



Bachelor Degree Project

# On cycle lengths in finite linear dynamical systems



Author: Joost Husen  
Supervisor: Marcus Nilsson  
Semester: Spring 2024  
Subject: Mathematics

## **Abstract**

This thesis seeks to make progress towards generalising cycle structures in finite linear dynamical systems. The main results in this thesis find the cycle structures of nilpotent, invertible and diagonal matrices. It also presents and analyses statistical data of the maximum possible length of a cycle.

## **Acknowledgements**

I would like to thank my supervisor Marcus Nilsson for the suggestion of the topic and his help and ideas provided throughout the process of writing this thesis.

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Iterative methods of finding the cycle structure</b>	<b>2</b>
2.1	Floyd's tortoise hare algorithm . . . . .	2
2.2	Brent's algorithm . . . . .	4
2.3	Floyd's algorithm vs Brent's algorithm . . . . .	7
<b>3</b>	<b>Algebraic methods of finding the cycle structure</b>	<b>7</b>
3.1	Number of elements with period $r$ . . . . .	7
3.1.1	Möbius formula . . . . .	7
3.1.2	The one by one case . . . . .	8
3.1.3	Smith Normal Form . . . . .	8
3.2	Other methods . . . . .	11
3.3	Matrix order . . . . .	11
<b>4</b>	<b>Special case matrices</b>	<b>12</b>
4.1	Nilpotent matrices . . . . .	12
4.2	Invertible matrices . . . . .	13
4.3	Diagonal matrices . . . . .	14
4.3.1	cycle structure . . . . .	15
<b>5</b>	<b>Statistical analysis of matrices</b>	<b>18</b>
5.1	Maximal cycle length modulo $m$ . . . . .	19
5.2	Proportion of matrices with maximal cycle length . . . . .	20
<b>6</b>	<b>Discussion</b>	<b>20</b>

# 1 Introduction

In this thesis we look at cycle lengths in finite linear dynamical systems (flds). A flds can be seen as a tuple  $(f, S)$ , where  $S$  is a set and  $f: S \rightarrow S$  a function. Specifically we want to apply  $f$  to a single point over and over, this creates a set

$$\{x, f(x), f(f(x)), f(f(f(x))), \dots\} = \{x, f(x), f^2(x), f^3(x), \dots\}.$$

We will be looking at the system with  $f(x) = Ax \pmod m$ , where  $m \in \mathbb{Z}$ ,  $A \in \mathbb{Z}_m^{n \times n}$  an  $n \times n$  matrix with entries modulo  $m$ , and  $x \in S = \mathbb{Z}_m^n$  an  $n \times 1$  vector with entries modulo  $m$ . We will denote this system as  $(A, \mathbb{Z}_m^n)$ . We then end up with a set

$$\{x, Ax, A^2x, A^3x, \dots\},$$

all in modulo  $m$ . The name linear dynamical system comes from the fact that  $f(x) = Ax$  is linear function.

Because the set  $\mathbb{Z}_m^n$  is finite, which gives the name finite linear dynamical system, we will eventually have that  $x_0 \equiv A^{k_1}x_0 \equiv A^{k_2}x_0 \pmod m$ ,  $k_1 \neq k_2$  positive integers. We can say that  $A^kx_0 \equiv x_0 \pmod m$ ,  $k$  a positive integer. We say that  $x_0$  is periodic and has period or cycle length  $k$  if there's no  $0 < d < k$  for which  $A^d x_0 = x_0 \pmod m$ . In the case where  $k = 1$ , i.e.  $Ax \equiv x \pmod m$ , we say that  $x$  is a fixed point. In the case where there is no  $k$  such that  $A^k x \equiv x \pmod m$ , we say that  $x$  is non-cyclic or  $x$  is pre-periodic.

We introduce a new representation of the system through a graph. We write  $\mathfrak{G}(f, S) = (V, E)$ , where  $V$  is a set of vertices and  $E$  is a set of directed edges between the elements of  $V$ .

**Example 1.** Consider the system  $(A, \mathbb{Z}_5^2)$ , where  $A = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix}$ . So our set consists of  $\{x = [x_1 \ x_2]^T : 0 \leq x_i \leq 4, i = 1, 2\}$ . To get the edges that belong to our graph we iterate over all elements in our set and take  $f(x) = Ax$ . When we do that we can plot everything into the graph represented in Figure 1.1.

We will often use a graphical representation of a system as opposed to an algebraic representation for ease of understanding and readability.

In this thesis we are interested in all cycles generated by a matrix  $A$  over a set  $\mathbb{Z}_m^n$ . In section 2 and 3 we introduce several methods of finding the cycle structure of  $A$ . Floyd's and Brent's algorithm are both methods that iterate over all points, starting at an input  $x_0$  then computing the next point  $Ax_0$  and continuing till a cycle has been found.

After that we use algebraic methods, first using the fact that we can find the number of solutions to  $(a^r - 1)x \equiv 0 \pmod m$  which gives us the number of points  $x$  that are such that  $A^r x \equiv x \pmod m$ , secondly using the Smith normal form of the matrix  $A^r - I$ , where we take the product of  $\gcd(s_r, m)$ , where  $s_r$  is the  $r$ -th diagonal element of the Smith normal form, to find the number of points  $x$  such that  $A^r x \equiv x \pmod m$ . We denote the number of such points by  $\eta(r)$ . We then combine these methods with the Möbius inversion formula to find the number of points of period  $r$ .

In chapter 4 we look at special case matrices. First we find that for nilpotent matrices the system is easily predicted, a single fixed point in  $x = 0$  and all other points are non-cyclic. For invertible matrices we find that all points are periodic.

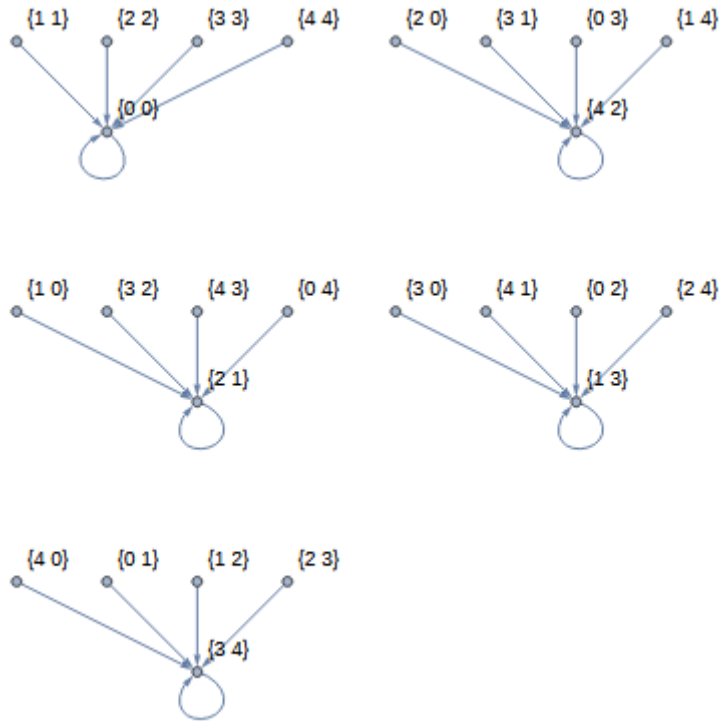


Figure 1.1: Graph of the system  $(A, \mathbb{Z}_5^2)$

And for diagonal matrices we find that we can take the least common multiple of the cycle lengths of the diagonal elements to find the length and quantity of cycles in the cycle structure of the full matrix.

In chapter 5 we finish off by stating a handful of conjectures that are left unproven with statistical analysis to back them up.

Dynamical systems can be found in several areas of applied mathematics such as electrical engineering, machine learning, or pseudorandomisation. An example of the use in electrical engineering can be found in [4], where a modulo 2 dynamical system gets used to correct noise. A linear congruential generator is of the form  $f(x) = Ax + c$ , where  $c \in \mathbb{Z}_m^n$ , usually the system is in  $n = 1$ , choosing  $c = 0$  makes it a system of the type researched in this thesis.

## 2 Iterative methods of finding the cycle structure

### 2.1 Floyd's tortoise hare algorithm

**Algorithm 1.** The first known reference to Floyd's algorithm was in Knuth (1969) [5], as an exercise in his book, he attributed the algorithm to Floyd, however, Floyd did not publish anything describing this algorithm.

The inputs for Floyd's algorithm are a function (a matrix multiplication in our case  $x \mapsto Ax, A \in \mathbb{Z}_m^{n \times n}$ ) and a starting point (a vector  $x_0 \in \mathbb{Z}_m^n$ ). It returns the length of the cycle ( $\lambda$ ) and the distance the starting point is from the closest point in the cycle ( $\mu$ ). Since we are only interested in the cycle lengths in this paper, we omit the explanation of finding  $\mu$ .

The algorithm is as follows.

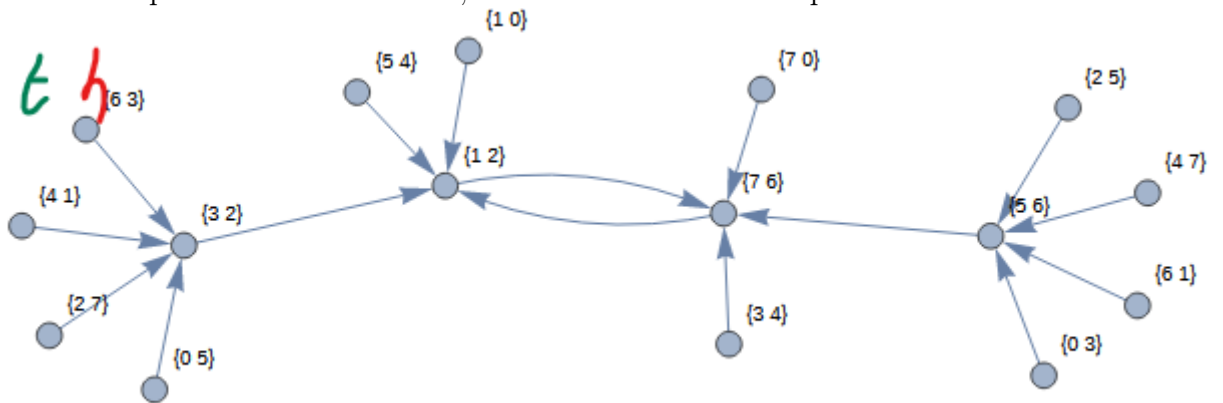
1. Finding the cycle

- First set two pointers, one the tortoise (t), the other the hare (h), at  $x_0$ .
- move the tortoise one step (i.e. compute  $Ax$ ), and move the hare two steps (i.e. compute  $A^2x$ ). Repeat till the tortoise and the hare are pointing towards the same point.

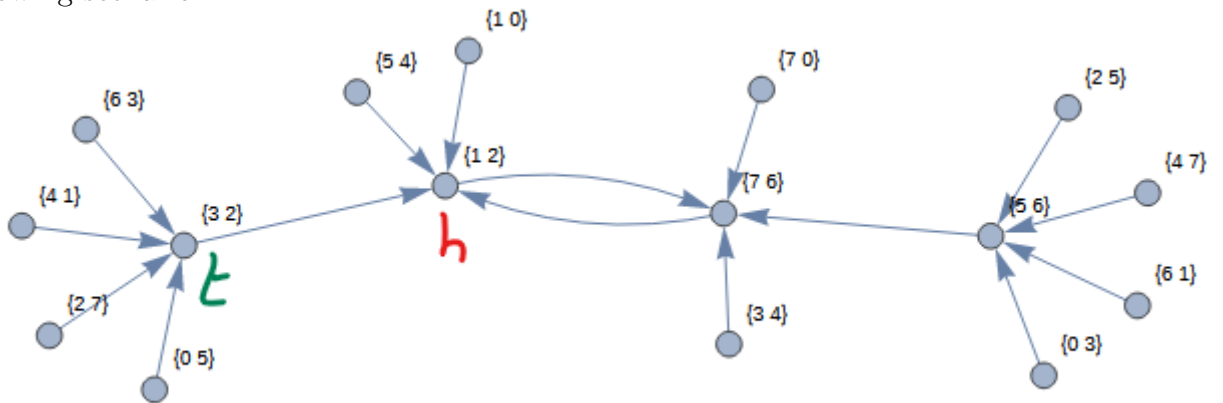
## 2. Finding $\lambda$

- Set  $\lambda(t) = 0$ , a counting process counting the number of steps the hare takes from now on..
- Continuously let the hare take one step at a time whilst the tortoise remains still till the hare and the tortoise point at the same point.
- The resulting  $\lambda(t)$  is the length of the cycle.

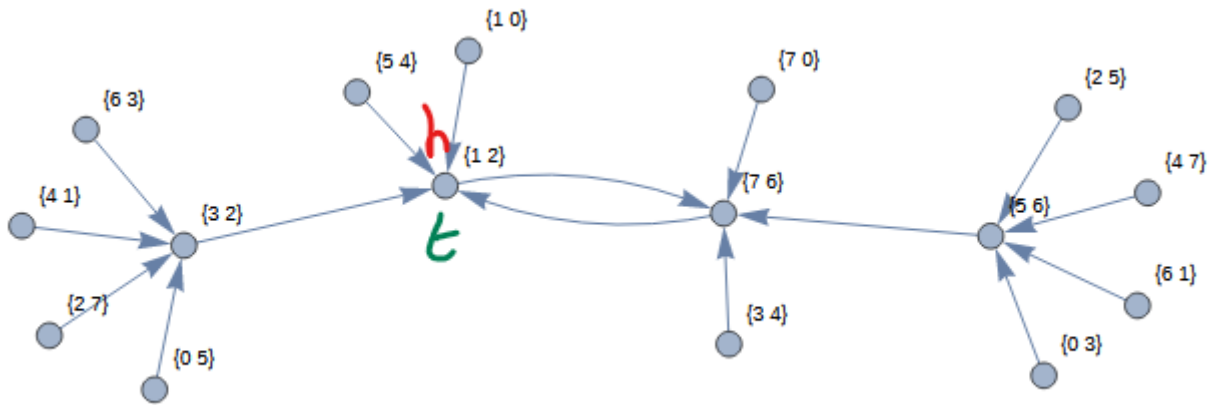
**Example 2.** Consider the matrix  $A = \begin{bmatrix} 1 & 7 \\ 2 & 2 \end{bmatrix} \pmod 8$ , and  $x_0 = \begin{bmatrix} 6 \\ 3 \end{bmatrix}$ . We plot the relevant part of the graph to get an idea of what we're supposed to get. The green t illustrates the position of the tortoise, the red h illustrates the position of the hare.



As per the algorithm we move the tortoise 1 spot and the hare 2 giving the following scenario.

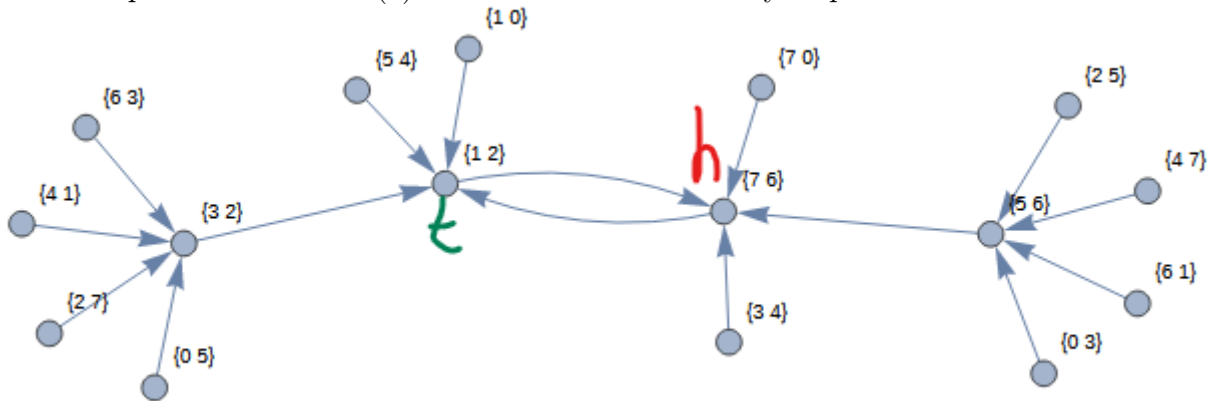


Again.

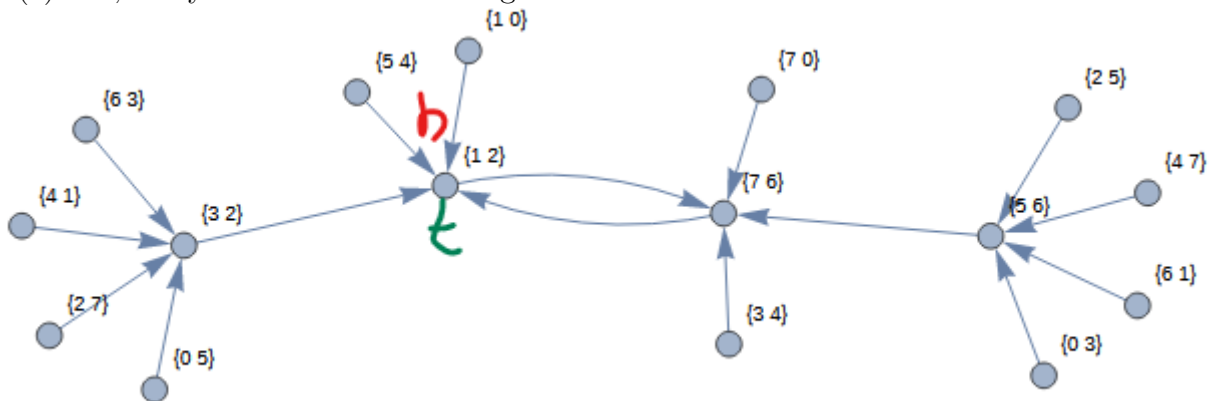


They are now on the same spot so we've found a cycle.

Now we must find the cycle length. The tortoise will remain still. The hare will move one step at a time. Set  $\lambda(s) = 0$  and add one for every step.



$\lambda(s) = 1$ , not yet the same so do it again.



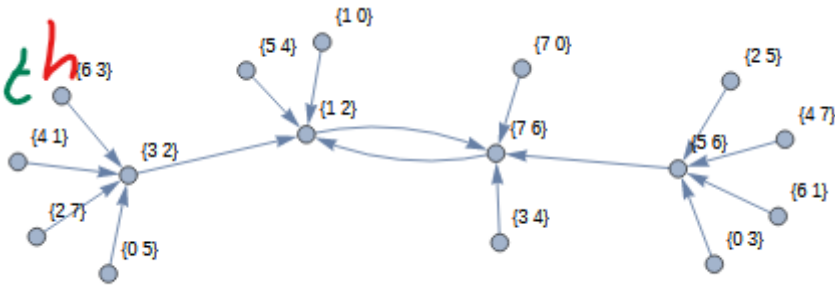
$\lambda(s) = 2$ , the two pointers point to the same node, so this is our final result. By our algorithm we have a cycle length of two.

## 2.2 Brent's algorithm

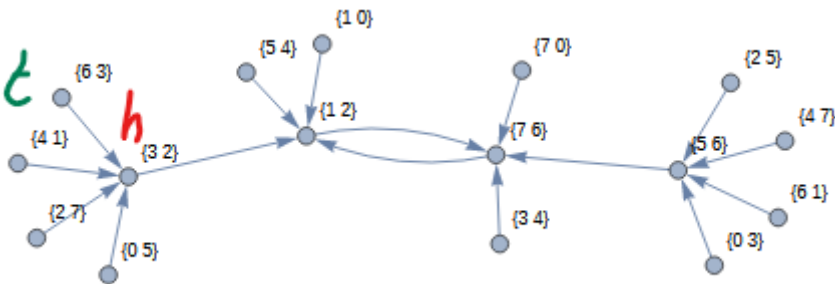
**Algorithm 2.** Just like Floyd's cycle finding algorithm, Brent's cycle finding algorithm [1] takes a function (a matrix multiplication in our case  $x \mapsto Ax, A \in \mathbb{Z}_m^{n \times n}$ ) and a starting point (a vector  $x_0 \in \mathbb{Z}_m^n$ ). It returns the length of the cycle ( $\lambda$ ) and the distance the starting point is from the closest point in the cycle ( $\mu$ ). Since we are only interested in the cycle lengths in this paper, we omit the explanation of finding  $\mu$ .

1. Check if  $x_0$  is a fixed point.
  - Set  $t = x_0$ , where  $t$  is the tortoise pointer.
  - Set  $h = Ax_0$ , where  $h$  is the hare.
  - Set  $p = 1$  and  $\lambda(s) = 1$ .
  - If  $t = h$ , then  $x_0$  is stationary return  $\lambda(s) = 1$ .
2. Setting up the remainder of the algorithm. If  $x_0$  is not fixed check what its cycle length is instead.
  - Let  $\lambda(s) = 0$ , a counting function counting the number of steps by taken by the hare.
  - Let  $\mathcal{P} = \{p_1, p_2, p_3, \dots\}$ , where  $p_1 = 2$  and  $p_j = 2p_{j-1}$ ,  $j = 2, 3, 4, \dots$
  - Set  $t$  to point at the same node as  $h$ .
  - Do step 3 using  $p_i = p_1$ .
3. Starting point - we return here every time we've gone through all substeps but  $t \neq h$ .
  - If  $t = h$ , return  $\lambda(s)$ .
  - Else if  $\lambda(s) = p_i$ , set  $\lambda(s) = 0$ , set  $t$  to point at the same node as  $h$ , and repeat step 3 with  $p_{i+1}$ .
  - Else the hare takes one step (i.e. compute  $Ah$ ).

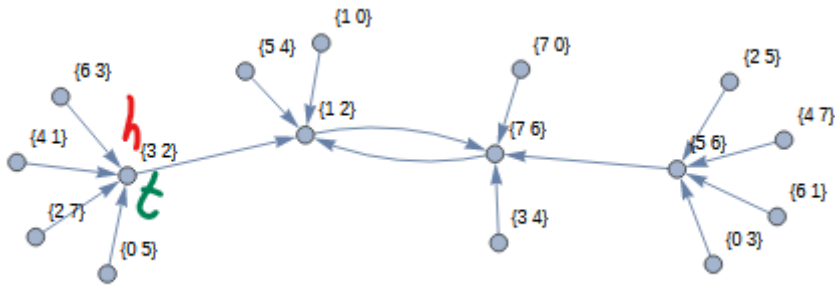
**Example 3.** Consider the same matrix  $A = \begin{bmatrix} 1 & 7 \\ 2 & 2 \end{bmatrix}$ , and starting point  $x_0 = \begin{bmatrix} 6 \\ 3 \end{bmatrix}$ , as above. The green  $t$  denotes the position of the tortoise, the red  $h$  illustrates the position of the hare. We start with  $p = 1$



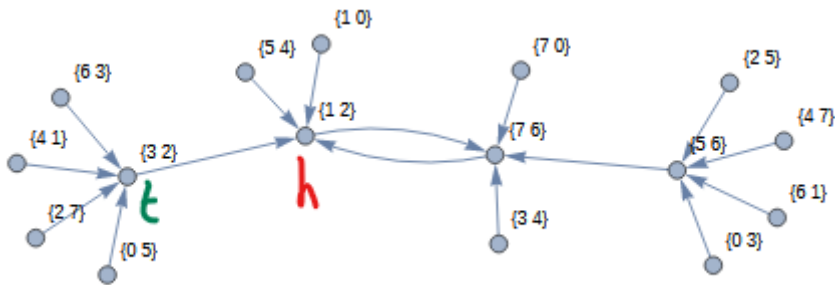
This is our starting position.



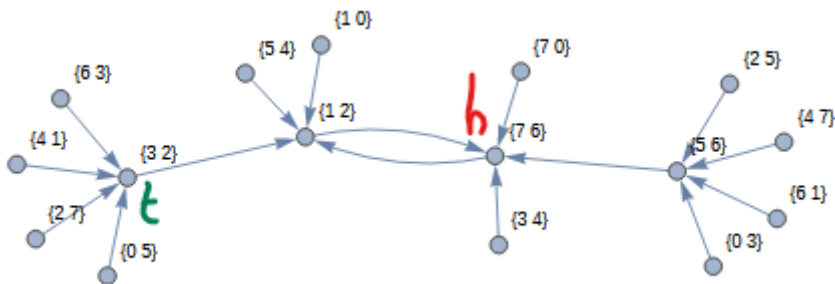
$\lambda = 1$ , we move the hare one step and see that  $h \neq t$ , so we set  $p = 2$  and  $\lambda = 0$ , and teleport the  $t$  to  $h$ .



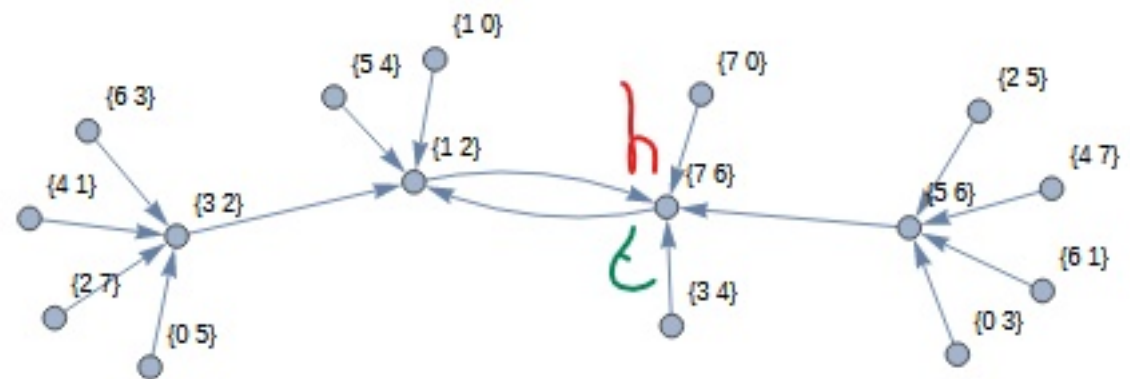
Bringing us to this situation.



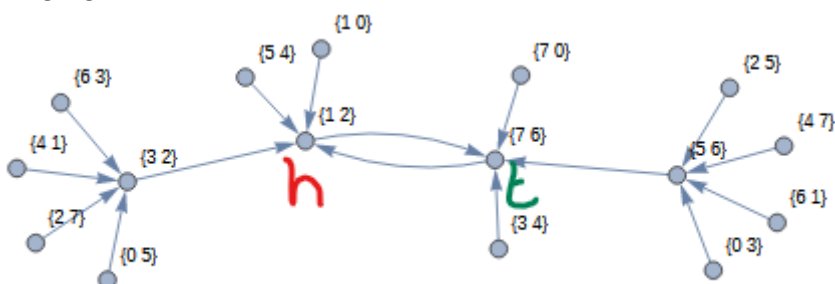
$\lambda = 1$ ,  $h \neq t$  so we take another step.



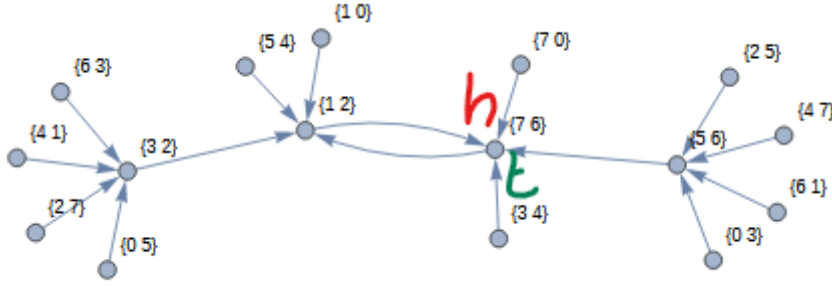
$\lambda = 2$ ,  $h \neq t$  so we set  $p = 4$ ,  $\lambda = 0$ , and teleport  $t$  to  $h$ .



Bringing us to this situation.



$\lambda = 1, h \neq t$  so we take another step



$\lambda = 2, h = t$  so we are done and return  $\lambda = 2$ , which we can see is correct.

### 2.3 Floyd's algorithm vs Brent's algorithm

According to [1], Brent's algorithm is, on average, 36% faster than Floyd's algorithm. Later on in this paper, when a statistical analysis is done on some larger matrices such as in Section 5, Brent's algorithm is verifiably faster. Therefore, there is an argument that Floyd's algorithm is obsolete for the needs of this paper and one should always use Brent's algorithm. Floyd's algorithm was, however, used for most of the examples and part of the statistical data of this paper.

## 3 Algebraic methods of finding the cycle structure

### 3.1 Number of elements with period $r$

We define  $\eta(r)$  to be the number of points for which  $A^r x \equiv x \pmod{m}$ . Note that this counts all the points  $x$  with period  $r$  and period  $d$  such that  $d \mid r$ .

We shall first discuss how to go from  $\eta(r)$  to the number of points of period  $r$  which we shall denote by  $\psi(r)$ . We also define  $\Psi(r)$  to be the number of cycles of length  $r$ , note that we have  $\Psi(r) = \frac{\psi(r)}{r}$ .

After discussing how to find  $\psi(r)$ , we shall discuss how to find  $\eta(r)$ .

#### 3.1.1 Möbius formula

**Definition 1** (Möbius function). Let  $n \in \mathbb{Z}^+$ , then

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1 \\ (-1)^k, & \text{if } n \text{ has a prime factorisation of } k \text{ unique primes without duplicates} \\ 0, & \text{otherwise} \end{cases}$$

**Theorem 1** (Möbius inversion formula). [8] Let  $f, g$  be arithmetic functions ( $f, g: \mathbb{Z} \rightarrow \mathbb{C}$ ) such that

$$g(n) = \sum_{d|n} f(d),$$

then

$$f(n) = \sum_{d|n} \mu(d) \cdot g\left(\frac{n}{d}\right),$$

where  $\mu$  is the Möbius function.

By the Möbius inversion formula we get

$$\psi(r) = \sum_{j|r} \eta\left(\frac{r}{j}\right) \mu(j). \quad (1)$$

Now that we know how to find  $\psi(r)$ , we shall discuss how to find  $\eta(r)$ .

### 3.1.2 The one by one case

**Proposition 1.** *Let  $a, b \in \mathbb{Z}$ ,  $m \in \mathbb{Z}^+$  and let  $\gcd(a, m) = d$ . Then the number of solutions to  $ax \equiv b \pmod{m}$  is equal to*

- 0 if  $d \nmid b$ ,
- $d$  if  $d \mid b$ .

*Proof.* We have  $ax \equiv b \pmod{m}$  which gives  $ax \equiv b + mr$  which gives  $ax - mr \equiv b$ . By the properties of a linear Diophantine equation this has solutions if and only if  $\gcd(a, m) \mid b$ .

Let  $x_0$  be a solution to the Diophantine equation. Then we have

$$x_0 + \frac{k_1 m}{d} \equiv x_0 + \frac{k_2 m}{d} \pmod{m},$$

which gives

$$\frac{k_1 m}{d} \equiv \frac{k_2 m}{d} \pmod{m},$$

which gives

$$k_1 \equiv k_2 \pmod{d}.$$

In modulo  $d$  there are exactly  $d$  solutions to this equation. □

**Corollary 1.1.** *Let  $f :: \mathbb{Z}_m \rightarrow \mathbb{Z}_m$ ,  $f(x) = ax$ , where  $a \in \mathbb{Z}_m$  is known. The number of elements for which holds that  $f^r(x) = a^r x = x$  is equal to the number of solutions to*

$$(a^r - 1)x \equiv 0 \pmod{m}, \quad (2)$$

*which is given by  $\gcd(a^r - 1, m)$ .*

*Proof.* This follows directly from the previous proposition. □

By (2), we have that for one dimensional matrices

$$\eta(r) = \gcd(a^r - 1, m) \quad (3)$$

### 3.1.3 Smith Normal Form

Another method uses the Smith normal form of the matrix  $A^r - I$ .

**Definition 2** (Smith normal form). Consider a matrix  $B \in \mathbb{Z}_m^{n \times n}$ . The Smith normal form of  $B$  is a diagonal matrix  $S$  with the diagonal entries  $s_1, s_2, \dots, s_n$  such that  $s_1 \mid s_2 \mid \dots \mid s_k$  and  $s_{k+1}, s_{k+2}, \dots, s_n = 0$ . There will also be two matrices  $P$  and  $Q$  such that  $S = PBQ$ .

**Algorithm 3** (Smith Normal Form). [3] In order to find  $P$ ,  $Q$ , and  $S$  we first consider

$$B = \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & B' & & \\ \vdots & & & \\ b_{n1} & & & \end{bmatrix},$$

using standard row and column operations we can alter all  $b_{1j}$  and  $b_{i1}$ ,  $i, j > 1$  such that

- $b_{kl} = 0$ , if  $b_{11} \mid b_{kl}$ ;
- $0 < b_{kl} < b_{11}$ , if  $b_{11} \nmid b_{kl}$  (by division algorithm).

If there exists a  $b_{kl} \neq 0$ , then we can make a row or column swap such that  $b_{kl}$  is our new  $b_{11}$ . and continue the above exercises till we have a scenario where all  $b_{kl} = 0$ .

Now we must ensure that  $b_{11}$  divides all elements of  $B'$ , if it doesn't yet the way we can do this is by doing a row or a column operation from a row or column number not 1 to the first row or column, then doing the previous step again. This will give that the new  $b_{11}$  is smaller than the previous one.

Eventually we will reach a point such that  $b_{11}$  divides all elements of  $B'$  and all other elements on the first row and column are equal to 0. At that point we take  $B'$  and do the same operation as we did on  $B$  giving us an  $b_{22}$  that divides everything.

When we go to  $B'$  we can only add and subtract the elements of  $A'$  from each other, we know from algebra that if  $b \mid c$  and  $b \mid d$  then  $b \mid (c + d)$  so we can be sure that  $b_{11} \mid b_{22}$ .

Continuing on with  $b_{33}, b_{44}, \dots, b_{nn}$ , we will get the  $S$  as described above.

In order to find  $P$  and  $Q$  we can use the same method (at the same time as finding  $S$ ), but by taking a look at the matrix

$$\begin{bmatrix} B & I_n \\ I_n & * \end{bmatrix},$$

where the elements of  $*$  are irrelevant. Both of the  $I_n$  will be modified as we do our operations as described above when trying to find  $S$ . Once we have found  $S$  our matrix will be of the form

$$\begin{bmatrix} S & P \\ Q & * \end{bmatrix},$$

giving us all three of the matrices we were looking for.

**Example 4.** Consider the matrix  $B = \begin{bmatrix} 2 & 4 & 1 \\ 3 & 2 & 6 \\ 1 & 0 & 4 \end{bmatrix}$ . In order to find the Smith form

of this matrix we construct

$$\begin{bmatrix} B & I_3 \\ I_3 & * \end{bmatrix} = \begin{bmatrix} 2 & 4 & 1 & 1 & 0 & 0 \\ 3 & 2 & 6 & 0 & 1 & 0 \\ 1 & 0 & 4 & 0 & 0 & 1 \\ 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{bmatrix}.$$

Subtracting the first row from the second gives

$$\begin{bmatrix} 2 & 4 & 1 & 1 & 0 & 0 \\ 1 & -2 & 5 & -1 & 1 & 0 \\ 1 & 0 & 4 & 0 & 0 & 1 \\ 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{bmatrix}.$$

Interchanging the first and second row gives

$$\begin{bmatrix} 1 & -2 & 5 & -1 & 1 & 0 \\ 2 & 4 & 1 & 1 & 0 & 0 \\ 1 & 0 & 4 & 0 & 0 & 1 \\ 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{bmatrix}.$$

Subtracting the first row twice from the second and once from the third gives

$$\begin{bmatrix} 1 & -2 & 5 & -1 & 1 & 0 \\ 0 & 8 & -9 & 3 & -2 & 0 \\ 0 & 2 & -1 & 1 & -1 & 1 \\ 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{bmatrix}.$$

Adding the first column twice to the second and subtracting it five times from the third gives

$$\begin{bmatrix} 1 & 0 & 0 & -1 & 1 & 0 \\ 0 & 8 & -9 & 3 & -2 & 0 \\ 0 & 2 & -1 & 1 & -1 & 1 \\ 1 & 2 & -5 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{bmatrix}.$$

Interchanging row two and three gives

$$\begin{bmatrix} 1 & 0 & 0 & -1 & 1 & 0 \\ 0 & 2 & -1 & 1 & -1 & 1 \\ 0 & 8 & -9 & 3 & -2 & 0 \\ 1 & 2 & -5 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{bmatrix}.$$

Adding the second column to the third gives

$$\begin{bmatrix} 1 & 0 & 0 & -1 & 1 & 0 \\ 0 & 2 & 1 & 1 & -1 & 1 \\ 0 & 8 & -1 & 3 & -2 & 0 \\ 1 & 2 & -3 & & & \\ 0 & 1 & 1 & & & \\ 0 & 0 & 1 & & & \end{bmatrix}.$$

Interchanging the second and third column gives

$$\begin{bmatrix} 1 & 0 & 0 & -1 & 1 & 0 \\ 0 & 1 & 2 & 1 & -1 & 1 \\ 0 & -1 & -2 & 3 & -2 & 0 \\ 1 & -3 & 2 & & & \\ 0 & 1 & 1 & & & \\ 0 & 1 & 0 & & & \end{bmatrix}.$$

Adding the second row to the third row gives

$$\begin{bmatrix} 1 & 0 & 0 & -1 & 1 & 0 \\ 0 & 1 & 2 & 1 & -1 & 1 \\ 0 & 0 & 10 & 4 & -3 & 1 \\ 1 & -3 & 2 & & & \\ 0 & 1 & 1 & & & \\ 0 & 1 & 0 & & & \end{bmatrix}.$$

Subtracting the second column twice from the third gives

$$\begin{bmatrix} 1 & 0 & 0 & -1 & 1 & 0 \\ 0 & 1 & 0 & 1 & -1 & 1 \\ 0 & 0 & 10 & 4 & -3 & 1 \\ 1 & -3 & 8 & & & \\ 0 & 1 & -1 & & & \\ 0 & 1 & -2 & & & \end{bmatrix} = \begin{bmatrix} S & P \\ Q & * \end{bmatrix}.$$

**Proposition 2.** According to Zerz [9], if we let  $S_i$  be the Smith form of  $I - A^i$ , then we have

$$\eta(i) = \prod_{k=1}^n \gcd(m, s_k),$$

where  $s_k$  is the  $k$ -th diagonal element of  $S_i$ .

### 3.2 Other methods

Other methods for finding  $\eta(r)$  exist, see for example [7], which uses more elementary methods.

### 3.3 Matrix order

**Definition 3.** Let  $A \in \mathbb{Z}_m^{n \times n}$ , we define the order of  $A$ , denoted  $\text{ord}(A)$ , to be  $k$  if there exists a  $k$  such that  $A^k = I$  and there's no  $0 < l < k$  such that  $A^l = I$ .

**Example 5.** Consider the matrix  $A = \begin{bmatrix} 2 & 3 & 5 \\ 1 & 4 & 2 \\ 3 & 5 & 1 \end{bmatrix} \pmod{7}$ , by iteratively computing

$A^k \pmod{7}$ ,  $k = 1, 2, 3, \dots$  we find that  $k = 18$  gives  $A^k = A^{18} = I$  giving that  $\text{ord}(A) = 18$ .

**Definition 4.** Let  $A \in \mathbb{Z}_m^{n \times n}$  such that there is no  $k$  for which  $A^k = I$ . However, since  $A$  is a finite linear dynamical system under itself  $((f, s) = (A, \mathbb{Z}_m^{n \times n}))$  there must be  $k_1 \neq k_2$  such that  $A^{k_1} = A^{k_2}$ , we say that  $\text{ord}(A) = k_2 - k_1$ .

**Example 6.** Consider the matrix

$$A = \begin{bmatrix} 1 & 2 & 0 \\ 2 & 2 & 2 \\ 2 & 2 & 2 \end{bmatrix} \pmod{3}.$$

We find

$$A^2 = \begin{bmatrix} 2 & 0 & 1 \\ 1 & 0 & 2 \\ 1 & 0 & 2 \end{bmatrix}, A^3 = \begin{bmatrix} 1 & 0 & 2 \\ 2 & 0 & 1 \\ 2 & 0 & 1 \end{bmatrix}.$$

After this we get  $A^2 = (A^{2+2k})$  and  $A^3 = A^{3+2k}$ , where  $k = 1, 2, 3, \dots$ , so the order of the matrix is 2.

**Proposition 3.** *All possible cycle lengths are divisors of  $\text{ord}(A)$ .*

*Proof.* Let  $A \in \mathbb{Z}_m^{n \times n}$  be arbitrary with  $\text{ord}(A) = k$ . Let  $A^c$  be the first matrix in the cycle. So we have that  $A^c = A^{k+c}$ .

Suppose there is a point  $x$  of period  $r < k$  such that  $r \nmid k$ . Then there is a cyclic point  $x_0$  such that

$$A^c x_0 = A^{r+c} x_0 = A^r A^c x_0.$$

Applying a change of coordinates,  $y_0 = A^c x_0$ , we get

$$A^r y_0 = y_0.$$

We have that

$$y_0 = A^k y_0 = A^{k+c} x_0 = A^k y_0 = A^{ar+b} y_0 = A^b y_0,$$

but this gives that  $y_0$  and thus  $x_0$  is  $b < r$  cyclic, a contradiction. Giving the result.  $\square$

Through this we conclude that we only have to check for divisors of the order of  $A$  when checking for the lengths of cycles in a system.

We now have both algebraic and non-algebraic methods of finding the cycle structure of a dynamical system. Now we shall look at some special case systems.

## 4 Special case matrices

### 4.1 Nilpotent matrices

**Definition 5.** Consider a matrix  $A \in \mathbb{Z}_m^{n \times n}$ , we say that  $A$  is nilpotent if there exists a  $k$  such that  $A^k = 0$ .

Note that  $\text{ord}(A) = 1$ . We can show that for any nilpotent matrix, the system  $(A, \mathbb{Z}_m^n)$  has a single fixed point, with no other cycles.

**Lemma 1.** *Let  $f(x) = Ax$ ,  $A \in \mathbb{Z}_m^{n \times n}$  nilpotent, and  $x \in \mathbb{Z}_m^n$ . Then for some  $k \in \mathbb{Z}_+$  we have*

$$f^k(x) = 0.$$

*Proof.* Since  $A$  is nilpotent we have

$$f^k(x) = A^k x = 0_{n \times n} x = 0. \quad \square$$



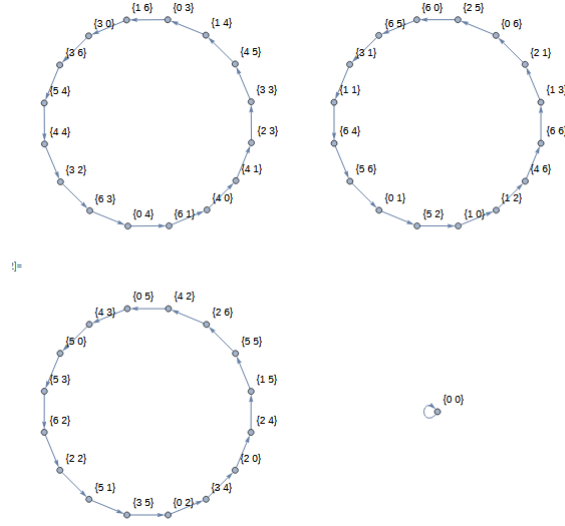


Figure 4.3: Example of the graph generated by an invertible matrix

*Proof.* Suppose  $A$  is invertible with inverse  $B$ . We have

$$1 = \det(I) = \det(AB) = \det(A) \det(B)$$

giving that  $\det(A) = (\det(B))^{-1}$ . Conversely, if  $\det(A)$  is a unit then

$$A \operatorname{adj}(A) = \det(A)I = \operatorname{adj}(A)A$$

giving that

$$A((\det(A))^{-1} \operatorname{adj}(A)) = I = ((\det(A))^{-1} \operatorname{adj}(A))A$$

giving that  $A$  is invertible with

$$A^{-1} = (\det(A))^{-1} \operatorname{adj}(A). \quad \square$$

*remark: in a field (i.e. when  $m$  is prime) every non-zero element is a unit.*

**Proposition 5.** *Let  $A \in \mathbb{Z}_m^{n \times n}$  be invertible. Then the graph  $\mathfrak{G}(A, \mathbb{Z}_m^n)$  is cyclic, i.e. all elements are part of a cycle.*

*Proof.* Suppose that  $\mathfrak{G}$  is not cyclic. Then there exists a  $x_0$ , cyclic, such that  $Ax_c = x_0$ ,  $x_c$  cyclic, and  $Ax_l = x_0$ ,  $x_l$  not cyclic, giving that  $A^{-1}x_0 = x_c$  and  $A^{-1}x_0 = x_l$ . But by injectivity of matrix multiplications we have that  $x_c = x_l$ , a contradiction, giving the result.  $\square$

**Example 8.** Consider  $A = \begin{bmatrix} 1 & 5 \\ 2 & 2 \end{bmatrix} \pmod{7}$ , we have that  $\det(A) \equiv 1 \cdot 2 - 2 \cdot 5 \pmod{7} \equiv -8 \pmod{7} \equiv 6 \pmod{7}$ . By our proposition,  $A$  should generate a cyclic graph. We plotted the graph in figure 4.3, we can see that the graph is fully cyclic as expected.

### 4.3 Diagonal matrices

By Equation (3), we know that  $\eta(r) = \gcd(a^r - 1, m)$  for  $1 \times 1$  matrices. Furthermore, by Equation (1), we know that  $\psi(r) = \sum_{d|r} \eta\left(\frac{r}{d}\right) \mu(d)$ , where  $\mu$  is the Möbius function.

We can combine these two elements to get

$$\psi(r) = \sum_{d|r} \gcd(a^{r/d} - 1, m) \mu(d) \quad (4)$$

and

$$\Psi(r) = \frac{1}{r} \sum_{d|r} \gcd(a^{r/d} - 1, m) \mu(d). \quad (5)$$

### 4.3.1 cycle structure

**Definition 8.** The euler totient function, denoted by  $\phi(m)$  counts the number of positive integers  $n$  smaller than  $m$  such that  $\gcd(m, n) = 1$ .

**Lemma 4.** Let  $a \in \mathbb{Z}_m^n$ . Then the order of  $a$  is a divisor of  $\phi(m)$ .

*Proof.* The size of the multiplicative group of integers modulo  $m$  is  $\phi(m)$ . By Lagrange's theorem, the size of all subgroups (cycles) must divide the size of the group, giving the result.  $\square$

**Lemma 5.** Let  $A_j = \{A_{j,1}, A_{j,2}, \dots, A_{j,r_j}, \dots\}$ , for  $j = 1, 2, \dots, n$  be ordered sets. Let

$$S = \{(A_{1,1}, A_{2,1}, \dots, A_{n,1}), \dots, (A_{1,r}, A_{2,r}, \dots, A_{n,r})\}$$

ordered, such that

$$(A_{1,r+1}, A_{2,r+1}, \dots, A_{n,r+1}) \text{ is equivalent to } (A_{1,1}, A_{2,1}, \dots, A_{n,1}).$$

Then  $r = \text{lcm}(r_1, r_2, \dots, r_n)$ .

*Proof.* We shall prove this by induction. First, suppose  $n = 2$ . We know that  $A_{1,1} \equiv A_{1,k_1 \cdot r_1+1}$  and  $A_{2,1} \equiv A_{2,k_2 \cdot r_2+1}$ ,  $k_1, k_2 \in \mathbb{Z}_+$ . Both equivalences hold if and only if

$$k_1 \cdot r_1 = k_2 \cdot r_2,$$

this is true if

$$k_1 \cdot r_1 = k_2 \cdot r_2 = \text{lcm}(r_1, r_2)$$

or a multiple thereof. This gives that the cycle length of two combined cycles is given by  $\text{lcm}(r_1, r_2)$ .

Suppose that for  $n = p$ , the cycle length of cycles with lengths  $r_1, r_2, \dots, r_p$  is given by  $\text{lcm}(r_1, r_2, \dots, r_p)$ . We shall now prove that for  $n = p + 1$  the cycle length of cycles with lengths  $r_1, r_2, \dots, r_p, r_{p+1}$  is given by  $\text{lcm}(r_1, r_2, \dots, r_p, r_{p+1})$ .

The first  $p$  elements generate a single cycle of length  $r_0 = \text{lcm}(r_1, r_2, \dots, r_p)$  by the induction hypothesis. So we have two cycles, one of length  $r_0$  and one of length  $r_{p+1}$ . By the first part of this proof, the cycle length of the combined cycle of these two is given by  $\text{lcm}(r_0, r_{p+1})$ . Overall this gives

$$\text{lcm}(r_0, r_{p+1}) = \text{lcm}(\text{lcm}(r_1, r_2, \dots, r_p), r_{p+1}) = \text{lcm}(r_1, r_2, \dots, r_p, r_{p+1}),$$

giving the result.  $\square$

**Lemma 6.** Let  $A = \{A_1, A_2, \dots, A_a, \dots\}$  where  $A_1$  through  $A_a$  are unique elements, ordered and the elements  $A_{k \cdot a + i} = A_i$  for every integer  $k$ . Let  $B = \{B_1, B_2, \dots, B_b, \dots\}$  where  $B_1$  through  $B_b$  are unique elements, ordered and the elements  $B_{k \cdot b + i} = B_i$  for every integer  $k$ .

Let  $S_1 = \{(A_1, B_1), (A_2, B_2), \dots, (A_{\text{lcm}(a,b)}, B_{\text{lcm}(a,b)})\}$ ,  
 $S_2 = \{(A_1, B_2), (A_2, B_3), \dots, (A_{\text{lcm}(a,b)}, B_1)\}$ , et cetera for all  $S_r$ ,  $r \in \mathbb{Z}_+$ .

Claim: There are exactly  $\text{gcd}(a, b)$  unique sets amongst all  $S_r$ .

*Proof.* without loss of generality we assume that  $a > b$ . Take the subset

$$D = \{(A_1, B_j), (A_2, B_{j+1}), \dots, (A_a, B_{j+a-1})\}$$

of an arbitrary  $S_r$ . clearly  $|D| = a$ . There's exactly  $\frac{\text{lcm}(a,b)}{a}$  such subsets of the arbitrary  $S_r$  where the first element of the first tuple is equivalent to  $A_1$ . This means that  $\frac{\text{lcm}(a,b)}{a}$  unique elements of  $B_j$  have been in the same tuple as  $A_1$ . By shifting the  $B_j$  elements once, we get

$$D_2 = \{(A_1, B_{j+1}), (A_2, B_{j+2}), \dots, (A_a, B_{j+a})\},$$

which is a subset of  $S_{r+1}$  and gives another  $\frac{\text{lcm}(a,b)}{a}$  unique elements of  $B_j$  that are linked to  $A_1$ . There's a total of  $b$  elements of the form  $B_j$  so the number of shifts we have to do can be computed by

$$\frac{\text{lcm}(a, b)}{a} \cdot x = b,$$

which gives

$$x = \text{gcd}(a, b).$$

This gives that there is exactly  $\text{gcd}(a, b)$  unique subsets amongst all  $S_r$ .  $\square$

**Proposition 6.** Let  $A \in \mathbb{Z}_m^{n \times n}$  be a diagonal matrix. Let  $\Psi_k(t)$  be the number of cycles of length  $t$  for the  $k$ -th diagonal element. The number of cycles of length  $i$  created by the diagonal matrix is given by

$$\Psi_A(i) = \sum_{C_i} \frac{1}{r_1} \prod_{j=1}^n \text{gcd}(r_1, r_j) \cdot \Psi_j(r_j)$$

where  $r_j$  is the cycle length of the  $j$ -th diagonal element and  $C_i$  is the set of all combinations such that  $\text{lcm}(r_1, r_2, \dots, r_n) = i$ .

*Proof.* By Lemma 6 we have that  $n$  cycles of lengths  $r_1, r_2, \dots, r_n$  combined generate a single cycle of length  $i = \text{lcm}(r_1, r_2, \dots, r_n)$ .

By Lemma 6, the number of unique ways to combine cycles of lengths  $r_1, r_2$  is given by  $\text{gcd}(r_1, r_2)$ . This means that the number of unique ways to combine  $n$  cycles of lengths  $r_1, r_2 \dots r_n$  is given by

$$\prod_{j=2}^n \text{gcd}(r_1, r_j).$$

Since  $\frac{1}{r_1} \cdot \text{gcd}(r_1, r_1) = 1$ , we write

$$\prod_{j=1}^n \text{gcd}(r_1, r_j).$$

This gives the number of unique ways per cycle. If we know the number of cycles of different lengths we can multiply by that number giving

$$\prod_{j=1}^n \gcd(r_1, r_j) \cdot \Psi_j(r_j).$$

Now we need to count all the different ways to get a cycle of length  $i$ , which is given by  $\sum_{C_i}$ . In total we get

$$\Psi_A(i) = \sum_{C_i} \frac{1}{r_1} \prod_{j=1}^n \gcd(r_1, r_j) \cdot \Psi_j(r_j). \quad \square$$

**Corollary 6.1.** *Let  $A \in \mathbb{Z}_m^{n \times n}$  be a diagonal matrix. Then the maximum cycle length of any cycle created by  $A$ , diagonal, is smaller or equal to  $\phi(m)$ .*

*Proof.* We know that the cycle length is given by the least common multiple of elements that are all divisors of  $\phi(m)$  hence their least common multiple is at most  $\phi(m)$ .  $\square$

Combining all these elements we get

$$\Psi_A(i) = \sum_{C_i} \frac{1}{r_1} \prod_k (\gcd(r_1, r_k) \sum_{h|i} (\gcd(a^{i/h} - 1, m) \cdot \mu(h))), \quad (6)$$

where  $r_1 = \max\{r_1, r_2, \dots, r_n\}$ .

**Example 9.** Consider the matrix  $A = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 5 \end{bmatrix} \pmod{7}$ , the individual cycle structures can be calculated through the methods described in 3.1 and are given by:

- $\Psi_1(1) = 1, \Psi_1(3) = 2;$
- $\Psi_2(1) = 1, \Psi_2(3) = 2;$
- $\Psi_3(1) = 1, \Psi_3(6) = 1.$

We find  $C_1 = \{(1, 1, 1)\}$ ,  $C_3 = \{(1, 3, 1), (3, 1, 1), (3, 3, 1)\}$ , and

$C_6 = \{(1, 1, 6), (1, 3, 6), (3, 1, 6), (3, 3, 6)\}$ . This gives

$$\begin{aligned}
\Psi_A(1) &= \frac{1}{1}(\gcd(1, 1) \cdot 1)^3 = 1, \\
\Psi_A(3) &= \frac{1}{3} \cdot \gcd(3, 3) \cdot 2 \cdot \gcd(3, 1) \cdot 1 \cdot \gcd(1, 3) \cdot 1 \\
&\quad + \frac{1}{3} \cdot \gcd(3, 3) \cdot 2 \cdot \gcd(3, 1) \cdot 1 \cdot \gcd(1, 3) \cdot 1 \\
&\quad + \frac{1}{3} \cdot \gcd(3, 3) \cdot 2 \cdot \gcd(3, 3) \cdot 2 \cdot \gcd(1, 3) \cdot 1 \\
&= 2 + 2 + 2 \cdot 3 \cdot 2 = 2 + 2 + 12 = 16, \\
\Psi_A(6) &= \frac{1}{6} \cdot \gcd(6, 6) \cdot 1 \cdot \gcd(6, 1) \cdot 1 \cdot \gcd(6, 1) \cdot 1 \\
&\quad + \frac{1}{6} \cdot \gcd(6, 6) \cdot 1 \cdot \gcd(6, 3) \cdot 2 \cdot \gcd(6, 1) \cdot 1 \\
&\quad + \frac{1}{6} \cdot \gcd(6, 6) \cdot 1 \cdot \gcd(6, 3) \cdot 2 \cdot \gcd(6, 1) \cdot 1 \\
&\quad + \frac{1}{6} \cdot \gcd(6, 6) \cdot 1 \cdot \gcd(6, 3) \cdot 2 \cdot \gcd(6, 3) \cdot 2 \\
&= 1 + 3 \cdot 2 + 3 \cdot 2 + 3 \cdot 2 \cdot 3 \cdot 2 = 1 + 6 + 6 + 36 = 49.
\end{aligned}$$

**Example 10.** Consider the matrix  $A = \begin{bmatrix} 4 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 5 \end{bmatrix} \pmod{8}$ , the cycle structures are as follows:

- $\Psi_1(1) = 2, \Psi_1(2) = 3;$
- $\Psi_2(1) = 1;$
- $\Psi_3(1) = 4, \Psi_3(2) = 2.$

By Proposition 6, we have that the number of cycles is given by

$$\begin{aligned}
\Psi_A(1) &= \frac{1}{1} \cdot \gcd(1, 1) \cdot 2 \cdot \gcd(1, 1) \cdot 1 \cdot \gcd(1, 1) \cdot 4 = 8, \\
\Psi_A(2) &= \frac{1}{2} \cdot \gcd(1, 2) \cdot 2 \cdot \gcd(1, 2) \cdot 1 \cdot \gcd(2, 2) \cdot 2 \\
&\quad + \frac{1}{2} \cdot \gcd(2, 2) \cdot 3 \cdot \gcd(1, 1) \cdot 1 \cdot \gcd(1, 2) \cdot 4, \\
&\quad + \frac{1}{2} \cdot \gcd(2, 2) \cdot 3 \cdot \gcd(1, 2) \cdot 1 \cdot \gcd(2, 2) \cdot 2 \\
&= \frac{1}{2} \cdot 2 \cdot 2 \cdot 2 + \frac{1}{2} \cdot 2 \cdot 3 \cdot 4 + \frac{1}{2} \cdot 2 \cdot 3 \cdot 2 \cdot 2 = 4 + 12 + 12 = 28.
\end{aligned}$$

## 5 Statistical analysis of matrices

To find out the maximum possible cycle length of the set of all cycle lengths generated by all matrices  $A \in \mathbb{Z}_m^{n \times n}$ , we can iterate over all these matrices and use Brent's algorithm to find out the cycle lengths they produce.

Furthermore, if we want to how know many of these matrices create at least one cycle with length equal to that maximum length, we can iterate over all those

matrices, again using Brent's algorithm, and count how many such matrices there are.

In the first subsection 5.1 we do a numerical research the first question, in the second subsection 5.2 we research the second question.

In the end, we hope to give some data and ideas that may help prove some conjectures.

### 5.1 Maximal cycle length modulo $m$

The maximal cycle length for  $n \times n$  matrices modulo  $m$  for  $n = 2$  is given by the following table.

<b>m</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>8</b>	<b>9</b>	<b>10</b>
	3	8	6	24	24	48	12	24	60
<b>m</b>	<b>11</b>	<b>12</b>	<b>13</b>	<b>14</b>	<b>15</b>	<b>16</b>	<b>17</b>	<b>18</b>	<b>19</b>
	120	24	168	48	60	24	288	24	360
<b>m</b>	<b>20</b>	<b>21</b>	...	<b>25</b>	<b>27</b>	81			
	60	168	...	120	$\exists$ 72	$\exists$ 216			

The ones with a  $\exists$ , denote that there is at least one matrix that has a cycle with that length exists, no larger cycle was found, but not all matrices were checked for their maximum cycle length.

Furthermore, all prime numbers  $p$  up to 53 have maximal cycle length of the form  $p^n - 1$ .

**Conjecture 1.** *The maximum cycle length generated by a matrix is equal to the order of the matrix.*

From 3 we already know that all cycle lengths divide the order of  $A$ . So all that has to be proven is that there exists a cycle with length equal to the order.

**Conjecture 2.** *Let  $\mathfrak{S}(n, m) = \{A \in \mathbb{Z}_m^{n \times n}\}$ , where  $m = p^k$  a prime power. Then the largest possible cycle length is given by*

$$(p^n - 1) \cdot p^{k-1}.$$

*Note: for  $m = p^1$  a prime, we get  $p^{k-1} = 1$ .*

From the table we can see that this conjecture holds true for many specific scenarios. For matrices that has the maximum cycle length modulo a prime, we can see it also has the maximum cycle length modulo a power of that prime such as in the below example.

By Lemma 5.3 in [2] we have that if a point is  $r$  cyclic in modulo  $p^k$ , then it is either  $r$  cyclic or  $pr$  cyclic in modulo  $p^{k+1}$ . If we can show that for every modulo a prime  $p$  we have that the largest cycle is of length  $p^n - 1$  and there exists at least one point which multiplies its cycle length by  $p$  when lifted into a higher prime power, the conjecture will be proven.

**Example 11.** Let  $A = \begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix} \pmod{3}$ .  $A$  generates a one cycle and an eight cycle.

If we extend this into higher powers we get

- mod  $3^2$ :  $3 \times 24$  cycle,  $1 \times 8$  cycle, and  $1 \times 1$  cycle.

- mod  $3^3$ :  $9 \times 72$  cycle,  $3 \times 24$  cycle,  $1 \times 8$  cycle, and  $1 \times 1$  cycle.
- mod  $3^4$ :  $27 \times 216$  cycle,  $9 \times 72$  cycle,  $3 \times 24$  cycle,  $1 \times 8$  cycle, and  $1 \times 1$  cycle.

## 5.2 Proportion of matrices with maximal cycle length

By running all matrices through Brent's algorithm and finding out if they have the maximum possible cycle length we find the proportion of matrices that will result in a graph with a cycle of maximal length.

<b>m</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
	$\frac{2}{16} = 12.5\%$	$\frac{12}{81} \approx 14.81\%$	$\frac{24}{256} = 9.375\%$	$\frac{80}{625} \approx 12.8\%$
<b>m</b>	<b>6</b>	<b>7</b>	<b>8</b>	<b>9</b>
	$\frac{24}{1296} \approx 1.85\%$	$\frac{336}{2401} \approx 13.99\%$	$\frac{256}{4096} = 6.25\%$	$\frac{864}{6561} \approx 13.17\%$
<b>m</b>	<b>10</b>	<b>11</b>	<b>12</b>	<b>13</b>
	$\frac{96}{10000} = 0.96\%$	$\frac{1760}{14641} \approx 12.02\%$	$\frac{384}{20736} \approx 1.85\%$	$\frac{3744}{28561} \approx 13.11\%$
<b>m</b>	<b>14</b>	<b>15</b>	<b>16</b>	
	$\frac{5712}{38416} \approx 14.5\%$	$\frac{768}{50625} \approx 1.52\%$	$\frac{5712}{38416} = 6.25\%$	

## 6 Discussion

In this thesis several methods of finding the cycle structure created by a matrix  $A$  over a set  $\mathbb{Z}_m^n$  were discussed. As well as the cycle structure of several special case matrices. In the end we presented some conjectures along with statistical data of maximal cycle lengths.

This leaves room for future work in proving these conjectures. Perhaps some other papers have useful ideas regarding the problems

Another idea is the lifting of a matrix from modulo  $m$  to a higher modulo such as done in Example 11, we can see a pattern of having  $p^{k-1}$  cycles of the maximum length where  $p^k$  is the modulo. This pattern can be found in several examples. Perhaps conjecture 2 can be proven through the pattern shown in the example.

Perhaps it is also possible to extend conjecture 2 to general  $m$ , not just prime power. Though we cannot give any ideas for what to look into first.

Once conjecture 2, or its extended version, has been proven, one can look into how to construct a matrix  $A \in \mathbb{Z}_m^{n \times n}$ , gives  $m$  and  $n$  such that  $A$  generates at least one cycle of maximum length.

Separately, it should be possible to speed up the iterative methods of finding the cycle structure by using [6]. Lindenberg gives a maximum height (steps from  $x_0$  to the closest cyclic point) of a system. A two steps algorithm should be faster than both Floyd's and Brent's algorithm at least for larger  $m$  and  $n$ . First taking a number of steps equal to that max height, thus ensuring we are in the cycle, then taking one step at a time and checking if we're back to the start of our cycle. It remains to be seen how such an algorithm would fare if also looking to find the height of the system.

## References

- [1] Richard P Brent. "An improved Monte Carlo factorization algorithm". In: *BIT Numerical Mathematics* 20.2 (1980), pp. 176–184.
- [2] G. Deng. "Cycles of linear dynamical systems over finite local rings". In: *Journal of Algebra* 433 (2015), pp. 243–261.
- [3] R. Howard. "Rings, Determinants, the Smith Normal Form, and Canonical Forms for Similarity of Matrices". In: *Class notes for mathematics 700* (2002), pp. 70–76.
- [4] D. Huffman. "A linear circuit viewpoint on error-correcting codes". In: *IRE Transactions on Information Theory* 2.3 (1956), pp. 20–28. DOI: 10.1109/TIT.1956.1056806.
- [5] D.E. Knuth. "The Art of Computer Programming, vol. II: Seminumerical Algorithms". Addison-Wesley, 1969, p. 7.
- [6] B. Lindenberg. "On Fixed Point Convergence of Linear Finite Dynamical Systems". 2016.
- [7] R. Nyqvist M. Nilsson. "Number of solutions of Linear Congruence Systems". <https://arxiv.org/abs/1208.3550>. 2021. (Visited on 25/01/2024).
- [8] A. F. Möbius. "Über eine besondere Art vom Umkehrung der Reihen (in German)". In: *Journal für die reine und angewandte Mathematik* 9 (1832), pp. 105–123.
- [9] E. Zerz and H. Giese. "Computing the Cycle Structure of Finite Linear Dynamical Systems". In: *IFAC PapersOnLine* 53-2 (2020), pp. 4316–4321.