphism \(\varphi : M \to M_i/M_{i-1}\) defined by first taking \(m \to p^{a-1}m, \ m \in M\), and then follows by the projection from \(M_i\) onto \(M_i/M_{i-1}\). This homomorphism induces an \(f\)-module isomorphism \(M/M_{a-1} \to M_i/M_{i-1}\) since its kernel is \(M_{a-1}\). Thus all \(M_i/M_{i-1}\) (\(2 \leq i \leq a\)) are isomorphic as \(f\)-modules and have the same cycle structure, which implies that \(c_{11} = c\) for all \(i\), and the corollary follows from (2) of the theorem. \(\square\)

We remark that if \(f\) is not an automorphism then the above corollary does not apply, since not every element of \(M\) lies in a cycle.

### 3. Computing the Cycles

Under the assumption that the cycle lengths of a linear system over a finite field can be computed, we can use Theorem 2.1 to find the cycles of a linear system \(f : M \to M\) over a finite commutative ring \(R\). Our algorithm is divided into four steps.

1. **Reduce to an automorphism.** By Theorem 2.1 of [9] \(N = m \log_2(q)\) satisfies \(f^{N+1}(M) = f^N(M),\) where \(q = |R|,\) and \(m\) is given by a presentation of the \(R\)-module \(M\) as a quotient of the free module \(R^m: \)

\[\varphi : R^m \to M \text{ and } R^m/\ker(\varphi) \cong M.\]

Therefore we have an induced automorphism \(f : f^N(M) \to f^N(M).\) Consider the structure of the finitely generated abelian

\[\text{The assumption on the module considered in Theorem 2.1 [9] is somewhat different, but a quick check of the proof there reveals that it also applies to the case here.}\]
group \( f^N(M) \), and reduce it to the case where the module is defined by (1.2). Thus we assume the module \( M \) is defined by (1.2) in steps 2 – 4.

(2) **Compute the number** \( c_{i1} \) **for each induced automorphism** (see the paragraph precedes Theorem 1)

\[
\bar{f}_i : \mathbb{Z}_p^k_i \to \mathbb{Z}_p^k_i, 1 \leq i \leq a_m.
\]

If the minimal polynomial of \( \bar{f}_i \) is \( g_i \) and \( g_i = g_1^{r_{i1}} \cdots g_{is_i}^{r_{is_i}} \) is its irreducible factorization, then \( c_{i1} = \text{LCM}(h_{i1}, \ldots, h_{is_i}) \), where \( h_{ij} = \text{ord}(g_{ij}^{r_{ij}}) \). Since \( \mathbb{Z}_p \) is a field, one can use the existing approaches [4][6]. See also the discussions later.

(3) **Compute the order of** \( f \) **as an element of the automorphism group of** \( M \). Let \( n := p^{a_m-1} \cdot \text{LCM}(c_{11}, c_{21}, \ldots, c_{a_m1}) \). Then \( n \) is a multiple of the order of \( f \). Since the factorization of \( n \) is known from step 2 and step 3, we can use the following procedure to compute the order of \( f \):

```
Input: n — a multiple of the order of f.
Output: ord — the order of f.

ord ← n;
while (1) do
ordsmaller ← 0;
for (each prime factor p of ord)

if (f^{ord\_p} = I)
ord ← ord\_p;
ordsmaller ← 1;
break;
if (ordsmaller = 0)
return ord;
```

(4) **Compute the cycle lengths and the cycles.** Let the order of \( f \) be \( a \). Then the cycle lengths of \( f \) are given by the factors of \( a \), which are known from step 2. For a factor \( d \) of \( a \), solve the linear system \((f^d - I)X = 0\) to obtain the cycles of length \( d \).

**Analysis of the algorithm.** We ignore the factors contributed by \( q = |R| \) in our analysis, since for application purposes we can assume that \( q \) is relatively small.

In step 1, the computation of \( f^N \) takes time \( O(m^3) \). Also, to find the structure of the abelian group \( f^N(M) \), it requires to compute the
Smith normal form of the integer matrix of $f : f^N(M) \to f^N(M)$. It is well-known that the computation of the Smith normal form takes time $O(m^3)$.

In step 3, the given algorithm computes the order of $f$ in time $O(m^3)$ since computing $f^a/p$ requires at most time $O(m^2 \sqrt{m \log(m)})$.

The computations in step 4 are straightforward.

Since we could not find any readily accessible reference on the algorithm and its analysis for the case where $R = \mathbb{Z}_p$ is a field, we give a discussion of the complexity of step 2 as follows.

1. There is a randomized algorithm [8] to compute the minimal polynomial $m(x)$ of a linear map $T : \mathbb{Z}_p^k \to \mathbb{Z}_p^k$ in time $O(k^3)$ and uses $O(k)$ random vectors. Since $k \leq m$, this computation requires expected time no worse than $O(m^3)$.

2. To factorize $m(x)$, some algorithms from [5] can be used. Assume the degree of $m(x)$ is $d$ and let $M(d)$ be the number of field operations needed for multiplying two polynomials of degree at most $d$, then $m(x)$ can be factorized in expected number of $O(dM(d) \log(dp))$ field operations. Since $d \leq m$, this requires time no worse than $O(m^3)$.

3. Note that if $g(x)$ is an irreducible polynomial with ord$(g) = \alpha$, then ord$(g^u) = \alpha p^c$ where $c$ is the smallest integer such that $p^c \geq u$ [6].

Thus, our algorithm runs in expected time $\sim \tilde{O}(m^3)$.

4. Conclusion and Examples

We have developed an efficient algorithm to determine the cycle structure of a linear dynamical system over a finite commutative ring with identity and thus provided a solution to this problem.

We conclude our paper by considering three examples. The first example shows that the bound given by (2.4) is sharp.

**Example 4.1.** Let $R = \mathbb{Z}_{16}$, let $M = \mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_{16}$, and let $f : M \to M$ be defined by

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

with respect to the generators $e_1 = (1,0,0)^t$, $e_2 = (0,1,0)^t$, $e_3 = (0,0,1)^t$ of $M$. Then $a_m = 4,$

$$M_0 = (0) \subset M_1 = <2e_1, 4e_2, 8e_3> \subset M_2 = <e_1, 2e_2, 4e_3> \subset M_3 = <e_1, e_2, 2e_3> \subset M_4 = M,$$
and

\[ M_4/M_3 \cong \mathbb{Z}_2, \quad M_3/M_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2, \]
\[ M_2/M_1 \cong M_1/M_0 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2. \]

It is easy to see that the restriction of \( f \) to any of these quotients is the identity map, so \( c_{ij} = 1 \) for \( 1 \leq i \leq 4 \). Thus according to Theorem 2.1, the possible cycle lengths are factors of \( 2^3 \). For this example, there are cycles for each of the possible factors of \( 2^3 \). For instance, the cycle generated by \( 2e_1 + 2e_2 \) has length 2, the cycle generated by \( e_2 \) has length 4, and the cycle generated by \( e_3 \) has length 8.

The second example shows that there may not be a cycle of length \( p^b c \) (see Corollary 2.1 for notation) for any \( b > 0 \).

**Example 4.2.** For any prime \( p \) and any integers \( a, n > 1 \), consider the \( \mathbb{Z}_{p^a} \)-module \( \mathbb{Z}_{p^n} \) and the automorphism \( f \) defined by the cyclic permutation of the standard basis \( (e_1, e_2, \ldots, e_n) \):

\[ e_1 \rightarrow e_2 \rightarrow e_3 \rightarrow \cdots \rightarrow e_n \rightarrow e_1. \]

Then the order of \( f \) is \( n \) and the cycle lengths are the factors of \( n \) (for each \( d \mid n \), the non-zero element \( e_1 + e_{d+1} + e_{2d+1} + \cdots + e_{n-d+1} \) generates a cycle of length \( d \)).

Next, we use a simplified version of the network given by the diagram of Fig. 2B in [10] to construct an example. The original network consists of 29 nodes, the 7 red output nodes that having a single input node are omitted to make the presentation more streamline (these output nodes add very little extra to the computation). The omitted nodes are: FLIP, A20, RANTES, FasT, GZMB, MEK, and LCK. Our purpose here is to give an example from a real world network, finding a good linear model over a finite ring for the underlying biological system is beyond our scope here. We introduce the variables as in Table 1.

| IL15 | RAS | ERK | JAK | IL2RBT | STAT3 | IFNGT | FasL |
|------|-----|-----|-----|--------|-------|-------|------|
| \( x_1 \) | \( x_2 \) | \( x_3 \) | \( x_4 \) | \( x_5 \) | \( x_6 \) | \( x_7 \) | \( x_8 \) |
| PDGF | PDGFR | PI3K | IL2 | BclxL | TPL2 | SPHK | SIP |
| \( x_9 \) | \( x_{10} \) | \( x_{11} \) | \( x_{12} \) | \( x_{13} \) | \( x_{14} \) | \( x_{15} \) | \( x_{16} \) |
| sFas | Fas | DISC | Caspase | Apoptosis | IL2RAT |
| \( x_{17} \) | \( x_{18} \) | \( x_{19} \) | \( x_{20} \) | \( x_{21} \) | \( x_{22} \) |

**Table 1.** Legend of variable names of the network given by Fig. 2B in [10] (with 7 red output nodes omitted).
Example 4.3. The base ring is \( \mathbb{Z}_9 \) and the state space is \( \mathbb{Z}_9^{22} \). The update functions of the nodes are provided in Table 2.

|   | \( f_1 \) | \( f_2 \) | \( f_3 \) | \( f_4 \) | \( f_5 \) | \( f_6 \) | \( f_7 \) | \( f_8 \) |
|---|---|---|---|---|---|---|---|---|
| \( x_1 \) | \( x_1 \) | \( x_2 \) | \( x_1 \) | \( x_1 \) | \( x_4 \) | \( 3x_5 + x_6 \) | \( 2x_3 + x_5 + 3x_{14} \) |
| \( f_9 \) | \( f_{10} \) | \( f_{11} \) | \( f_{12} \) | \( f_{13} \) | \( f_{14} \) | \( f_{15} \) | \( f_{16} \) |
| \( x_9 \) | \( x_9 \) | \( x_{10} \) | \( -x_4 - x_{13} \) | \( -x_4 - x_{13} \) | \( x_{11} \) | \( 2x_{11} + x_{16} \) | \( x_{15} \) |
| \( f_{17} \) | \( f_{18} \) | \( f_{19} \) | \( f_{20} \) | \( f_{21} \) | \( f_{22} \) |
| \( x_{15} \) | \( -4x_1 - 4x_{11} - x_{17} \) | \( x_{18} \) | \( -x_1 + x_{19} \) | \( x_{20} \) | \( x_{12} \) |

Table 2. The update functions of the network given by Fig. 2B in [10]. The functions are
\[ f_1 = x_1, \quad f_2 = x_1, \quad f_3 = x_2, \ldots, \]
\[ f_8 = 2x_3 + x_5 + 3x_{14}, \text{ etc.} \]

Let \( A \) be the matrix of the above linear system with respect to the standard basis \((e_1, e_2, \ldots, e_{22})\). According to Theorem 2.1 of [9], the upper bound of the exponent for \( A^m \) to stabilize (i.e. \( A^{m+1}(\mathbb{Z}_9^{22}) = A^m(\mathbb{Z}_9^{22}) \)) is \( 22 \ln(9) < 48 \). So we take \( N = 48 \) and let \( B = A^N \). To find the cycle structure of \( A \), we need to find the cycle structure of the induced linear map (the other part is the kernel of \( B \)):
\[ A : B(\mathbb{Z}_9^{22}) \to B(\mathbb{Z}_9^{22}). \]

We make the following observation: if \( U \) and \( V \) are invertible matrices over \( \mathbb{Z}_9 \) such that \( UBV \) is the Smith normal form for \( B \), we can obtain the cycle lengths of \( A \) from the cycle lengths of \( UAU^{-1} \) as follows. Note that \( UABV = UA(U^{-1})(UBV) \) and \( UBV \) is a diagonal matrix. Since \( UBV \) gives the structure of the finite abelian group under consideration, we can read the action of \( UAU^{-1} \) from the corresponding upper left submatrix of \( UABV \) (i.e. we can just compute \( UABV \)).

Our computation showed that the abelian group generated by the columns of \( UBV \) is isomorphic to \( \mathbb{Z}_9^4 \), and the action induced by \( A \) is given by the following matrix:
\[ S = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \]

The elementary divisors of \( S \) over the field \( \mathbb{Z}_3 \) are \( x + 2, \ x + 1, \) and \( x^2 + x + 1, \) and the corresponding orders are \( 1, 2, \) and \( 3 \). Thus, according to Theorem 2.1, the possible cycles lengths are the factors of \( 3 \cdot 6 = 18 \).

By considering \( A^kB = B \), we find that the order of \( S \) is 18. This can also be obtained by computing the order of \( S \) modulo 9 directly. Thus,
the cycle lengths of the linear model are $1, 2, 3, 6, 9,$ and $18$. All the computations can be done using the *LinearAlgebra* package of *MAPLE* in less than one second. We remark that the computation can also be done in about the same amount of time for the full 29-node network.

**Acknowledgment.** Part of the work in this paper was done during the visit of YJW to the Department of Mathematical Sciences at the University of Wisconsin-Milwaukee in the summer of 2015. YJW wishes to thank the University of Wisconsin-Milwaukee and its faculty for the hospitality she received during her visit.

**References**

[1] D. Bollman, O. Colón-Reyes, and E. Orozco, Fixed points in discrete models for regulatory genetic networks, EURASIP Journal on Bioinformatics and Systems Biology, On-line ID 97356 (2007), 8 pages.

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

[3] G. Deng, Cycles of linear dynamical systems over finite local rings, Journal of Algebra, 433 (2015), pp. 243-261.

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

[5] J. von zur Gathen, and J. Gerhard, Modern Computer Algebra, Cambridge Press, 2003.

[6] A. Hernández-Toledo, Linear finite dynamical systems, Communications in Algebra, 33 (2005), pp. 2977-2989.

[7] T. W. Hungerford, Algebra, GTM 73 (1974), Springer.

[8] M. M. Neunhöffer, and C. E. Praeger, Computing minimal polynomials of matrices, LMS J. Comput. and Math. 11 (2008), pp. 252–279.

[9] G. Xu, and Y. M. Zou, Linear dynamical systems over finite rings, Journal of Algebra, 321 (2009), pp. 2149-2155.

[10] R. Zhang, et al., Network model of survival signaling in large granular lymphocyte leukemia, PNAS, 105 (2008), pp. 16308-16313.

School of Mathematical Sciences, Guangxi Teachers Education University, Nanning 530023, P. R. China

E-mail address: gus02@163.com

Department of Electrical Engineering and Computer Sciences, University of Wisconsin, Milwaukee, WI 53201, USA

E-mail address: gxu4uwm@uwm.edu

Department of Mathematical Sciences, University of Wisconsin, Milwaukee, WI 53201, USA

E-mail address: ymzou@uwm.edu