Available online at www.sciencedirect.com

ScienceDirect

IFAC PapersOnline CONFERENCE PAPER ARCHIVE

IFAC PapersOnLine 58-17 (2024) 374–379

Linear Dynamical Systems over Finite Rings ⋆

Yannic Rohde * **Eva Zerz** **

* *Lehrstuhl für Algebra und Zahlentheorie, RWTH Aachen University, 52062 Aachen, Germany (e-mail: yannic.rohde1@rwth-aachen.de).*
** *Lehrstuhl für Algebra und Zahlentheorie, RWTH Aachen University, 52062 Aachen, Germany (e-mail: eva.zerz@math.rwth-aachen.de).*

Abstract: We present the theory of linear systems over various kinds of finite commutative rings. Since these systems are finite, the trajectories have to run into repeating cycles eventually. This periodic behavior is the main interest of this topic. Using an approach similar to Fitting's lemma, a bijective-nilpotent decomposition of the system can be achieved, which in some cases even gives a decomposition of the system matrix. In particular, this allows us, to apply results about invertible system matrices, where all trajectories are purely periodic, to the more general setting. Finally, the algorithmic potential of the theory is discussed.

Keywords: Algebraic Systems Theory, Linear Systems, Finite Rings, Cycle Length, Periodicity.
AMS subject classifications: 93B11, 93B25, 93B40

1. INTRODUCTION

Let M be a finite module over some finite commutative ring. A finite linear dynamical system is a pair (M, φ), where φ is an M-endomorphism. The system describes a behavior over discrete time, where the possible states of the system are encoded in M and any initial state $x \in M$ transitions after time $t \in \mathbb{N}$ to $\varphi^t(x)$. Since M is finite and the behavior for any initial point $x \in M$ is deterministically described by φ, the orbit of x has to eventually run into a loop. This long term behavior is the central point of studies of these systems. As the size of the module M can become large in applications, the naive approach to go through the whole orbit quickly becomes too expensive. Therefore, structural results and efficient algorithmic approaches are crucial.

Finite linear dynamical systems find application in many areas in computer science and electrical engineering and more recently have been used in computational biology, see Toledo (2005), Bollman et al. (2007), and Laubenbacher and Stigler (2004). While the structure of systems over finite fields is well understood, the present paper focuses on the generalization to finite rings, as suggested for example by Bollman et al. (2007) and Colón-Reyes et al. (2006). It is also known that linear systems can describe convolutional codes, see Rosenthal (2001). And recently there has been growing interest in extending this theory from finite fields to rings as well, as stated for example in Napp et al. (2022). The most prominent example is the ring $\mathbb{Z}/m\mathbb{Z}$, where m is not necessarily a prime. Many central methods for linear maps in vector spaces, like matrix normal forms that require unique factorization of polynomials, can not be applied directly over rings. Typical techniques involve reducing the systems to the case of a finite field of prime order and using the existing theory for vector spaces, as seen in Deng (2015), Wei et al. (2016), and Lindenberg (2018). In this paper we will refine these methods and generalize the theory by using structural facts for commutative rings. An interesting byproduct will be an algorithm to compute the multiplicative order of invertible matrices in $(\mathbb{Z}/m\mathbb{Z})^{n\times n}$.

The paper is organized as follows. Section 2 will summarize some basic theory of rings and finite linear systems that will be used. Section 3 will present the central point of this paper, which is the bijective-nilpotent decomposition and especially, how that leads to a decomposition of the system matrix. In Section 4 and Section 5 we will show what methods there are to analyze the nilpotent and bijective part of the decomposition respectively. At the end of each of these sections we will consider the special case of quotient rings of integers, which allow for more computational focused approaches.

2. PRELIMINARIES

2.1 Ring Theory

As this paper works with finite commutative rings, we want to briefly recall some ring theory results that are used here. We will only consider commutative rings and denote them by R. We deal only with finitely generated (and thus finite) R-modules M.

A finitely generated module M is called *free* if it is isomorphic to R^n for some $n \in \mathbb{N}$. M is called *projective*, if it is a direct summand of a free module, i.e. if there is some $n \in \mathbb{N}$ and some R-module N, such that

$$R^n \cong M \oplus N.$$

⋆ The authors acknowledge funding by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) - Project number 286237555 through the Transregional Collaborative Research Centre "Symbolic Tools in Mathematics and their Application" (SFB/TRR 195).

10.1016/j.ifacol.2024.10.198

We will only consider commutative rings in this paper. Therefore, we can always assume the *invariant basis number* property, i.e. $R^n \cong R^m$ always implies $m = n$ (see for example Lam (2012)).

A ring R is called *Artinian* if satisfies the descending chain condition, that is, for any descending chain of ideals

$$I_1 \supset I_2 \supset \dots$$

there is some $k > 0$ such that $I_r = I_k$ for all $r \geq k$.

A ring is called *local* if it has a unique maximal ideal.

Example 1. The most important example throughout this paper will be the quotient rings of integers

$$R = \mathbb{Z}/m\mathbb{Z}$$

for some $m \in \mathbb{Z}$. As a finite ring it is especially Artinian but not necessarily local. The local rings of this kind are the rings $R = \mathbb{Z}/p^r\mathbb{Z}$ for some prime power p^r. The unique maximal ideal here is the ideal generated by $p \in \mathbb{Z}/p^r\mathbb{Z}$, $I = \langle p \rangle$.

Another fundamental result that will be used is the following variant of the structure theorem for finite abelian groups (see for example Lang (2002)):

Theorem 2. Any finite abelian group G is isomorphic to a direct sum of the form

$$\bigoplus_{i=1}^{\omega} \mathbb{Z}/p_i^{r_i}\mathbb{Z},$$

where $\omega \in \mathbb{N}$ and the p_i are (not necessarily distinct) primes.

2.2 Finite Linear Dynamical Systems

The central objects of the present paper will be finite linear dynamical systems. A *finite linear dynamical systems* is a pair (M, φ), where M is a finite module over some finite ring R and

$$\varphi \colon M \to M$$

is a module endomorphism. Here, φ represents the system rule and in the case of a free module $M = R^n$, φ can also be represented by a matrix $A \in R^{n\times n}$, the so called *system matrix*. The central objective for finite dynamical systems is the study of the orbits of its elements. By orbit we mean the sequences

$$x, \varphi(x), \varphi^2(x), \dots$$

for the different elements $x \in M$. In order to visualize the structure of a finite dynamical system we associate a directed graph to the system defined by $\mathcal{G} := (M, E)$, where M is the set of nodes and the edges are defined by

$$E := \{x \to f(x) \mid x \in M\}.$$

In this way, the orbits of the system are the possible paths in the associated graph. Since M is finite, these graphs consist only of cycles and trees, as explained below.

Product of systems An important aspect of the present paper will be the decomposition of systems. To specify what we mean by that, we define the *product* of systems as follows. Let (M, φ) and (N, ψ) be two finite linear dynamical systems. Then the product of the systems is the system

$$(M, \varphi) \times (N, \psi) := (M \times N, \varphi \times \psi),$$

where

$$(\varphi \times \psi)(m, n) = (\varphi(m), \psi(n)).$$

The graph of such a product of systems is just the product of graphs

$$\mathcal{G}_\varphi \times \mathcal{G}_\psi = (M \times N, E),$$

with

$$E = \{(m, n) \to (\varphi(m), \psi(n)) \mid (m, n) \in M \times N\}.$$

To decompose a system (M, φ) into a product of smaller systems, we need a decomposition of the module M into a direct sum $M = M_1 \oplus M_2$, with the additional condition that φ is invariant on the submodules M_1 and M_2. Then we can write

$$(M, \varphi) = (M_1, \varphi|_{M_1}) \times (M_2, \varphi|_{M_2}).$$

3. DECOMPOSITION IN BIJECTIVE AND NILPOTENT PART

Let R be a finite commutative ring, M a finite R-module, and φ an endomorphism on M. These define the finite linear system (M, φ), with the system rule

$$x_{i+1} := \varphi(x_i), \text{ for all } x_0 \in M, i \in \mathbb{N}.$$

3.1 Finite Fields

The classical case, where R is some finite field $\mathbb{F}$, has been studied in detail in Toledo (2005). Here, M is the $\mathbb{F}$-vector space $\mathbb{F}^n$ for some $n \in \mathbb{N}$ and the endomorphism φ is a matrix $A \in \mathbb{F}^{n\times n}$. The main idea is to use the unique factorization of the minimal polynomial of A and its corresponding rational canonical form of the matrix. In terms of the dynamical system $(\mathbb{F}^n, A)$, one of the main results from this idea, is a decomposition of the state space $\mathbb{F}^n$ into a direct sum of two A-invariant subspaces P, N of $\mathbb{F}^n$, where A, restricted to P, is bijective and A, restricted to N, is nilpotent. This gives a good insight to the structure of the dynamical system, since we can describe it as the product of the dynamical systems consisting of the bijective and the nilpotent part respectively. In particular, we can say a lot about the associated graphs of these two systems. The bijective part depicts an invertible map on a finite set and as such, the graph must consist of a union of cycles. The nilpotent part on the other hand has a graph where all paths lead to the $0 \in M$. Thus, the graph looks like a tree. And although it is not technically a tree, since it has a self-loop at 0, we will still call it a tree for the sake of this paper. The following small example illustrates that decomposition.

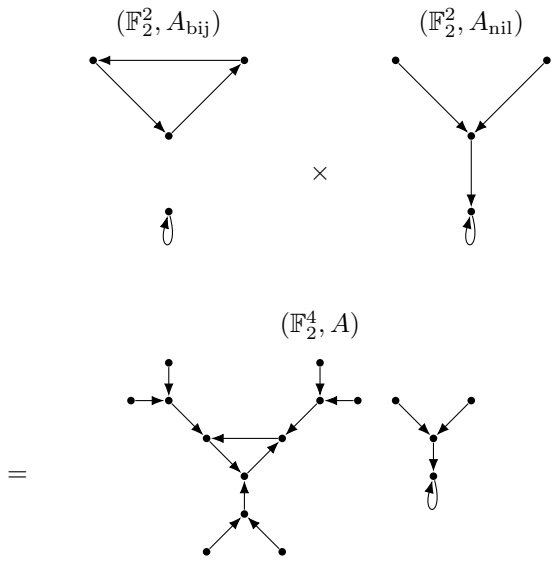
Example 3. We consider the system $(\mathbb{F}_2^4, A)$ with the system matrix

$$A := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \in \mathbb{F}_2^{4\times 4}$$

over the field with two elements $\mathbb{F}_2$. This matrix is already in a block diagonal form and we can see that

$$A_{\text{bij}} := \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \qquad A_{\text{nil}} := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

are bijective, respectively nilpotent. The corresponding partition $\mathbb{F}_2^4 = \mathbb{F}_2^2 \oplus \mathbb{F}_2^2$ results in the following decomposition of the system's graph into a tree and a union of cycles:



We can see that the resulting product-graph consists of the same cycles as the bijective part, with the tree from the nilpotent part glued to every cycle point.

3.2 Fitting's-Lemma-Approach

When R is not a field, this argument does not work. Due to the lack of unique factorization of polynomials, we can not assume that there is a well behaved normal form for matrix similarity such as the rational canonical form.

Nevertheless, there is an approach for decomposing a finite linear system over arbitrary commutative rings, that instead uses the idea of Fitting's Lemma. The idea was mentioned in Bollman et al. (2007).

Since the two chains

$$\operatorname{im}(\varphi) \supseteq \operatorname{im}(\varphi^2) \supseteq \operatorname{im}(\varphi^3) \supseteq \ldots, \text{ and}$$
$$\ker(\varphi) \subseteq \ker(\varphi^2) \subseteq \ker(\varphi^3) \subseteq \ldots$$

consist of submodules of the finite module M, there must be an exponent $h \in \mathbb{N}$ such that both chains become stationary. Hence, we get the submodules

$$P := \operatorname{im}(\varphi^h) \text{ and } N := \ker(\varphi^h).$$

The following lemma shows, why this leads to a decomposition of the system.

Lemma 4. For the finite linear system (M, φ), let $h \in \mathbb{N}$ be a number, such that we have $\operatorname{im}(\varphi^h) = \operatorname{im}(\varphi^{h+1})$ and $\ker(\varphi^h) = \ker(\varphi^{h+1})$ and define P and N as above. Then the following properties hold:

(1) $M = P \oplus N$
(2) P and N are φ-invariant
(3) φ is bijective on P
(4) φ is nilpotent on N

Proof.

(1) To show that $M = P + N$ we can take any $m \in M$ and observe that $\varphi^h(m) \in \operatorname{im}(\varphi^h) = \operatorname{im}(\varphi^{2h})$. Hence, there must exist some $n \in M$ with $\varphi^h(m) = \varphi^{2h}(n)$. We can then write
$$m = \varphi^h(n) + (m - \varphi^h(n)) \in P + N,$$
since
$$\varphi^h(m - \varphi^h(n)) = \varphi^h(m) - \varphi^{2h}(n) = 0.$$
To show that $P \cap N = \{0\}$, we consider any $m \in P \cap N$. From $m \in P$, we know that there is an $n \in M$ with $\varphi^h(n) = m$. And since $m \in N$, we conclude that $0 = \varphi^h(m) = \varphi^{2h}(n)$, so we have $n \in \ker(\varphi^{2h}) = \ker(\varphi^h)$. And this already implies that $0 = \varphi^h(n) = m$.
(2) This follows from the definition of P and N.
(3) This follows immediately from (1), since $\varphi(p) = 0$ would imply $p \in N$ and hence $p = 0$, for any $p \in P$.
(4) This follows directly from the definition of N. □

This means we get a similar bijective-nilpotent-decomposition of the system (M, φ) to the one for fields as described above. And analogously, we know that $(P, \varphi|_P)$ is a union of cycles and $(N, \varphi|_N)$ is a tree. We therefore call P the set of cycle points and N the set of tree points.

As a remark we mention that the smallest exponents at which the two chains become stationary are actually always the same. This makes it easier to talk about the minimal exponent.

Proposition 5. For the finite linear system (M, φ) define $h_1 \in \mathbb{N}$ as the smallest number, such that
$$\operatorname{im}(\varphi^{h_1}) = \operatorname{im}(\varphi^{h_1+1}) = P.$$
Analogously, define $h_2 \in \mathbb{N}$ as the smallest number, such that
$$\ker(\varphi^{h_2}) = \ker(\varphi^{h_2+1}) = N.$$
Then we have
$$h_1 = h_2.$$

Proof. To show that $h_1 \leq h_2$ we show that $\operatorname{im}(\varphi^{h_2}) \subseteq P$. So let x be any element of $\operatorname{im}(\varphi^{h_2})$. Then there exists some $y \in (\mathbb{Z}/q\mathbb{Z})^n$ with $\varphi^{h_2}(y) = x$. Using Lemma 4, we can write $y = y_P + y_N$ with $y_P \in P$ and $y_N \in N$. Then we have
$$x = \varphi^{h_2}(y_P) + \varphi^{h_2}(y_N) = \varphi^{h_2}(y_P) \in P.$$

To show that $h_2 \leq h_1$ we show that $N \subseteq \ker(\varphi^{h_1})$. For any $x \in N$ we know that $\varphi^{h_1}(x) \in P \cap N = 0$. Thus we get $x \in \ker(\varphi^{h_1})$. □

This shows that the we only need do talk about one smallest exponent h, necessary for this decomposition. We say that the system stabilizes after h steps and call h the *height* of the system. Furthermore, the height of the system is nothing else as the nilpotency index of its nilpotent part.

Example 6. Consider the system $((\mathbb{Z}/6\mathbb{Z})^3, A)$ with the system matrix
$$A := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 4 \\ 2 & 2 & 2 \end{pmatrix} \in (\mathbb{Z}/6\mathbb{Z})^{3\times 3}$$
over the ring of integers modulo 6. Then we can compute
$$\ker(A^2) = \ker(A^3) = \langle \begin{pmatrix} 3 \\ 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 0 \end{pmatrix} \rangle$$
and
$$\operatorname{im}(A^2) = \operatorname{im}(A^3) = \langle \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 3 \\ 0 \end{pmatrix} \rangle.$$
Therefore, we know that the system height is $h = 2$ and we get the decomposition $(\mathbb{Z}/6\mathbb{Z})^3 = P \oplus N$, where

$P = \mathrm{im}(A^2)$ and $N = \ker(A^2)$. Furthermore, we know that every point in P lies on a cycle and every point in N lies on a trajectory towards 0.

Matrix decomposition When it comes to computations and applications we typically want the module to be a free module $M = R^n$ so that we can express the endomorphism φ as a matrix A, which we call the system matrix. We saw this in Example 3 and Example 6 with our main example $M = (\mathbb{Z}/m\mathbb{Z})^n$.

However, in contrary to vector spaces, a decomposition of a free module into invariant submodules does not always lead to a similarity transformation of the matrix into a block-diagonal form. This is also displayed in Example 6, where P and N are not free.

Nevertheless, since we assume R to be finite, it is always Artinian. Hence, we can use the following standard result from commutative algebra. A proof can be found for example in Atiyah and Macdonald (1969) (Thm. 8.7).

Theorem 7. (structure theorem for Artinian rings). An Artinian ring R is uniquely (up to isomorphism) a finite direct product of Artinian local rings.

Hence, we get a decomposition of R into finite local rings. This gives us what we need because of another standard result, which is a consequence of Nakayama's lemma, as seen for example in Matsumura (1989) (Thm 2.5).

Theorem 8. Let R be a local ring. Then any finitely generated, projective R-module is free.

Together with the invariant basis number property of commutative rings, we can now state the following.

Theorem 9. Let R be a finite local ring, $M = R^n$ a free module, $A \in R^{n\times n}$ the system matrix and h, P, N defined as in Lemma 4. Then we have

$$P \cong R^{n_1} \text{ and } N \cong R^{n_2} \text{ with } n_1 + n_2 = n.$$

Especially, we get that A is similar over $R^{n\times n}$ to a block diagonal matrix

$$\begin{pmatrix} A_P & 0 \\ 0 & A_N \end{pmatrix},$$

with $A_P \in R^{n_1\times n_1}$ invertible and $A_N \in R^{n_2\times n_2}$ nilpotent. We can therefore decompose the system into

$$(R^n, A) = (P, A_P) \times (N, A_N).$$

So the method to decompose a system (R^n, A) over a general finite commutative ring R, is to first decompose R into local rings and then apply the bijective-nilpotent decomposition. We can then analyze the much easier components separately. We will illustrate this approach in the scenario of Example 6. In the case of $R = \mathbb{Z}/m\mathbb{Z}$, the decomposition into local rings corresponds to the Chinese remainder theorem along the factorization of m into prime powers p^r, where $\mathbb{Z}/p^r\mathbb{Z}$ is a local ring.

Example 10. We consider the system $((\mathbb{Z}/6\mathbb{Z})^3, A)$ from Example 6 again. But now, we decompose the ring into

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

which corresponds to the decomposition of the system

$$((\mathbb{Z}/6\mathbb{Z})^3, A) \cong ((\mathbb{Z}/3\mathbb{Z})^3, A_3) \times ((\mathbb{Z}/2\mathbb{Z})^3, A_2),$$

where $A_3 \equiv A \pmod 3$ and $A_2 \equiv A \pmod 2$. Hence we can do the same computations as in Example 6, but over the local rings (which are even fields in this case) $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$ now.

Let us look at $\mathbb{Z}/2\mathbb{Z}$ for this example. We get

$$\ker(A_2^3) = \ker(A_2^2) = \ker(\begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}) = \langle \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \rangle$$

and

$$\mathrm{im}(A_2^2) = \mathrm{im}(A_2^3) = \langle \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \rangle.$$

The block-diagonal form of A_2, corresponding to these free generators is

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \in (\mathbb{Z}/2\mathbb{Z})^{3\times 3}.$$

4. NILPOTENT PART

For this section we assume R to be a finite local ring, $A \in R^{n\times n}$ to be a nilpotent matrix and consider the system (R^n, A). This is one of two possible kinds of systems we get, after the reductions of the previous section. As seen in Example 3, the graph of the system is a tree. In this section we want describe shortly how this tree is structured.

4.1 Local rings

Firstly, some of the arguments from Toledo (2005) that were used for the case where R is a field, can also be applied here. An element $x \in R^n$ is called a *source point* of the tree, if it has no preimage. Since this is equivalent to $x \notin \mathrm{im}(A)$, we can conclude that the number of source point is

$$|\{x \in R^n \mid x \text{ is a source point }\}| = |R|^n - |\mathrm{im}(A)|.$$

Furthermore, for all points that are no source points, i.e. that are image points of A, we know that there are exactly $|\ker(A)|$ preimages. The only exception is the point 0. Since it has a self-loop, it has only $|\ker(A)| - 1$ preimages apart from itself. We define the *height* of an element $x \in R^n$ as

$$h_A(x) := \min\{k \in \mathbb{N} \mid A^k x = 0\}.$$

Since the points of height 1 are exactly the elements of $\ker(A) \setminus \{0\}$, we have $|\ker(A)| - 1$ points of height 1. Each one of these points can have either 0 or $|\ker(A)|$ many preimages, which means that the number of points of height 2 is less than $|\ker(A)||\ker(A) - 1|$. Inductively we get the following statement.

$$|\{x \in R^n \mid x \text{ has height } i\}| \leq |\ker(A)|^{i-1}|\ker(A) - 1|$$

Another important property of the system is its nilpotency index, i.e. the highest $k \in \mathbb{N}$ such that there is a point of height k. As we saw in Proposition 5, this is the same as the system's height, which is needed for computing P and N as well. Therefore, a sharp bound on the system height is of high value. Lindenberg (2018) proposed two of these bounds for the case that $R = \mathbb{Z}/p^r\mathbb{Z}$ for some prime p. More precisely, there is one bound that does not depend on the system matrix and one that is specific for the system matrix and is therefore the tighter one. However, the function independent bound is easier to compute and can be easily generalized to more general rings as follows.

Theorem 11. Let R be a finite ring, (R^n, A) be a linear finite system with $A \in R^{n\times n}$ nilpotent and h be the system height. If the prime factorization of $|R|$ is given by $p_1^{r_1} p_2^{r_2} \cdots p_\omega^{r_\omega}$, where all p_i are different, then the height is bounded by

$$h \leq n r_{\max},$$

where $r_{\max}$ is the largest of the prime factor exponents.

Proof. We can use the structure theorem of finitely generated abelian groups (stated in Theorem 2) to write $R^n = \bigoplus_{i=1}^{\omega} G_i$, where $|G_i| = p_i^{nr_i}$, which is the highest power of p_i in the order of R^n. Then it follows that each G_i is invariant under A.

This means that the height of A is the maximum of the heights h_i of A on the subgroups G_i. And for any G_i we get the chain of proper subgroups

$$G_i \supset AG_i \supset A^2 G_i \supset \cdots \supset A^{h_i} G_i = 0.$$

Since these must be proper subgroups, the length of the chain can be at most as long as the number of divisors of $|G_i| = p_i^{nr_i}$, which is nr_i. Therefore, we have

$$h = \max\{h_1, \ldots, h_\omega\} \leq \max\{nr_1, \ldots, nr_\omega\},$$

which concludes the proof. □

4.2 Quotient rings of integers

The tighter and function dependent bound of the system height found in Lindenberg (2018) is more specific to the case where $R = \mathbb{Z}/m\mathbb{Z}$, because it relies on reducing the system to systems over finite fields of prime order. Since we assume our ring to be local according to Section 3.2, we have $R = \mathbb{Z}/q\mathbb{Z}$ for a prime power $q = p^r$ in this case. The main argument is that for the trajectory of some $x \in (\mathbb{Z}/q\mathbb{Z})^n$ to reach 0 in $((\mathbb{Z}/q\mathbb{Z})^n, A)$, it has to reach 0 r times in the reduced systems $((\mathbb{Z}/p\mathbb{Z})^n, A \pmod p)$. Let us restate the theorem here.

Theorem 12. Let $((\mathbb{Z}/q\mathbb{Z})^n, A)$ be a system with height h. Then the height is bounded by

$$h \leq r h_1,$$

where h_1 is the height of the reduced system

$$((\mathbb{Z}/p\mathbb{Z})^n, A \pmod p).$$

5. BIJECTIVE PART

In this section we focus on the the other kind of systems we get after the decomposition of Section 3.2. Therefore, let R be a finite local ring, $A \in R^{n\times n}$ an invertible matrix and (R^n, A) the corresponding linear system. Since R^n is a finite set, we know that repeated application of A to any point $x \in R^n$ has to eventually reach a point twice. That is, there exist $k_1 > k_2 \in \mathbb{N}$, such that $A^{k_1}x = A^{k_2}x$. And since A is invertible, we can deduce that $A^{k_1-k_2}x = x$. Therefore, each point $x \in R^n$ lies on a cycle, the length of which we call the *period* of x, denoted as

$$\pi_A(x) := \min\{k \in \mathbb{N} \mid A^k x = x\}.$$

5.1 Local rings

The first thing to note is that A is an element of the finite group $\mathrm{GL}_n(R)$. As such, it has a a finite multiplicative order, which we call

$$\mathrm{ord}(A) := \min\{k \in \mathbb{N} \mid A^k = I_n\}.$$

We have the following fundamental connection to the cycle lengths of the system.

Lemma 13. Let R be a finite local ring and $A \in \mathrm{GL}_n(R)$. Then we have

$$\mathrm{ord}(A) = \mathrm{lcm}\{\pi_A(x) \mid x \in R^n\}.$$

Proof. Since $x = A^{\mathrm{ord}(A)}x$, it follows by the standard euclidean division argument, that $\pi_A(x) \mid \mathrm{ord}(A)$.
On the other hand, we have

$$A^{\mathrm{lcm}\{\pi_A(e_1),\ldots,\pi_A(e_n)\}} = I_n$$

for any basis $e_1, \ldots, e_n \in R^n$. □

Many of the deeper results about the cycle structure of these bijective systems are found for quotient rings of integers, i.e. for $R = \mathbb{Z}/m\mathbb{Z}$, and will be discussed in the next section. However, in Wei et al. (2016) there are methods developed for general commutative rings. The main idea is to use the structure theorem of finitely generated abelian groups in a similar way to the proof of Theorem 11. With this approach it is possible to simplify the problem to systems over finite fields of prime order. This results in an algorithmic approach to determine periods. In their work the authors mention that their results are specific for module automorphisms, i.e. for bijective systems. With the decomposition of the present paper, these results can now also be applied for general module homomorphisms.

5.2 Quotient rings of integers

In this section we focus on the case $R = \mathbb{Z}/m\mathbb{Z}$. This case is particularly interesting from a computational point of view and naturally has many applications. After the discussions in Section 3.2 we can break the systems down to local rings, which in this case are the rings of the form $R = \mathbb{Z}/p^r\mathbb{Z}$ for a prime p, via the Chinese remainder theorem. So for this section we fix some prime power $q := p^r$ and consider the system $((\mathbb{Z}/q\mathbb{Z})^n, A)$, for some invertible matrix $A \in (\mathbb{Z}/q\mathbb{Z})^{n\times n}$. The central method for most results in this setting is to reduce the system to systems modulo lower powers of p. By doing so inductively, the bottom case $\mathbb{Z}/p\mathbb{Z}$ can be reached, where we have more theory due to $\mathbb{Z}/p\mathbb{Z}$ being a field. Similar to the bound on the system's height, the order of the matrix $\mathrm{ord}(A)$ is a bound for the periods $\pi_A(x)$ of the points $x \in ((\mathbb{Z}/q\mathbb{Z})^n, A)$. More precisely, from Lemma 13 we know that periods are not only smaller than $\mathrm{ord}(A)$ but must divide it. Therefore, the following results on $\mathrm{ord}(A)$, found in Zerz and Giese (2020), are particularly useful.

Since the power of p is varying here, we introduce the following alternative notation for the order of an integer matrix modulo different numbers $m > 0$. Let $A \in \mathbb{Z}^{n\times n}$ be an integer matrix and assume $A \pmod m$ is invertible in $(\mathbb{Z}/m\mathbb{Z})^{n\times n}$. Then let

$$\mathrm{ord}_m(A) := \min\{k > 0 \mid A^k \equiv I_n \pmod m\},$$

which is the multiplicative order of the matrix $A \pmod m$ in $(\mathbb{Z}/m\mathbb{Z})^{n\times n}$. In the case of a local ring, i.e. m being a prime power, we have that $A \pmod{p^r}$ is invertible in $(\mathbb{Z}/p^r\mathbb{Z})^{n\times n}$ if and only if $p \nmid \det(A)$, which means that $A \pmod{p^t}$ is invertible in $(\mathbb{Z}/p^t\mathbb{Z})^{n\times n}$ for any $t \geq 1$. We then have the following connection between the orders of

A modulo different powers of p (Zerz and Giese (2020), Thm. 3 - Thm. 5).

Theorem 14. Let $A \in \mathbb{Z}^{n\times n}$ with $p \nmid \det(A)$. Then we have

$$\operatorname{ord}_{p^i}(A) \mid \operatorname{ord}_{p^j}(A) \text{ for all } 1 \leq i \leq j$$

and

$$\operatorname{ord}_{p^r}(A) = \operatorname{ord}_p(A)p^i \text{ for some } 0 \leq i \leq r-1.$$

Additionally, if there is a $t \geq 1$ with $\operatorname{ord}_{p^t}(A) \neq \operatorname{ord}_{p^{t+1}}(A)$ and we have $p \neq 2$ or $t \geq 2$, then we get the precise formula

$$\operatorname{ord}_{p^r}(A) = \operatorname{ord}_{p^t}(A)p^{r-t}$$

for all $r \geq t$.

Therefore, the problem is reduced again to the computation of $\operatorname{ord}_p(A)$, i.e. a computation over a field. For this there exist efficient algorithms like for example in Celler and Leedham-Green (1997). We propose the following algorithm to compute $\operatorname{ord}_{p^r}(A)$.

Algorithm 1.
Input: prime p, $r > 0$, $A \in \mathbb{Z}^{n\times n}$ invertible over $\mathbb{Z}/p\mathbb{Z}$
Output: Order $\operatorname{ord}_{p^r}(A)$

(1) compute $k \leftarrow \operatorname{ord}_p(A)$, e.g. by algorithm of Celler and Leedham-Green (1997)
(2) compute $B \leftarrow A^k$
(3) if $p = 2$ and $B \not\equiv I_n \pmod 4$ then
  (a) set $k \leftarrow kp$
  (b) set $B \leftarrow B^p$
(4) via binary search find the largest $t \leq r$ with
$$B \equiv I_n \pmod{p^t}$$
(5) return $\operatorname{ord}_{p^r}(A) = kp^{r-t}$

This algorithm scales logarithmically with the exponent r due to the binary search. Hence, it can handle high prime powers well. However, the size of the matrix has a big influence on the runtime, caused by the explicit computation of $A^{\operatorname{ord}_p(A)}$, where $\operatorname{ord}_p(A)$ also gets potentially larger for larger n.

The computation of a period of some point x in the system $((\mathbb{Z}/q\mathbb{Z})^n, A)$ can now be done by going through the divisors of $\operatorname{ord}_{p^r}(A)$ systematically. One could also choose a binary search approach for the exponent of p in the factorization of $\pi_A(x)$.

As for the general cycle structure of such a system, there is a method in Deng (2015) to determine the size and number of all cycles in $((\mathbb{Z}/q\mathbb{Z})^n, A)$. The method evolves around counting the elements of $\ker(A^k - I_n)$ via its Smith normal form, where k runs over all possible periods in

$$((\mathbb{Z}/p\mathbb{Z})^n, A \pmod p).$$

Another interesting result from this article is that for any two cycles of length l_1 and l_2, there must also be a cycle of length $\operatorname{lcm}(l_1, l_2)$ (Deng (2015), Lemma 5.6). In particular, this means that there is always a cycle of length $\operatorname{ord}(A)$.

6. CONCLUSION

In the present paper we developed a method to break down finite linear systems over rings into nilpotent and bijective systems. In both cases we gave an overview over various methods to analyze the system's structure. This resulted in efficient computational approaches especially for quotient rings of integers, which are the most prominent example.

We currently plan to further extend the results of this paper from systems described by the explicit system rule $x_{i+1} := Ax_i$, to systems described by an implicit rule $Ex_{i+1} := Ax_i$, where E is another matrix. If E is invertible, the system rule can be reformulated to the explicit case. Otherwise, we get a much larger class of systems. Tools like the Kronecker canonical form are known to be useful for these systems over fields and it is a natural approach to try to generalize such methods to systems over finite rings.

REFERENCES

Atiyah, M. and Macdonald, I. (1969). *Introduction to Commutative Algebra*. Addison-Wesley Publishing Company.

Bollman, D., Colón-Reyes, O., and Orozco, E. (2007). Fixed points in discrete models for regulatory genetic networks. *EURASIP Journal on Bioinformatics and Systems Biology*, 2007, 1–8.

Celler, F. and Leedham-Green, C.R. (1997). Calculating the order of an invertible matrix. In *Groups and computation, II (New Brunswick, NJ, 1995)*, volume 28 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, 55–60. Amer. Math. Soc., Providence, RI.

Colón-Reyes, O., Jarrah, A., Laubenbacher, R., and Sturmfels, B. (2006). Monomial dynamical systems over finite fields. *Complex Systems*, 16, 333–342.

Deng, G. (2015). Cycles of linear dynamical systems over finite local rings. *Journal of Algebra*, 433, 243 – 261.

Lam, T.Y. (2012). *Lectures on modules and rings*, volume 189. Springer Science & Business Media.

Lang, S. (2002). *Algebra*. Springer, New York, NY.

Laubenbacher, R. and Stigler, B. (2004). A computational algebra approach to the reverse engineering of gene regulatory networks. *Journal of Theoretical Biology*, 229(4), 523–537.

Lindenberg, B. (2018). Stabilization bounds for linear finite dynamical systems. *Journal of Algebra*, 511, 516–534.

Matsumura, H. (1989). *Commutative Ring Theory*. Cambridge University Press.

Napp, D., Pinto, R., and Rocha, C. (2022). State representations of convolutional codes over a finite ring. *Linear Algebra and its Applications*, 640, 48–66.

Rosenthal, J. (2001). Connections between linear systems and convolutional codes. In B. Marcus and J. Rosenthal (eds.), *Codes, Systems, and Graphical Models*, 39–66. Springer New York, New York, NY.

Toledo, R.A.H. (2005). Linear finite dynamical systems. *Communications in Algebra*, 33(9), 2977–2989.

Wei, Y., Xu, G., and Zou, Y.M. (2016). Dynamics of linear systems over finite commutative rings. *Applicable Algebra in Engineering, Communication and Computing*, 27(6), 469–479.

Zerz, E. and Giese, H. (2020). Computing the cycle structure of finite linear systems. In *Proc. IFAC World Congress*. Berlin.