# Algebraic Methods for Finite Linear Cellular Automata

Dow, R. A.

# Algebraic Methods for Finite Linear Cellular Automata

A thesis submitted to the
University of London for the
degree of Doctor of Philosophy by

**R. A. Dow**

Queen Mary and Westfield College,
University of London, Febuary 1996.

# Abstract

Cellular automata are a simple class of extended dynamical systems which have been much studied in recent years. Linear cellular automata are the class of cellular automata most amenable to algebraic analytic treatments, algebraic techniques are used to study finite linear cellular automata and also finite linear cellular automata with external inputs.

General results are developed for state alphabet a finite commutative ring and a notion of qualitative dynamical similarity is introduced for those systems consisting of a fixed linear cellular automata rule but with distinct time independent inputs. Sufficient conditions for qualitative dynamical similarity are obtained in the general case.

Exact results are obtained for the case of state alphabet a finite field, including new results for finite linear cellular automata without inputs and a complete description of the behaviour of the corresponding system with time independent inputs. Necessary and sufficient conditions for qualitative dynamical similarity in this case are given.

Results for the hitherto untreated case of state alphabet the integers modulo $p^k$, $p$ prime and $k > 1$, are obtained from those for the finite field case by the technique of idempotent lifting. These two cases suffice for the treatment of the general case of state alphabet the integers modulo any positive integer $m > 1$, in particular a necessary and sufficient condition for qualitatively similar dynamics in the presence of time independent inputs is given for this case.

The extension of the results for time independent inputs to the case of periodic and eventually periodic inputs is treated and the generalisation of the techniques developed to higher dimensional linear cellular automata is discussed.

# Acknowledgements

The list of people to whom I owe thanks for the support, both academic and personal, I have received during the preparation of this thesis is long, but special thanks must go to two individuals: David Arrowsmith, my supervisor, whose door was always open and who showed considerable patience and Denise Herraghty, my partner, whose support and understanding have been vital and whose forbearance in the last month of the gestation of this volume was formidable.

The mathematics department at Queen Mary and Westfield College is a stimulating environment to work in and my gratitude extends to all the staff (academic and secretarial) and to my fellow students. In particular I am indebted to Anne Cook for being extremely competent, Richard Frewin for much help on matters relating to computers and Peter Kropholler for useful discussions on the algebraic aspects of my work. I also wish to thank those of my friends in or once of the department I have not already mentioned: Xochitl Cano-Blanco, Andy Davies, Simon Green, Eamon Kerrins, Richard Nelson, Ruth Silverstone, Leonard Soicher and John Watson.

My family and my friends from outside of the academic environment have been of considerable support, in particular Justin Atkinson, Joanna Dolby, Tim Hanson, Matthew Ramsey, Joanna Sweeny and last but certainly not least Bob White, without whose financial aid in the last few months I would never have completed this thesis.

# Contents

# Chapter 1

# Introduction

Cellular automata are a type of extended dynamical system which are discrete in both time and space and which have attracted considerable attention in recent years, both as interesting systems in their own right and as the simplest examples of extended systems. Linear cellular automata are the class of cellular automata most amenable to analytical study and there is evidence that an understanding of linear cellular automata will aid the understanding of nonlinear cellular automata (for instance see the papers by Jen [1] and Bartlett and Garzon [2]).

A natural question to ask of any autonomous closed system is: what happens to the behaviour of the system in the presence of external inputs? Such inputs can be viewed as the natural consequence of the systems interaction with the world around it or as a deliberate attempt at influencing or controlling the behaviour of the system. As far as we are aware there has been no previous attempt made to study deterministic cellular automata in the presence of external inputs and we begin such a study by looking at linear cellular automata in the presence of inputs.

Before we begin a general discussion of the contents of this thesis we shall briefly discuss its history. The work began as a study of additive cellular automata with external time independent inputs using the methods introduced for additive cellular automata in the classic paper by Martin *et.al.* [3]. In the course of this work it became apparent that the number of qualitatively different behaviours exhibited by the system consisting of a linear cellular automata and a time independent input as different choices of input were made was very small in comparison to the number of possible choices of input.

In attempting to quantify the above comment and to catalogue the possible behaviours available to the system we introduced a notion of qualitative dynamical similarity (which is described in chapter 2, section 2.3) and developed theorem 2.3.3 in an attempt to find necessary and sufficient conditions for qualitative dynamical similarity between systems consisting of the same linear cellular automata but with different inputs, however theorem 2.3.3 relies upon a strong condition and it was not clear *a priori* that this condition would be satisfied in any generality. In attempting to prove that the condition of theorem 2.3.3 is satisfied for a large class of state alphabets (the integers modulo $m$ for any integer $m > 1$ or equivalently $\mathbb{Z}/m\mathbb{Z}$) we were led to introduce the formalisation of the methods of Martin *et.al.* which we describe in detail in section 1.5.3.

It rapidly became evident that it was in fact worth "starting from scratch" and thus we reworked the theory of linear cellular automata with periodic boundary conditions

over a finite field using the above mentioned method and including time independent inputs. The use we made of direct products of rings in the above task then suggested that we could extend results from the finite field case to that of state alphabet $\mathbb{Z}/p^k\mathbb{Z}$, $p$ prime and $k > 1$, for which no results had been available previously.

In the rest of this chapter we present the basic definitions and ideas, beginning with a formal definition of a cellular automata in section 1.1 and introducing boundary conditions and finite cellular automata in section 1.2. Hybrid cellular automata are discussed in section 1.3 as some results for hybrids of linear cellular automata are included in chapter 2 and also as linear cellular automata with time independent inputs are equivalent to a class of hybrid cellular automata (see section 1.5.4). In section 1.4 state transition graphs and cycle sets are discussed, these are useful tools used throughout this thesis.

Section 1.5 is devoted to finite linear cellular automata (as is the rest of the thesis) beginning in 1.5.1 with a short review of the literature on this topic. Matrix representations of finite linear cellular automata are discussed in section 1.5.2. In 1.5.3 the representation of linear cellular automata with periodic boundary conditions which is used throughout the thesis is introduced and discussed in detail. In this representation the cellular automata on $N$ cells becomes a linear map from a ring $R_N$ (related to a finite commutative ring $R$ chosen as state alphabet) to itself.

In 1.5.4 time independent inputs are introduced, in the case of periodic boundary conditions on $N$ cells the system is now equivalent to an affine map from $R_N$ to itself. The relevant results obtained by Martin *et.al.* [3] are described in 1.5.5.

In chapter 2 we discuss the general case where the state alphabet $R$ is any finite commutative ring, beginning in section 2.1 with some basic results and the development of some notation used throughout the thesis. Recent interest in cellular automata as pseudorandom number generators (see [4],[5] and [6]) focuses on the possibility of single cycles visiting all non-zero configurations of the system, we show that linear cellular automata with periodic boundary conditions and state alphabet a finite commutative ring on $N > 1$ cells cannot posses such cycles in theorem 2.1.1. In section 2.2 the structure of the state transition graph of a finite linear cellular automata with time independent input is discussed and related to the state transition graph of the cellular automata without inputs.

In section 2.3 the idea of qualitative dynamical similarity between systems consisting of the same linear cellular automata but with different inputs is introduced and sufficient conditions for such qualitative dynamical similarity to occur are found in terms of an

equivalence relation on the set of possible inputs. In theorem 2.3.3 a necessary and sufficient condition for qualitative dynamical similarity is found, provided a certain condition is satisfied. Much of our treatment of linear cellular automata with periodic boundary conditions and time independent inputs for more restricted choices of state alphabet is geared toward showing that the condition of theorem 2.3.3 is satisfied. The results of chapter 2 can be regarded as a toolbox for use in later chapters.

In chapters 3 and 4 we consider cellular automata with periodic boundary conditions and state alphabet a finite field $\mathbb{F}_{p^q}$ (any prime $p$ and any integer $q > 0$), beginning in chapter 3 by obtaining a direct product decomposition of the ring $R_N$ in this case, related to the factorisation of the polynomial $x^N - 1$ over $\mathbb{F}_{p^q}$. The rings in this direct product are completely primary (that is every element is either a unit or nilpotent) and in fact are either finite fields themselves or ring extensions of finite fields with a maximal, principal, ideal of nilpotent elements (technically speaking such rings are known as *local* and the ideal consisting of all the nilpotent elements is a *prime* ideal, however these concepts are not discussed in the main text). The rest of chapter 3 is devoted to discussing the relevant dynamics in these rings and establishing the connections between the cases of $np^r$ cells and $np^{r+j}$ cells where integer $n > 0$ is coprime to $p$ and $r, j \in \mathbb{N}$.

In chapter 4 the results of chapter 3 are employed to gain exact results for linear cellular automata with state alphabet the finite field $\mathbb{F}_{p^q}$ and periodic boundary conditions, both with and without inputs. Whilst some of the material in chapters 3 and 4 is equivalent to earlier work, not all of it is, in particular the results relating behaviour on $np^r$ cells to that on $np^{r+j}$ cells, where integer $n > 0$ is coprime to $p$ and $r, j \in \mathbb{N}$ and of course all the material relating to time independent inputs.

In theorem 4.3.1 we show that the condition of theorem 2.3.3 is satisfied when the state alphabet is a finite field and that in this case there are at most $r + 2$ possible qualitatively distinct behaviours available to the system with time independent inputs on $np^r$ cells where $n$ is coprime to $p$.

In section 4.4 a notion of qualitative dynamical similarity for distinct linear rules on $N$ cells is introduced and discussed, some results are obtained, this is an interesting area for further research. In section 4.5 the direct product decomposition is rewritten in terms of idempotent elements in preparation for chapter 5.

In chapter 5 linear cellular automata with periodic boundary conditions and state alphabet the integers modulo $m$ for any positive integer $m > 1$ are considered. In fact

we focus almost entirely on the case $m = p^k$, $p$ prime and $k > 1$ as this case together with the case of $R = \mathbb{F}_p$ suffices to describe the more general case. No results were previously available for $R = \mathbb{Z}_{/p^k}$ (or equivalently $\mathbb{Z}/p^k\mathbb{Z}$) with $k > 1$.

We are able to extend and utilise results from the finite field case ($k = 1$ being a special case of the finite field case as $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$) by the technique of idempotent lifting, beginning in section 5.1 with the direct product decomposition of $R_N$ in the present case. The rest of section 5.1 is devoted to examining the relationships between the relevant rings in the $np^r$ and $np^{r-j}$ cases, $n$ coprime to $p$ and $r > j > 0$, and for different values of $k$.

Section 5.2 is devoted to discussing the dynamics in a single ring in the direct product decomposition of $R_N$ in the zero input case and section 5.3 is devoted to discussing the dynamics in a single ring in the direct product decomposition of $R_N$ in the non-zero input case. For reasons of space only results concerning periodic behaviour are discussed in this chapter. When the number of cells is not coprime to $p$ the results in these sections are not as complete as the equivalent results in the finite field case, this is due to the more complicated structure of the maximal ideal of nilpotent elements in this case.

In section 5.4 the results from previous sections are combined to give results for linear cellular automata with periodic boundary conditions, again these results are not as complete as those for the finite field case and this is another area for future research.

In section 5.5 the general case of $R$ equal to the integers modulo $m$, $m$ any integer greater than 1, is discussed briefly as well as some other straightforward generalisations from the results of chapters 3, 4 and 5. In particular we prove two results, both because of their importance and as an example of how the results from the finite field cases and the $\mathbb{Z}/p^k\mathbb{Z}$ case make the $\mathbb{Z}/m\mathbb{Z}$ case easy for composite $m$, firstly that linear cellular with state alphabet the integers modulo $m$, time independent inputs and periodic boundary conditions on $N > 1$ cells cannot generate cycles of length $m^N$ and secondly that such cellular automata satisfy the condition of theorem 2.3.3.

In chapter 6 two generalisation are briefly discussed. In section 6.1 we consider time dependent inputs which are themselves periodic and show that results for the periodic behaviour of such systems can be derived from the time independent input case. In section 6.2 the extension of our techniques to two or more dimensions is discussed, this section is a preliminary investigation and this is another area for further research. Appendix A is a review of some of the algebra used in this thesis (and is referred to

in several places in the main text). Appendix B contains the proofs of various results which were omitted from the main text for reasons of space.

## 1.1 The definition of a cellular automata

We shall be concerned with cellular automata on regular lattices, where by a regular lattice $\mathcal{L}$ we mean a regular array of sites (or cells) in one or more dimensions. We shall assume in this section that $\mathcal{L}$ is infinite. We shall follow Toffoli and Margolus [7] in our general definition of a cellular automata. To each site in $\mathcal{L}$ one can assign a state from a state alphabet $A$, a finite set, which we assume contains an element 0. Each assignment of an element of $A$ to each site of $\mathcal{L}$ is called a configuration of $A$ on $\mathcal{L}$. Thus the set of configurations of $A$ on $\mathcal{L}$, denoted by $Q$, is the Cartesian product of copies of $A$ indexed by $\mathcal{L}$:

$$Q = A^{\mathcal{L}}.$$

The configuration where each site has state zero is sometimes known as the quiescent state. Let $S$ be the abelian group of translations of $\mathcal{L}$ onto itself. For instance when (as it usually will be in this document) $\mathcal{L}$ is an $n$-dimensional integer lattice (*i.e.* an array of equally spaced points in $n$-dimensions, often called an $n$-dimensional square lattice), then

$$S = \mathbb{Z}^n.$$

(In fact in this case we can identify $\mathcal{L}$ with $\mathbb{Z}^n$ as $\mathcal{L}$ is naturally indexed by $\mathbb{Z}^n$).

The elements of $S$ will be called displacements. The action of a displacement $s \in S$ on a site $i \in \mathcal{L}$ yields a new site $s + i$. A neighbourhood is a finite set of displacements, one applies a neighbourhood $X$ as an operator to a site $i$ to yield a set of sites. the $X$-neighbourhood of $i$, formally

$$i + X = \{i + x : x \in X\}.$$

$y \in i + X$ is called a neighbour of $i$. The size of $X$ is the number of elements in $X$, $|X|$. The radius of $X$ is the length of the longest displacement.

Let $q \in Q$, then the $i - th$ component of $q$ is the state of site $i$ in $q$, denoted $q_i$. The neighbourhood projection operator $[i + X]$ extracts from $q$ the collection of states of the neighbours of $i$:

$$[i + X](q) \in A^X.$$

Thus for each $i$, $[i+X]$ may be thought of as a map $Q \longrightarrow A^X$.

**Example 1.1.1**

Let $\mathcal{L} = \mathbb{Z}$, (the one dimensional integer lattice) let $X = \{-1, 0, 1\} \subset \mathbb{Z}$, so $X$ has radius 1. Arbitrarily choosing a site as origin (*i.e.* to have index zero), let $q$ be the configuration

$$q = \ldots q_{-3}q_{-2}q_{-1}q_0q_1q_2q_3 \ldots \in A^{\mathbb{Z}}.$$

Then

$$\begin{aligned} [0+X](q) &= (q_{-1}, q_0, q_1) \\ [-2+X](q) &= (q_{-3}, q_{-2}, q_{-1}) \end{aligned}$$

and in general

$$[i+X](q) = (q_{i-1}, q_i, q_{i+1}). \quad \blacklozenge$$

**Example 1.1.2**

Let $\mathcal{L} = \mathbb{Z}^2$, the two dimensional square lattice. The Von Neumann neighbourhood $X = V$ is

$$V = \{(0,0), (1,0), (0,1), (-1,0), (0,-1)\} \subset \mathbb{Z}^2.$$

Then for the site $i$ with coordinates $(I, J)$ relative to an arbitrarily chosen origin in the lattice and any $q \in A^{\mathbb{Z}^2}$ we have

$$[i+V](q) = (q_{(I,J)}, q_{(I+1,J)}, q_{(I,J+1)}, q_{(I-1,J)}, q_{(I,J-1)})$$

where $q_{(x,y)}$ denotes the state of the site with coordinates $(x, y)$ in configuration $q$. Note that $V$ has radius 1. Another two dimensional neighbourhood with radius 1 is the Moore neighbourhood $M$

$$M = V \cup \{(1,1), (-1,1), (-1,-1), (1,-1)\} \subset \mathbb{Z}^2. \quad \blacklozenge$$

Let $f$ be a mapping,

$$f : A^X \longrightarrow A,$$

then $f$ can be applied at each site $i$ of configuration $q$ to yield a new configuration $q'$:

$$q_i' = f([i+X](q)). \tag{1.1.1}$$

Formally the map $f$ is known as the rule table and the pair $(X, f)$ is the local rule. We shall consistently abuse this terminology and refer to $f$ as the local rule. The radius of the local rule is the radius of $X$. The local rule induces a global map $F$, often called the global rule,

$$F : Q \longrightarrow Q$$

via equation (1.1.1). We can now define a cellular automata formally.

**Definition 1.1.1** *A cellular automata is a 4-tuple $(\mathcal{L}, A, X, f)$ where the finite set $A$ is the state alphabet, $f$ is a rule table, $\mathcal{L}$ is a regular lattice and $X$ is a neighbourhood.*

The definition 1.1.1 is somewhat cumbersome and we shall often just refer to the cellular automata by the local rule $f$ or the global rule $F$. We shall some times refer to a cellular automata with state alphabet $A$ as a cellular automata over $A$. A cellular automata is said to satisfy the quiescence condition if its local rule $f$ satisfies

$$f(0, \ldots, 0) = 0.$$

An important feature of cellular automata is that they commute with the translations of the lattice $\mathcal{L}$, that is, if $s \in S$ and $q \in Q$ then if $F$ is the global rule of a cellular automata then

$$F(s(q)) = s(F(q)),$$

where $s$ acts on $q$ by $q_i \mapsto q_{s+i}$.

If $f$ is the map $A^X \longrightarrow \{0\}$ then we shall call $f$ the *trivial rule* or *zero rule*, if $f$ is such that some iterate $t$ of $f$ (*i.e.* the $t-th$ composition of $f$ with itself, $f \circ \ldots \circ f$. $t$ times) is the trival rule we shall call $f$ a *nilpotent* rule.

**Example 1.1.3**

In example 1.1.1 take $A = \mathbb{F}_2$, the finite field with two elements ($\mathbb{F}_2 = \{0, 1\}$). Then any map $f : \mathbb{F}_2^X \longrightarrow \mathbb{F}_2$ is the local rule of a so-called *elementary* cellular automata $(\mathbb{Z}, \mathbb{F}_2, X, f)$. The title elementary refers to the fact that this is the simplest form of cellular automata, in that it has radius 1 and a non-trivial state alphabet of minimal size. For instance the cellular automata with local rule given by

$$f(a_{-1}, a_0, a_1) = a_{-1} + a_1,$$

where $a_{-1}, a_0, a_1$ are any elements of $\mathbb{F}_2$ and the addition on the right hand side is the addition in $\mathbb{F}_2$, is an elementary cellular automata, denoted as rule 90 in the labelling scheme for elementary cellular automata introduced by Wolfram [8]. It is clear that rule 90 satisfies the quiescence condition. Rule 90 is often taken as a typical example of a linear cellular automata rule and has been extensively studied (for instance [3], [9], [10], [11] and [12]). ♦

The time evolution of a cellular automata is defined at the local level by

$$q_i^{t+1} = f([i + X](q^t)) \tag{1.1.2}$$

where $q^t$ is the configuration at time $t$ in the evolution from some initial condition $q = q^0$ and $q_i^t$ is the state of the $i - th$ site at time $t$ in the evolution. At the global level we have

$$q^{t+1} = F(q^t). \tag{1.1.3}$$

We shall write $F^k(q)$ for the $k - th$ iterate of the global rule $F$ for initial configuration $q \in Q$. We define the orbit of $q \in Q$ under the cellular automata as follows:

**Definition 1.1.2** *Let $q \in Q$, then the (forward) orbit of $q$ under the cellular automata $(\mathcal{L}, A, X, f)$ is*

$$O(q) = \{F^i(q) : i \in \mathbb{N}\}$$

*where $F$ is the global map induced by $f$. Similarly the backward orbit of $q$ is*

$$O^-(q) = \{p : p \in A^{\mathcal{L}}, F^i(p) = q, \text{ some } i \in \mathbb{N}\}.$$

A predecessor of a configuration $q \in Q$ under a cellular automata is another configuration $p \in Q$ such that $F(p) = q$. A given configuration $q$ may have more than one predecessor, or it may have none. In the latter case $q$ is known as a "Garden of Eden" state, such configurations were first considered by Moore [13]. If every configuration has a unique predecessor then the cellular automata is said to be *invertible* or *reversible*, we shall say more about reversibility at the end of this section.

We now turn our attention to the reoccurrence of a configuration under a cellular automata.

**Definition 1.1.3** *The configuration $q \in Q$ is eventually periodic with period $k \geq 1$ under the cellular automata $(\mathcal{L}, A, X, f)$ if there is an integer $T \geq 0$ such that*

$$F^{T+k}(q) = F^T(q).$$

*If* $T = 0$ *then say* $q$ *is periodic.*

When a configuration $q$ is eventually periodic (periodic) we say that the orbit of $q$ is eventually periodic (periodic). In this case if $k$ is the least positive integer satisfying definition 1.1.3 we shall say that $q$ evolves to a cycle of length $k$ under the cellular automata, and that $F^T(q)$ has prime period $k$. Thus a cycle is the (forward) orbit of a periodic configuration. From now on orbit should be taken to mean forward orbit unless specified otherwise.

A cellular automata is said to be *globally injective* if its global rule is injective. Formally a cellular automata with global rule $F$ is said to be reversible if there is another cellular automata with global rule $F'$ such that for any pair of configurations $c$ and $c'$, $F(c) = c'$ if and only if $F'(c') = c$. Richardson [14] showed that a cellular automata is globally injective if and only if it is reversible. Culik II *et.al.* [15] have shown that for a one dimensional cellular automata the global map $F$ is injective if and only if it is injective on all spatially periodic configurations.

## 1.2 Boundary conditions and finite cellular automata in one dimension

The cellular automata we have been considering so far have been infinite cellular automata, however this thesis is mainly concerned with finite cellular automata, these can be obtained from infinite cellular automata by imposing boundary conditions. In the one dimensional case we shall be considering two types of boundary conditions, fixed value boundary conditions and periodic boundary conditions. In the first case the states of all but a finite number $N$ of consecutive sites are fixed. Usually the sites with fixed states are all assumed to be in the zero state, this is the case of null or Dirichlet boundary conditions.

**Example 1.2.1**

Let $f$ be the local rule of an elementary cellular automata (as defined in example 1.1.3). Let $N$ be a strictly positive integer, let the states of the sites $\ldots, -2, -1, N, N+1, \ldots$ be held at 0, so that a configuration $q$ can only have non-zero values at sites $0, 1, \ldots, N-1$. Then the result of applying the global rule $F$ is

$$\begin{array}{cccccccc} \ldots & 0 & q_0 & q_1 & \ldots & q_{N-1} & 0 & \ldots \\ & & & & \downarrow F & & & \\ \ldots & 0 & f(0,q_0,q_1) & f(q_0,q_1,q_2) & \ldots & f(q_{N-2},q_{N-1},0) & 0 & \ldots \end{array} \quad \blacklozenge$$

In practice, for any fixed value boundary conditions and a one dimensional cellular automata rule of radius $r$, it is only necessary to specify the values of the sites $-r, \ldots, -1, N, \ldots, N+r-1$, as the values of other sites can have no affect on the evolution of the $N$ sites whose states are not fixed. We shall see in section 1.5 that a one dimensional cellular automata with any fixed value boundary conditions is equivalent to the same one dimensional cellular automata with null boundary conditions and a constant external input a each time step.

The second type of boundary conditions we shall be using in one dimension are periodic boundary conditions. Additive cellular automata with periodic boundary conditions in more than one dimension are discussed in chapter 6. In one dimension, with the sites indexed by $\mathbb{Z}$ one chooses $N$ sites indexed $0, 1, \ldots, N-1$. Then site $N$ is identified with site 0, site $N+1$ is identified with site 1 *etc.* and site $-1$ is identified with site $N-1$, site $-2$ is identified with site $N-2$ *etc.* Thus, with $0 \leq i \leq N-1$, we have for a configuration $q$ of a cellular automata with these boundary conditions

$$\begin{aligned} q_{i+N} &= q_i \\ q_{-i} &= q_{N-i} \end{aligned} \tag{1.2.1}$$

One can think of the sites of a cellular automata with these boundary conditions as being arranged on a circle or cylinder (such cellular automata are sometimes called cylindrical cellular automata). Alternatively one can think of this system as being the infinite system but with the configurations $q$ restricted to those that consist of infinite repetitions of the same block of $N$ sites. Thus the study of finite cellular automata with periodic boundary conditions is equivalent to the study of the action of infinite cellular automata on configurations consisting of infinite repetitions of a finite configuration. The result of Culik II *et.al.* mentioned at the end of the previous section can thus be restated as: a one dimensional cellular automata is reversible if and only if the corresponding cellular automata on $N$ cells with periodic boundary configurations is reversible for all $N > 0$.

**Example 1.2.2**

Let $f$ be the local rule of an elementary cellular automata (as defined in example 1.1.3). Let $N$ be a strictly positive integer, then with periodic boundary conditions on $N$ cells, a configuration $q$ consists of $N$ elements of $A$, $q_0, q_1, \ldots, q_{N-1}$, and the action of the

global rule $F$ is

$$\begin{array}{ccccccc} q_0 & & q_1 & \cdots & q_{N-2} & q_{N-1} & \\ & & & \downarrow F & & & \\ f(q_{N-1},q_0,q_1) & f(q_0,q_1,q_2) & \cdots & f(q_{N-3},q_{N-2},q_{N-1}) & f(q_{N-2},q_{N-1},q_0) & \blacklozenge \end{array}$$

Orbits, periodic configurations, cycles *etc.* are defined as in the infinite case. Because for finite cellular automata the number of configurations is finite all configurations are eventually periodic. The configurations of a finite cellular automata on $N$ cells can always be thought of as the elements of $A^N$.

## 1.3 Hybrid cellular automata

Let $\mathcal{L}$ be a regular lattice, as in section 1.1, let $\mathcal{X}$ be a family of neighbourhoods indexed by $\mathcal{L}$ and let $\mathcal{F}$ be a family of rule tables indexed by $\mathcal{L}$. Then for each $i$, with $X_i \in \mathcal{X}$, $\mathfrak{f}_i \in \mathcal{F}$,

$$\mathfrak{f}_i : A^{X_i} \longrightarrow A.$$

Let $q \in Q$, then the $i-th$ neighbourhood projection operator $[i + X_i]$ acts at site $i$, $[i + X_i](q) \in A^{X_i}$. $\mathcal{X}$ and $\mathcal{F}$ can be applied to a configuration $q$ to yield a new configuration $q'$ via

$$q_i' = \mathfrak{f}_i([i + X_i](q)). \tag{1.3.1}$$

Thus $\mathcal{X}$ and $\mathcal{F}$ induce a global rule $\mathfrak{F}$ as $X$ and $f$ did in section 1.1 and we can formally define a hybrid cellular automata:

**Definition 1.3.1** *A hybrid cellular automata is a 4-tuple $(\mathcal{L}, A, \mathcal{X}, \mathcal{F})$ where $\mathcal{L}$ is a regular lattice, $A$ is the state alphabet, $\mathcal{X}$ is a family of neighbourhoods indexed by $\mathcal{L}$ and $\mathcal{F}$ is a family of rule tables indexed by $\mathcal{L}$.*

We shall usually refer to $\mathcal{F}$ as the set of local rules, intuitively the system defined above is that obtained by using local rule $\mathfrak{f}_i$ at site $i$ at each time step.

**Example 1.3.1**

Let $\mathcal{L} = \mathbb{Z}$ and $A = \mathbb{F}_2$. Let $\mathcal{X}$ be such that $X_i = X = (-1, 0, 1)$ for each $i$. In $\mathcal{F}$ let

$$\begin{array}{rcll} \mathfrak{f}_i(q_{i-1}, q_i, q_{i+1}) & = & q_{i-1} + q_{i+1}, & i \text{ even} \\ \mathfrak{f}_i(q_{i-1}, q_i, q_{i+1}) & = & (q_{i-1} + q_{i+1})q_i & i \text{ odd.} \end{array}$$

Then $(\mathcal{L}, \mathbb{F}_2, \mathcal{X}, \mathcal{F})$ is a hybrid cellular automata. $\blacklozenge$

Periodic configurations *etc.* are defined just as for ordinary cellular automata. Finite hybrid cellular automata are obtained by applying boundary conditions just as for cellular automata.

**Example 1.3.2**

Consider example 1.3.1 with periodic boundary conditions and $N$ even. One has

$$\begin{array}{ccccccc} q_0 & & q_1 & & \cdots & q_{N-2} & q_{N-1} \\ & & & & \downarrow \mathfrak{F} & & \\ q_{N-1}+q_1 & & (q_0+q_2)q_1 & & \cdots \quad q_{N-3}+q_{N-1} & & (q_{N-2}+q_0)q_{N-1} \end{array} \quad \blacklozenge$$

It is clear that, in general, hybrid cellular automata do not commute with the translations of $\mathcal{L}$.

## 1.4 State transition graphs and cycle sets

### 1.4.1 The state transition graph of a cellular automata

The *state transition graph* of a cellular automata (especially a finite cellular automata) is a useful tool for visualising the dynamical structure of the system. A *graph* $\Gamma$ is a pair of sets $V(\Gamma), E(\Gamma)$, where $V(\Gamma)$ is the set of *vertices* of $\Gamma$ and $E$ is the set of *edges* of $\Gamma$. To each element $e$ of $E(\Gamma)$ two points of $V(\Gamma)$ are associated, the endpoints of $e$. The end points need not be distinct, if they are not distinct $e$ is said to be a *loop*. Two vertices are said to be *adjacent* if they are joined by an edge.

If the endpoints of each $e \in E(\Gamma)$ form an ordered pair $(v_1, v_2)$ then $\Gamma$ is called a *directed graph* or *digraph*, $e$ is called a directed edge. and can be thought of as an arrow from $v_1$ to $v_2$. We can now define the state transition graph of a cellular automata with global rule $F$ whether finite or infinite. The same definition applies for hybrid cellular automata.

**Definition 1.4.1** *The state transition graph* $\Gamma(F)$ *of the cellular automata with global rule* $F$ *is the directed graph with* $V(\Gamma) = A^{\mathcal{L}}$ *(or* $V(\Gamma) = A^N$ *for a finite cellular automata on* $N$ *cells) and a directed edge from vertex* $p$ *to a vertex* $q$ *if and only if* $F(p) = q$.

Thus fixed points (cycles of length one) of a cellular automata correspond to loops in the state transition graph. A graph is finite if both $V(\Gamma)$ and $E(\Gamma)$ are finite, thus the state transition graph of a finite cellular automata is finite.

Given a vertex $v \in V(\Gamma)$ of a digraph $\Gamma$, the *out-degree* of $v$ is the number of directed edges $(v, u)$ in $E(\Gamma)$ and the *in-degree* of $v$ is the number of directed edges $(u, v)$ in $E(\Gamma)$. Clearly if $\Gamma(F)$ is the state transition graph of a cellular automata then the out-degree of every vertex $v$ is 1, if in addition the in-degree of every vertex is 1 then the cellular automata must be reversible.

A *path* is a sequence of vertices $v_0, \ldots, v_m$, such that there is a directed edge $(v_i, v_{i+1})$ for $0 \leq i \leq m-1$ and each $v_i$ is distinct apart from possibly $v_0 = v_m$, in which case the path is called a *circuit*. Clearly a path $v_0, \ldots, v_m$ in the state transition graph of a cellular automata corresponds to a portion of the forward orbit of $v_0$ under the cellular automata and a circuit $v_0, \ldots, v_m$ corresponds to a cycle of length $m+1$. We shall abuse notation and refer to circuits in the state transition graph of a cellular automata as cycles. If every vertex $v$ in the state transition graph of a cellular automata is on a cycle then clearly the cellular automata is reversible.

A *subgraph* of a graph or digraph $\Gamma$ is a graph or digraph $\gamma$ such that $V(\gamma) \subseteq V(\Gamma)$ and $E(\gamma) \subseteq E(\Gamma)$. A graph is said to be *connected* if there is a path between every pair of vertices, we shall say that a digraph is connected if it is connected as a graph. A graph or digraph that contains no circuits and is connected is called a *tree*. The state transition graph of finite cellular automata irreversible on $N$ cells is characterised by the presence of trees joining the main graph at elements of cycles (one says that such a tree is *rooted* at the element of the cycle).

The *height* of a tree is the maximum number of vertices visited on any path starting at a vertex in the tree and terminating at the element of a cycle that the tree is rooted to, this corresponds to the maximum possible number of time steps taken for a configuration of the cellular automata to reach a cycle. A vertex in a tree is said to be at height $t$ if $t$ is the minimum number of vertices visited by any path from that vertex to the element of the cycle at which the tree is rooted. In fact, as the out-degree of every vertex in the state transition graph of a cellular automata is 1 and the graph is directed, there is only one possible path from a vertex in a tree to the element of the cycle that the tree is rooted to. A vertex with in-degree zero will sometimes be referred to as a leaf, such a vertex corresponds to a Garden of Eden configuration in the state transition graph of a cellular automata. See figures 1.1 and 1.2 for examples of a state transition graph.

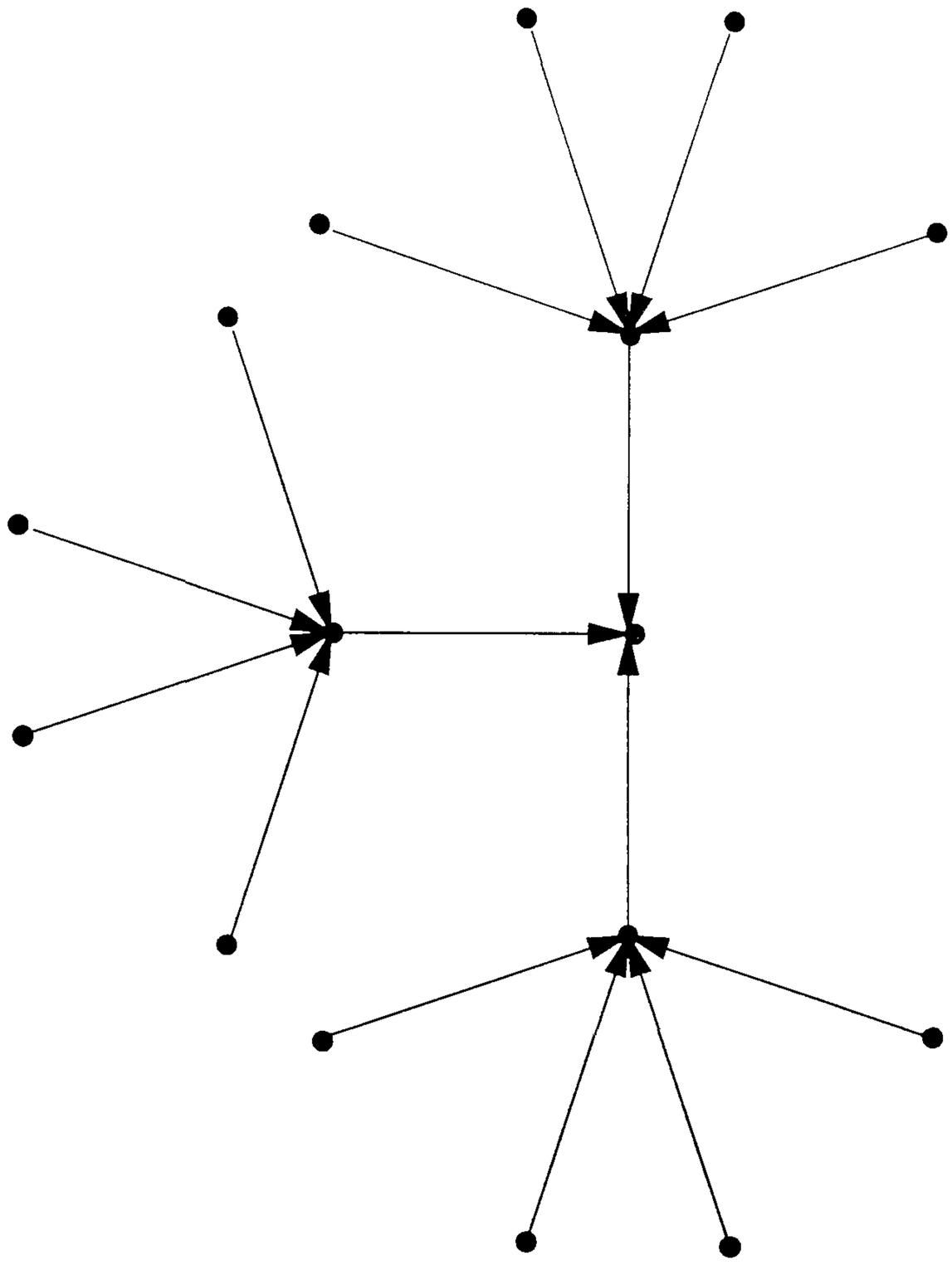

Figure 1.1: The state transition graph of rule 90 on 4 cells with periodic boundary conditions, in this case the state transition graph consists of a single tree rooted at 0.

### 1.4.2 Cycle sets

Cycle sets provide a convenient qualitative description of the cycle structure of a finite cellular automata (*i.e.* how many cycles of what lengths). The notion of a cycle set is borrowed from the theory of linear modular systems (for instance see [16]).

**Definition 1.4.2** *Let $F$ be the global rule of some finite cellular automata and suppose that under $F$ there are $n_i$ distinct cycles of length $\phi_i$, $1 \leq i \leq k$, for some positive integers $n_i, \phi_i$ and $k$. Then the* cycle set *of $F$ is*

$$\Sigma(F) = \{n_1[\phi_1], \ldots, n_k[\phi_k]\}.$$

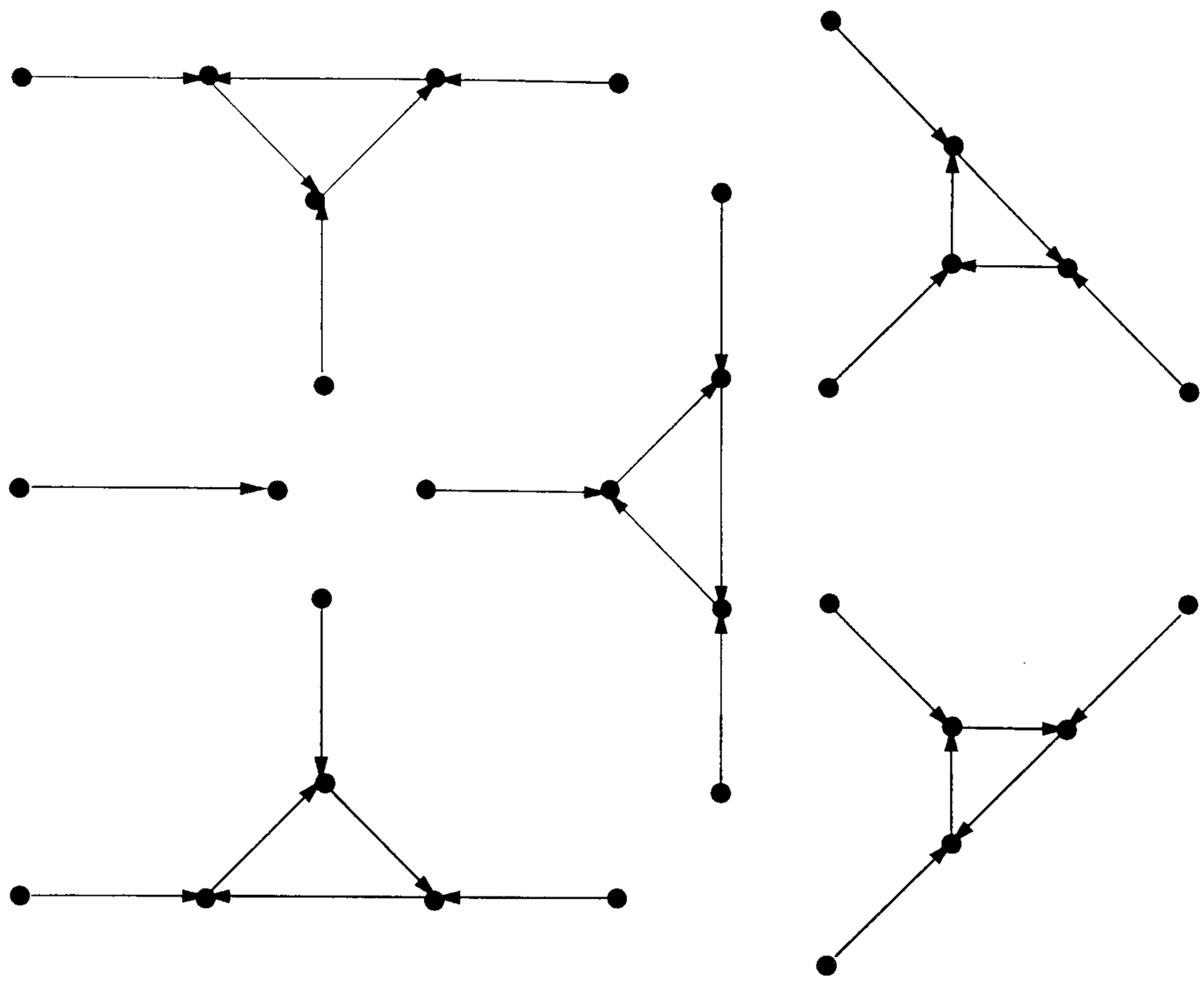

Figure 1.2: The state transition graph of rule 90 on 5 cells with periodic boundary conditions, in this case the state transition graph consists of a fixed point at 0 and 5 cycles of length 3, with a very simple tree rooted at all the vertices on cycles.

Each expression $n_i[\phi_i]$ is known as a *cycle term.* There is a product of cycle sets, we first define the product of two cycle terms by

$$n[\phi].m[\Gamma] = nm\mathrm{gcd}(\phi,\Gamma)[\mathrm{lcm}(\phi,\Gamma)].$$

The product of two cycle sets is then defined by

$$\begin{aligned}\Sigma(F).\Sigma(G) &= \{n_1[\phi_1],\ldots,n_k[\phi_k]\}.\{m_1[\Gamma_1],\ldots,m_l[\Gamma_l]\} \\ &= \cup_{i=1}^{k}\cup_{j=1}^{l}\{n_i[\phi_i].m_j[\Gamma_j]\}. \qquad (1.4.1)\end{aligned}$$

It is often convenient to write cycle sets as formal sums

$$\Sigma(F) = \sum_{i=1}^{l} n_i[\phi_i],$$

the product is then defined by

$$\Sigma(F).\Sigma(G) = \sum_{i=1}^{l}\sum_{j=1}^{k} n_i[\phi_i].m_j[\Gamma_j].$$

The sum can be simplified where two cycle terms $n[\phi]$ and $m[\Gamma]$ are such that $\phi = \Gamma$, one just defines

$$n[\phi] + m[\phi] = (n + m)[\phi].$$

One can consider the set of cycle sets as a ring, which we shall denote by $C(\mathbb{Z})$, with zero element $0[1]$ and identity $1[1]$. Additively $C(\mathbb{Z})$ is isomorphic to $\mathbb{Z}[x]$, via

$$\sum_{i=1}^{l} n_i[\phi_i] \mapsto \sum_{i=1}^{l} n_i x^{\phi_i - 1},$$

however the multiplicative structure is different from that of $\mathbb{Z}[x]$. We note that $C(\mathbb{Z})$ is not an integral domain, for instance

$$(-2[3] + 1[6])1[4] = 0.$$

## 1.5 Finite linear cellular automata

### 1.5.1 A brief review of the finite linear cellular automata literature

We give a brief overview of the literature relating to finite linear cellular automata, the reader looking for sources on more general cellular automata should consult, for instance, [17] and [18] and the references therein. A possible source of confusion that should be noted is that some authors use the term linear to mean one dimensional. The majority of the work that has been done on linear cellular automata has been for the infinite case, which we do not discuss here. As far as we are aware there has been no attempt made to study linear cellular automata in the presence of time independent inputs prior to this thesis.

The most referenced paper on finite additive cellular automata is that by Martin *et.al* [3] from 1984, which concentrates mainly on periodic boundary conditions. They derive results about the structure of the state transition diagram of a linear cellular automata in terms of algebraic and number theoretical quantities. The results they obtained were mostly for state alphabet $\mathbb{F}_p$, the finite field with $p$ elements, and one dimensional cellular automata, however they do briefly discuss the higher dimensional case and the case of state alphabet $\mathbb{Z}_{/m}$, $m$ a composite integer but they were unable to provide any results for state alphabet $\mathbb{Z}_{/p^k}$, $p$ prime and $k > 1$. We discuss some of their results in detail in section 1.5.5.

Linear cellular automata with periodic boundary conditions and state alphabet a finite field were studied by Jen in [19], concentrating on the occurrence of shifts and the

relation of spatial periodicity in configurations of the cellular automata to their temporal periodicity, the method involved application of the theory of recurring sequences over finite fields. A polynomial method for studying rule 90 (see example 1.1.3) with null boundary conditions was introduced by Nohmi in [20] and extended by Kawahara *et.al.*, in [21], to two dimensions, and by Kawahara and Lee [22] to a higher order form of rule 90. These authors obtained strong results but in very specific cases and only for null boundary conditions.

Voorhees [23] used a complex polynomial representation to study the injectivity of one dimensional cellular automata with periodic boundary conditions, motivated by relation between between injectivity with periodic boundary conditions and in the infinite case. The results obtained were primarily for state alphabet $\mathbb{F}_2$. Vivaldi [24] studied one dimensional cellular automata with periodic boundary conditions and state alphabet a finite field in general, not just linear cellular automata, employing a polynomial method based on the functional completeness of finite fields, that is the fact that any function on $\mathbb{F}_{p^q}$ can be represented by a unique polynomial (see [25], page 100) and hence any rule table can be so expressed. A connection with algebraic dynamics was established. In Vivaldi's method linear cellular automata are represented by linearised polynomials (see [26], chapter 3).

The most well known paper using a matrix representation of additive cellular automata is that by Guan and He [27] where cellular automata over finite fields with periodic boundary conditions were represented by means of circulant matrices. The approach was that of decomposing a finite dimensional vector space representing the possible configurations of the cellular automata, into subspaces invariant under a particular linear map (the circulant matrix representing the cellular automata). They obtained results in one and higher dimensions and for higher order cellular automata, including an algorithm for finding the cycle set (though they do not use that terminology) based on determining the Jordan form of the matrix representing the rule. More recently Tadakis and Matsufuji [10] considered rule 90 with null boundary conditions and state alphabet $\mathbb{F}_2$ using a matrix representation, as did Stevens *et.al.* [12]. Tadikis [9] considered rules 90 and 150, again with null boundary conditions and state alphabet $\mathbb{F}_2$, and again in 1994 but with periodic boundary conditions [11] and also with some discussion of hybrids of rules 90 and 150. All of these papers used eigenvalue analysis on the matrix representing the rule and all were rather specific.

One of the motivations for the studies by the authors mentioned in the previous

paragraph is recent interest in the use of cellular automata and hybrid cellular automata in very large scale integrated circuits, in particular as pseudorandom number generators, see the papers by Compagner and Hoogland [4], Hortensius *et.al.* [5] and Preis *et.al.* [6]. This interest is focused mainly on the occurrence of cycles of maximal possible length.

Finally Jen [1] showed in 1990 that certain nonlinear cellular automata, with periodic boundary conditions, can be mapped onto linear cellular automata and thus results from the additive case can be utilised in the nonlinear case. In 1993 Bartlett and Garzon [2] showed that a class of nonlinear cellular automata, the monomial cellular automata, are in certain cases closely related to additive cellular automata. Though the work of Bartlett and Garzon was for the infinite case their idea should still work in the finite case.

### 1.5.2 Matrix representation of finite linear cellular automata

One dimensional linear cellular automata have linear local rules of the form

$$\begin{aligned} a_i^{t+1} &= f(a_{i-l}^t, \ldots, a_i^t, \ldots, a_{i+l}^t) \\ &= \alpha_{-l} a_{i-l}^t + \ldots + \alpha_0 a_i^t + \ldots + \alpha_l a_{i+l}^t \end{aligned} \tag{1.5.1}$$

where $l$ is a positive integer, the radius of the rule, and the states $a_i$ and rule coefficients $\alpha_j, -l \leq j \leq l$, are elements of a state alphabet $R$ and $a_i^t$ is the state of the $i-th$ cell at time $t$. We shall assume that $R$ is a finite commutative ring, for instance $\mathbb{Z}_{/m}$ the ring of integers modulo $m$, where $m > 0$ is an integer, or a finite field $\mathbb{F}_{p^q}$ where $p > 0$ is a prime integer and $q \in \mathbb{Z}, q > 0$. Linear local rules satisfy the quiescence condition. We shall sometimes use a shorthand notation for the local rule and write, instead of (1.5.1),

$$f : a_i \mapsto \alpha_{-l} a_{i-l} + \ldots + \alpha_l a_{i+l}.$$

**Example 1.5.1**

$R = \mathbb{F}_2$ and the elementary cellular automata rule 90.

$$f(a_{i-1}, a_i, a_{i+1}) = a_{i-1} + a_{i+1}. \quad \blacklozenge$$

**Example 1.5.2**

$R = \mathbb{Z}_{/4}$, then the radius 3 local rule defined below is a linear rule.

$$f(a_{i-3}, a_{i-2}, a_{i-1}, a_i, a_{i+1}, a_{i+2}, a_{i+3}) = 2(a_{i-3} + a_{i+3}) + 3(a_{i-2} + a_{i+2}) + a_i. \quad \blacklozenge$$

We shall be concerned with finite cellular automata on $N$ cells with either periodic or fixed value boundary conditions. Thus any collection of $N$ elements of $R$, indexed from 0 to $N-1$, can be thought of as a state of the system, such a collection can also be thought of as an element of the $R$-module $R^N$. The local rule $f$ induces a global rule $F_N$ on $N$ cells which gives the global dynamics;

$$\begin{aligned} F_N &: R^N \longrightarrow R^N \\ s^{t+1} &= F_N(s^t) \end{aligned} \tag{1.5.2}$$

where $s^t \in R^N$ is the (global) state of the system at time $t$. When $F_N$ is a bijection we say that the global rule is reversible (or invertible) and that the cellular automata is reversible for $N$ cells.

The linearity of the local rule implies that the global rule is additive, that is

$$F_N(P+Q) = F_N(P) + F_N(Q) \tag{1.5.3}$$

for each $N$ and any $P, Q \in R^N$. Consequently, such cellular automata rules are often called additive, and we shall use that name. Further, such global rules map the state where every cell has state 0 to the same state, *i.e.* they satisfy the quiescence condition,

$$F_N(0) = 0.$$

We shall represent a state $a \in R^N$ by a column vector

$$\mathbf{a} = (a_0, a_1, \ldots, a_{N-1})^T.$$

For null or periodic boundary conditions we can represent the global rule by an $N \times N$ matrix $\mathbf{T}$ with entries in $R$. For null boundary conditions, and the linear local rule (1.5.1), this matrix is defined by

$$\{\mathbf{T}\}_{ij} = \alpha_{j-i}, \tag{1.5.4}$$

where $\alpha_{-l-k} = \alpha_{l+k} = 0$ for each $k \in \mathbb{N}_{>0}$. For periodic boundary conditions one has

$$\{\mathbf{T}\}_{i((i+j) \bmod N)} = \alpha_j, \ -l \leq j \leq l \tag{1.5.5}$$

and all other entries zero (we shall introduce another representation of additive cellular automata with periodic boundary conditions in the next section and use that

representation throughout this thesis, the matrix representation is described here for completeness). In either case the global cellular automata dynamics is given by

$$\left.\begin{array}{rcl} \mathbb{T}: R^N & \longrightarrow & R^N \\ \mathbf{a} & \mapsto & \mathbf{T}\mathbf{a} \\ \mathbf{a}^{t+1} & = & \mathbb{T}(\mathbf{a}^t) \end{array}\right\} \tag{1.5.6}$$

$\mathbb{T}$ is a module endomorphism of $R^N$.

Now consider a hybrid of linear rules on $N$ cells, with a local linear rule $\mathfrak{f}_i$ acting at site $i$ with radius $l(i)$,

$$\mathfrak{f}_i(a_{i-l(i)}, \ldots, a_{i+l(i)}) = \sum_{j=-l(i)}^{l(i)} \alpha_{i,j} a_{i+j}. \tag{1.5.7}$$

The global rule of such a hybrid can still be represented by an $N \times N$ matrix $\mathfrak{T}$. For null boundary conditions this matrix is defined by

$$\{\mathfrak{T}\}_{i(i+j)} = \alpha_{i,j},\ 0 \leq i+j \leq N-1, \tag{1.5.8}$$

and all other entries zero. For periodic boundary conditions we have

$$\{\mathfrak{T}\}_{i((i+j) \bmod N)} = \alpha_{i,j}. \tag{1.5.9}$$

Then in either case the global hybrid cellular automata dynamics are given by

$$\left.\begin{array}{rcl} \mathfrak{T}: R^N & \longrightarrow & R^N \\ \mathbf{a} & \mapsto & \mathfrak{T}\mathbf{a} \\ \mathbf{a}^{t+1} & = & \mathfrak{T}(\mathbf{a}^t) \end{array}\right\} \tag{1.5.10}$$

For fixed boundary conditions other than null and a linear local rule of radius $l$ (or a hybrid of linear local rules with maximum radius $l$), suppose the boundary sites $-1, \ldots, -l$ and $N, \ldots, N+l-1$ have the fixed values $a_{-1}, \ldots, a_{-l}$ and $a_N, \ldots, a_{N+l-1}$. Then if the matrix representing the global rule for null boundary conditions is $\mathbf{T}$ (or $\mathfrak{T}$ for a hybrid) then the global dynamics are given by

$$\left.\begin{array}{rcl} \mathbb{T}_{\mathbf{U}}: R^N & \longrightarrow & R^N \\ \mathbf{a} & \mapsto & \mathbf{T}\mathbf{a} + \mathbf{U} \\ \mathbf{a}^{t+1} & = & \mathbb{T}_{\mathbf{U}}(\mathbf{a}^t) \end{array}\right\} \tag{1.5.11}$$

or

$$\left.\begin{array}{rcl} \mathfrak{T}_{\mathbf{U}}: R^N & \longrightarrow & R^N \\ \mathbf{a} & \mapsto & \mathfrak{T}\mathbf{a} + \mathbf{U} \\ \mathbf{a}^{t+1} & = & \mathfrak{T}_{\mathbf{U}}(\mathbf{a}^t) \end{array}\right\} \tag{1.5.12}$$

for the hybrid case. In the non-hybrid case **U** is the vector with $i-th$ entry

$$u_i = \sum_{s=1}^{l-i} \alpha_{-i-s} a_{-s} + \sum_{s'=0}^{l+i-N} \alpha_{N+s'-i} a_{N+s'} \tag{1.5.13}$$

and in the hybrid case **U** is the vector with $i-th$ entry

$$u_i = \sum_{s=1}^{l-i} \alpha_{i,-i-s} a_{-s} + \sum_{s'=0}^{l+i-N} \alpha_{i,N+s'-i} a_{N+s'}. \tag{1.5.14}$$

Systems of the form 1.5.11 and 1.5.12 correspond to linear cellular automata and hybrids of linear cellular automata in the presence of time independent inputs and are considered in detail in the following chapters.

### 1.5.3 Representation of linear cellular automata with periodic boundary conditions

We shall consider the case of periodic boundary conditions on $N$ cells in some detail. Fixing $N$ we may identify the state space of the cellular automata with $R^N$ as in section 1.5.2. We may in turn identify the elements of $R^N$ bijectively with the subset of $R[x]$, the polynomial ring in one indeterminate over $R$, consisting of those elements of $R[x]$ of degree less than $N$. This set is additively indistinguishable from $R^N$. Martin *et al.* [3] showed that the action of the global rule $F_N$ on a state of the system represented in this way could be represented by the multiplicative action of a Laurent polynomial (which they refer to as a *dipolynomial*) $\mathbb{T}(x, x^{-1}) \in R[x, x^{-1}]$ and then reducing the result modulo $x^N - 1$. The operation of taking a polynomial or Laurent polynomial modulo $x^N - 1$ is a ring homomorphism from $R[x]$ or $R[x, x^{-1}]$ onto the quotient ring $R_N$,

$$R_N = \frac{R[x]}{(x^N - 1)R[x]} \cong \frac{R[x, x^{-1}]}{(x^N - 1)R[x, x^{-1}]} \tag{1.5.15}$$

where $(x^N - 1)R[x]$ is the ideal generated by $x^N - 1$ in $R[x]$. Motivated by the above observation it seems natural to identify the state space with the ring $R_N$ rather than $R^N$ or the subset of $R[x]$ described above. $R_N$ is additively indistinguishable from $R^N$ and the Laurent polynomial giving the action of the global rule can be replaced by an element of $R_N$, as we shall see. Using an element of $R_N$ in this way has the advantage that now all operations take place within the ring $R_N$ and is equivalent to the approach of Martin *et al*, and may be regarded as a formalisation of their method.

In detail a state $a \in R^N$, $a = (a_0, a_1, \ldots, a_{N-1})$ is identified with an element of $R_N$ via the map $\kappa$:

$$\begin{aligned} \kappa &: R^N \longrightarrow R_N \\ \kappa(a) &= a(x) + (x^N - 1)R[x] \\ &= \sum_{i=0}^{N-1} a_i x^i + (x^N - 1)R[x]. \end{aligned} \tag{1.5.16}$$

This identification is bijective since, as $x^N - 1$ is monic, each coset has a unique representative $a(x)$ of degree less than $N$ and each such polynomial is the representative of some coset in $R_N$. It is clear that $\kappa$ preserves additive structure, that is, $\kappa$ is a group homomorphism from $R^N$ to the additive group of $R_N$.

The action of the global rule is given, in this representation, by multiplication by an element $\mathbb{T}$ of $R_N$ defined as follows.

**Definition 1.5.1** *With $R$ and $N$ given, and local rule $f$ as in equation* (1.5.1)

$$\begin{aligned} \mathbb{T} &= \alpha_0 + \sum_{i=1}^{l} (\alpha_i x^{N-i} + \alpha_{-i} x^i) + (x^N - 1)R[x] \\ &= \mathbb{T}(x) + (x^N - 1)R[x]. \end{aligned}$$

Note that, despite the notation, if $N < l$ then $\alpha_0 + \sum_{i=1}^{l} (\alpha_i x^{N-i} + \alpha_{-i} x^i)$ may not be a polynomial but a Laurent polynomial, however by lemma A.2.4, and the comments afterwards we are justified in assuming $\mathbb{T} \in \frac{R[x]}{(x^N-1)R[x]}$ and $\mathbb{T}(x)$ is the polynomial described in the proof of lemma A.2.4.

Thus the global rule is represented by a map

$$\begin{aligned} \mathbb{T}_0 : R_N &\longrightarrow R_N \\ \kappa(a) &\mapsto \mathbb{T}\kappa(a). \end{aligned} \tag{1.5.17}$$

as we show in the following lemma.

**Lemma 1.5.1** *With $\mathbb{T}_0$ as defined above the action of the global rule induced by $f$ is represented by*

$$\kappa(a^{t+1}) = \mathbb{T}_0(\kappa(a^t))$$

Proof:

The state of the $i-th$ site at time $t+1$ under the action of the rule $f$ defined by (1.5.1) and under periodic boundary conditions on $N$ cells is

$$a_i^{t+1} = \sum_{j=-l}^{l} \alpha_j a^t_{(i+j)\text{mod } N}.$$

Thus we must check that the coefficient of $x^i$ in $a^{t+1}(x)$,

$$\kappa(a^{t+1}) = a^{t+1}(x) + (x^N - 1)R[x],$$

is $\sum_{j=-l}^{l} \alpha_j a^t_{(i+j)\text{mod } N}$. We note that on multiplying $\kappa(a^t)$ by $\alpha_j x^{N-j} + (x^N - 1)R[x]$, $x^i$ has coefficient $\alpha_j a^t_{(i+j)\text{mod } N}$. Similarly on multiplying by $\alpha_{-j}x^j + (x^N - 1)R[x]$, $x^i$ has coefficient $\alpha_{-j} a^t_{(i-j)\text{mod } N}$. On multiplying by $\alpha_0 + (x^N - 1)R[x]$ the coefficient of $x^i$ is $\alpha_0 a_i$. Since one can write

$$\mathbb{T} = \sum_{j=-l}^{l} (\alpha_{-j} x^{N+j} + (x^N - 1)R[x]),$$

the result follows. ■

Lemma 1.5.1 shows that the map $\mathbb{T}_0$ represents the global dynamics faithfully in $R_N$, in view of this we shall normally just write $a$ for $\kappa(a)$ and consider $R_N$ to be the global state space of the cellular automata and $\mathbb{T}_0$ to be the global rule. Given $a \in R_N$ we shall often refer to $a(x)$ without explanation, in this case we mean the canonical representative $a(x)$ of $a$, *i.e.* the unique element of $a$ of degree less than $N$, whose coefficients give the states of the cells if $a$ is thought of as a configuration of the system.

**Example 1.5.3**

The local rule of example 1.5.1 gives, on $N$ cells, the global rule represented by

$$\mathbb{T} = x + x^{N-1} + (x^N - 1)\mathbb{F}_2[x] \in \frac{\mathbb{F}_2[x]}{(x^N - 1)\mathbb{F}_2[x]}.$$

When $N = 4$, let $a$ be the configuration

$$a = (a_0, a_1, a_2, a_3).$$

With periodic boundary conditions the action of rule 90 on this configuration is to send $a$ to $F(a)$,

$$F(a) = (a_3 + a_1, a_0 + a_2, a_1 + a_3, a_2 + a_0).$$

In $R_N$ we have, in detail,

$$\begin{aligned}
a &= a_0 + a_1x + a_2x^2 + a_3x^3 + (x^4 - 1)\mathbb{F}_2[x] \\
\mathbb{T}a &= (x + x^3 + (x^4 - 1)\mathbb{F}_2[x])(a_0 + a_1x + a_2x^2 + a_3x^3 + (x^4 - 1)\mathbb{F}_2[x]) \\
&= (x + x^3)(a_0 + a_1x + a_2x^2 + a_3x^3) + (x^4 - 1)\mathbb{F}_2[x] \\
&= a_0x + a_1x^2 + (a_0 + a_2)x^3 + (a_1 + a_3)x^4 + a_2x^5 + a_3x^6 + (x^4 - 1)\mathbb{F}_2[x] \\
&= a_3 + a_1 + (a_0 + a_2)x + (a_1 + a_3)x^2 + (a_2 + a_0)x^3 + (x^4 - 1)\mathbb{F}_2[x] \\
&= \kappa(F(a)). \quad \blacklozenge
\end{aligned}$$

**Example 1.5.4**

The local rule of example 1.5.2 gives, on $N$ cells, the global rule represented by

$$\mathbb{T} = 1 + 3x^2 + 2x^3 + 2x^{N-3} + 3x^{N-2} + (x^N - 1)\mathbb{Z}_{/4}[x] \in \frac{\mathbb{Z}_{/4}[x]}{(x^N - 1)\mathbb{Z}_{/4}[x]} \quad \blacklozenge$$

Equation (1.5.17) defines, for given $R$ and each $N$, a map $f \mapsto \mathbb{T}$ from the space of all linear local rules onto $R_N$. The ring $R_N$ can be thought of as a module over itself, ${}_{R_N}R_N$ written as a left $R_N$-module (though the distinction between left and right modules is not important in this case because $R_N$ is commutative). Thus, since

$$End({}_{R_N}R_N) \cong R_N$$

(see [25], page 169) we see that each global additive cellular automata rule may be identified with a (module) endomorphism of $R_N$, and the cellular automata dynamics is equivalent to that given by iteration of this endomorphism. Thus we shall sometimes refer to $\mathbb{T}$ as a linear map of $R_N$ to itself and we shall no longer make any distinction between the map $\mathbb{T}_0$ and the element $\mathbb{T} \in R_N$ (and thus drop the subscript 0 from $\mathbb{T}_0$).

### 1.5.4 Linear cellular automata with time independent inputs

We shall be concerned not just with the behaviour of additive cellular automata but also with the behaviour of such automata under the influence of external inputs. In this chapter we assume that these inputs are constant and applied at each time step.

We shall sometimes refer to the inputs as controls and to the system consisting of an additive cellular automata plus external inputs as a controlled cellular automata. The inputs are applied locally, site $i$ has input $u_i \in R$ at each time step,

$$\begin{aligned} a_i^{t+1} &= f_i(a_{i-l}^t, \ldots, a_{i+l}^t) \\ &= f(a_{i-l}^t, \ldots, a_{i+l}^t) + u_i. \end{aligned} \tag{1.5.18}$$

From the above it is evident that a system of this form can be thought of as a hybrid of up to $|R|$ related rules, the rule applied at site $i$ is $f_i$ whose action is given by applying the linear rule $f$ and then adding the constant $u_i$. Such rules are no longer linear (for $u_i \neq 0$) as the image of zero is no longer zero and will be referred to as affine local rules. We shall be considering the finite case on $N$ cells with either periodic or fixed boundary conditions. The global rule is no longer additive if any $u_i$ is non-zero as clearly in this case $F_N(A) + F_N(B) \neq F_N(A + B)$, where $F_N$ is the global rule of the cellular automata plus inputs on $N$ cells. When the input is uniform, i.e. $u_i = u \neq 0$, $i = 0, \ldots, N-1$, one is applying the affine rule everywhere.

**Example 1.5.5**

Let $R = \mathbb{F}_2$, if input $u = 1$ is applied at every cell then for instance rule 90 becomes its complement, rule 165 (a non-additive rule), while a non-uniform input applied to rule 90 is equivalent to a hybrid of rules 90 and 165. ♦

We shall consider first the case of periodic boundary conditions, the presence of inputs $u_i$ at site $i$ is represented in $R_N$ by the addition of a constant $U$ at each time step,

$$\begin{aligned} U &= U(x) + (x^N - 1)R[x] \\ &= \sum_{i=0}^{N-1} u_i x^i + (x^N - 1)R[x]. \end{aligned} \tag{1.5.19}$$

Thus we now have the global rule $F_{N,U}$ represented by an affine map which gives the dynamics

$$\left.\begin{aligned} \mathbb{T}_U : R_N &\longrightarrow R_N \\ a &\mapsto \mathbb{T}a + U \\ a^{t+1} &= \mathbb{T}_U(a^t) \end{aligned}\right\} \tag{1.5.20}$$

The composition of $\mathbb{T}_U$ with itself $k$ times will be denoted by $\mathbb{T}_U^k$ and where necessary we will write

$$\mathbb{T}_U^k(a^t) = a^{t+k} \tag{1.5.21}$$

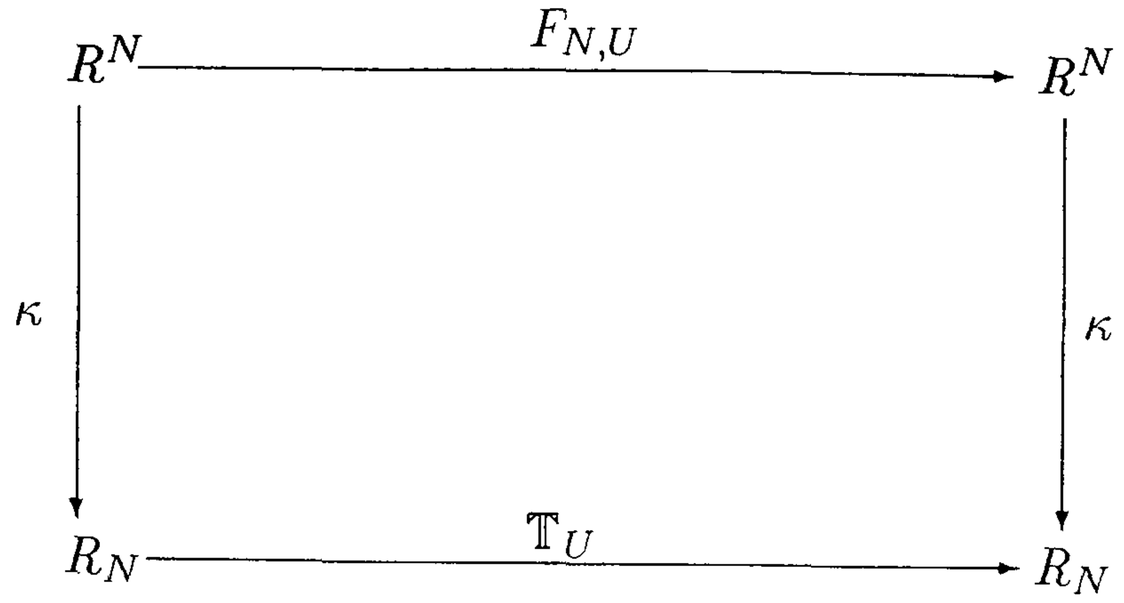


Figure 1.3: $\kappa \circ F_{N,U} = \mathbb{T}_U \circ \kappa$.

Of course the system defined by equations (1.5.20) reduces to that defined by (1.5.17) on taking $U = 0$ and we shall consider additive cellular automata as systems of the form (1.5.20) with $U = 0$ throughout the text, with $\mathbb{T}$ written for $\mathbb{T}_0$ in accordance with remarks made earlier. The general relationship between the dynamics in $R^N$ and $R_N$ is summed up by the commuting diagram in figure 1.3.

The above discussion suggests that we look at the systems with dynamics defined by

$$\left.\begin{array}{rcl} \mathbb{T}_U : \frac{R[x]}{g(x)R[x]} & \longrightarrow & \frac{R[x]}{g(x)R[x]} \\ a & \mapsto & \mathbb{T}a + U \\ a^{t+1} & = & \mathbb{T}_U(a^t) \end{array}\right\} \tag{1.5.22}$$

where the leading coefficient of $g(x) \in R[x]$ is a unit and $\mathbb{T}, U \in \frac{R[x]}{g(x)R[x]}$. Unless noted otherwise all results about systems defined by (1.5.20) hold for systems defined by (1.5.22), by just replacing $R_N$ with $\frac{R[x]}{g(x)R[x]}$ everywhere. Further, such results will still hold if $R[x]$ is replaced by $R[x_1, \ldots, x_n]$ and $g(x)$ by $g_1(x_1), \ldots, g_n(x_n)$ *etc.*. This is because most of the proofs we shall be presenting for general $R$ do not rely on any properties peculiar to $R_N$, but just upon the properties of finite commutative rings. We shall have some use for these more general results in latter chapters.

When the boundary conditions are fixed rather than periodic or we have a hybrid system with either form of boundary conditions $U$ is replaced by the vector

$$\mathbf{U} = (u_0, u_1, \ldots, u_{N-1})^T \tag{1.5.23}$$

where $u_i$ is the input at site $i$ at each time step. Formally for null boundary conditions we are considering the system defined by

$$\left.\begin{array}{rcl} \mathbb{T}_{\mathbf{U}} : R^N & \longrightarrow & R^N \\ \mathbf{a} & \mapsto & \mathbf{Ta} + \mathbf{U} \\ \mathbf{a}^{t+1} & = & \mathbb{T}_{\mathbf{U}}(\mathbf{a}^t) \end{array}\right\} \tag{1.5.24}$$

while for the hybrid case we have

$$\left.\begin{array}{rcl} \mathfrak{T}_{\mathbf{U}} : R^N & \longrightarrow & R^N \\ \mathbf{a} & \mapsto & \mathfrak{T}\mathbf{a} + \mathbf{U} \\ \mathbf{a}^{t+1} & = & \mathfrak{T}_{\mathbf{U}}(\mathbf{a}^t) \end{array}\right\} \tag{1.5.25}$$

For fixed boundary conditions other than zero, we consider the systems 1.5.24 and 1.5.25 with $\mathbf{U}$ replaced by $\mathbf{U} + \mathbf{V}$ where $V$ is defined by 1.5.13 or 1.5.14.

We finish this section with a result for periodic boundary conditions.

**Theorem 1.5.1** *Suppose that*

$$R_N \cong \prod_{i=1}^{n} R_{N,i}$$

*for some rings $R_{N,i}$ and with isomorphism $\phi$ induced by homomorphisms $\phi_i : R_N \longrightarrow R_{N,i}$. Then for each $\mathbb{T}, U \in R_N$*

$$\Sigma(\mathbb{T}_U) = \prod_{i=1}^{n} \Sigma(\phi_i \circ \mathbb{T}_U) = \prod_{i=1}^{n} \Sigma(\phi_i(\mathbb{T})_{\phi_i(U)})$$

Proof:

As $\phi$ is a ring isomorphism it preserves dynamical structure, *i.e.*

$$a^{t+1} = \mathbb{T}_U(a^t) = \mathbb{T}a^t + U$$

if and only if

$$\phi(a)^{t+1} = \phi(\mathbb{T})_{\phi(U)}(\phi(a^t)) = \phi(\mathbb{T})\phi(a^t) + \phi(U)$$

Suppose first that $\mathbb{T}, U \in R_{N,1} \times R_{N,2}$. For each $a \in R_{N,1} \times R_{N,2}$ let $a_i = \phi_i(a) \in R_{N,i}$, $i = 1, 2$, similarly for $\mathbb{T}_i, U_i$. Suppose that in $R_{N,i}$ under $(\mathbb{T}_i)_{U_i}$ there are $m_i$ orbits of length $\mathrm{t}_i$. Let $a \in R_{N,1} \times R_{N,2}$ be such that $a_1$ is on a cycle of length $\mathrm{t}_1$ and $a_2$ is on a

cycle of length $t_2$, then clearly $a$ is on an orbit of length $\mathrm{lcm}(t_1, t_2)$. There are $m_1 t_1 m_2 t_2$ such elements in $R_{N,1} \times R_{N,2}$ hence the number of such orbits is

$$\frac{m_1 t_1 m_2 t_2}{\mathrm{lcm}(t_1 t_2)} = m_1 m_2 \mathrm{gcd}(t_1 t_2)$$

which is the product of the cycle terms $m_1[t_1]$ and $m_2[t_2]$. Thus we have

$$\Sigma(\mathbb{T}_U) = \Sigma((\mathbb{T}_1)_{U_1}).\Sigma((\mathbb{T}_2)_{U_2}).$$

The result now follows by induction. ■

### 1.5.5 The work of Martin, Odlyzko and Wolfram

We review some of the results of Martin *et al.* [3] but rewrite them in the language of section 1.5.3. Those authors concentrated on the case $R = \mathbb{F}_p$ and also proved some results for $R = \mathbb{Z}_{/k}$, $k$ a composite integer.

**Lemma 1.5.2** [Martin, Odlyzko and Wolfram]
*For given $R, N$ and $\mathbb{T}$, two elements $a, b \in R_N$ evolve to the same element $c \in R_N$ under $\mathbb{T}$ after $t$ time steps if and only if*

$$a = b + q,\ q \in R_N.\ \mathbb{T}^t q = 0. \tag{1.5.26}$$

Proof:

Clearly if $a = b + q$ where $\mathbb{T}^t q = 0$ then $\mathbb{T}^t a = \mathbb{T}^t b$. If $\mathbb{T}^t a = \mathbb{T}^t b$ then $\mathbb{T}^t(a - b) = 0$ so let $q = a - b$ and the result follows. ■

**Theorem 1.5.2** [Martin, Odlyzko and Wolfram]
*The trees rooted at each element of each cycle occurring under $\mathbb{T}$ are all identical to the tree rooted at 0.* ■

We prove a generalisation of the above theorem in the next chapter and so omit the proof here.

**Lemma 1.5.3** [Martin, Odlyzko and Wolfram]
*For $R = \mathbb{F}_{p^q}$, $p$ a prime integer, $q > 0$ and given $N$ and $\mathbb{T}$, then configuration $a \in \frac{\mathbb{F}_{p^q}[x]}{(x^N-1)\mathbb{F}_{p^q}[x]}$ is reachable in $j$ time steps if and only if $\Lambda_j(x) \mid a(x)$ in $\mathbb{F}_{p^q}[x]$, where*

$$\Lambda_j(x) = \mathrm{gcd}(x^N - 1, \mathbb{T}^j(x)) \tag{1.5.27}$$

Proof:

Suppose that $a \in R_N$ has a predecessor $b$ under $\mathbb{T}^j$, $\mathbb{T}^j b = a$, then in $\mathbb{F}_{pq}[x]$ we have

$$\mathbb{T}^j(x)b(x) - a(x) = g(x)(x^N - 1)$$

for some $g(x) \in \mathbb{F}_{pq}[x]$, so $x^N - 1 \mid (\mathbb{T}^j(x)b(x) - a(x))$. But $\Lambda_j(x) \mid x^N - 1$ and $\Lambda_j(x) \mid \mathbb{T}^j(x)$ hence $\Lambda_j(x) \mid a(x)$.

Now suppose that $\Lambda_j(x) \mid a(x)$ for some $a \in R_N$, then

$$a(x) = \Lambda_j(x)b(x)$$

for some $b(x) \in \mathbb{F}_{pq}[x]$, so in $R_N$ we have $a = \Lambda_j b$. Now as $\mathbb{F}_{pq}$ is a field we have

$$\Lambda_j(x) = f(x)\mathbb{T}^j(x) + h(x)(x^N - 1)$$

for some $f(x), h(x) \in \mathbb{F}_{pq}[x]$. Thus in $R_N$

$$\Lambda_j = f\mathbb{T}^j$$

so $\mathbb{T}^j f b = \Lambda_j b = a$. Thus

$$fb = f(x)b(x) + (x^N - 1)\mathbb{F}_{pq}[x]$$

is a predecessor of $a$ under $\mathbb{T}^j$. ■

The following corollary characterises the units (reversible rules) in $R_N$ when $R$ is a finite field.

**Corollary 1.5.1** *If $R = \mathbb{F}_{pq}$, then for given $N$, $\mathbb{T} \in R_N$ is a unit if and only if* $\gcd(\mathbb{T}(x), x^N - 1) = 1$.

Proof:

If $\mathbb{T}$ is reversible then every configuration has a predecessor so $\Lambda_1(x) \mid a(x)$ for every $a \in R_N$, hence $\Lambda_1(x) = 1$. Conversely if $\Lambda_1(x) = 1$ then $\Lambda_1(x) \mid a(x)$ for each $a \in R_N$ so each $a$ has a predecessor hence $\mathbb{T}$ is reversible hence $\mathbb{T}$ is a unit. ■

Let $\Pi_N(\mathbb{T})$ be the length of the cycle that 1 evolves to under $\mathbb{T}$ (clearly this is the maximum cycle length that occurs).

**Lemma 1.5.4** [Martin, Odlyzko and Wolfram]
*For $R = \mathbb{F}_p$ and $N$ a multiple of $p$,*

$$\Pi_N(\mathbb{T}) \mid p\Pi_{N/p}(\mathbb{T}')$$

*where* $\mathbb{T}'$ *represents the global rule for the same local rule as* $\mathbb{T}$ *but on* $N/p$ *cells. If* $N$ *is not a multiple of* $p$ *then*

$$\Pi_N(\mathbb{T}) \mid p^{\mathrm{ord}_N(p)} - 1,$$

*where* $\mathrm{ord}_N(p)$ *is the minimum integer* $j$ *such that* $p^j \equiv 1 \bmod N$. ■

We prove stronger results than this for $R = \mathbb{F}_{p^q}$ in chapters 3 and 4 and so omit the proof of lemma 1.5.4. Martin *et al.* also proved a result on tree structure when $R = \mathbb{F}_p$, we prove similar results in Chapter 4 and so omit such results here.

The results obtained by Martin *et al.* for $R = \mathbb{Z}_{/k}$, $k$ a composite integer depend upon the following result.

**Lemma 1.5.5** [Martin, Odlyzko and Wolfram]
*When* $R = \mathbb{Z}_{/k}$ *where* $k = \prod_{i=1}^{n} p_i^{\alpha_i}$, *each* $p_i$ *a distinct prime and* $\alpha_i > 0$, *the value* $a$ *of a site obtained by evolution of an additive cellular automata from some initial condition is given uniquely in terms of the values* $a(p_i^{\alpha_i})$ *attained by that site in the evolution of the set of cellular automata obtained by reducing* $\mathbb{T}(x)$ *and all site values modulo* $p_i^{\alpha_i}$.
■

We prove the following result, which taken together with theorem 1.5.1 is equivalent to lemma 1.5.5.

**Theorem 1.5.3** *Let* $k$ *be a positive integer, with unique factorisation into powers of primes given by*

$$k = \prod_{i=1}^{n} p_i^{\alpha_i}$$

*where* $\alpha_i > 0$, $1 \leq i \leq n$. *Then for all* $N > 0$

$$\frac{\mathbb{Z}_{/k}[x]}{(x^N - 1)\mathbb{Z}_{/k}[x]} \cong \prod_{i=1}^{n} \frac{\mathbb{Z}_{/p_i^{\alpha_i}}[x]}{(x^N - 1)\mathbb{Z}_{/p_i^{\alpha_i}}[x]}.$$

Proof:

The map $\pi_i : \mathbb{Z}_{/k} \longrightarrow \mathbb{Z}_{/p_i^{\alpha_i}}$, given by $a + k\mathbb{Z} \mapsto a + p_i^{\alpha_i}\mathbb{Z}$ is clearly a surjective ring homomorphism for $1 \leq i \leq n$. Then, by lemma A.2.3, for each $i$ there is a homomorphism

$$\phi_i : \frac{\mathbb{Z}_{/k}[x]}{(x^N - 1)\mathbb{Z}_{/k}[x]} \longrightarrow \frac{\mathbb{Z}_{/p_i^{\alpha_i}}[x]}{(x^N - 1)\mathbb{Z}_{/p_i^{\alpha_i}}[x]},$$

given by

$$a(x) + (x^N - 1)\mathbb{Z}_{/k}[x] \mapsto \chi_i(a(x)) + (x^N - 1)\mathbb{Z}_{/p_i^{\alpha_i}}[x]$$

where $\chi_i : \mathbb{Z}_{/k}[x] \longrightarrow \mathbb{Z}_{/p_i^{\alpha_i}}[x]$ is the homomorphism induced by $\pi_i$. Define

$$\Phi : \frac{\mathbb{Z}_{/k}[x]}{(x^N - 1)\mathbb{Z}_{/k}[x]} \longrightarrow \prod_{i=1}^{n} \frac{\mathbb{Z}_{/p_i^{\alpha_i}}[x]}{(x^N - 1)\mathbb{Z}_{/p_i^{\alpha_i}}[x]}$$

by

$$a \mapsto (\phi_1(a), \phi_2(a), \ldots, \phi_n(a)).$$

$\Phi$ is a homomorphism since each $\phi_i$ is. We examine the kernel of $\Phi$:

$$\begin{aligned}
\text{Ker } \Phi &= \{a : \phi_i(a) = 0, 1 \leq i \leq n\} \\
&= \{a : \chi_i(a(x)) = 0, 1 \leq i \leq n\} \\
&= \{a : \sum_{j=0}^{\deg\, a(x)} \pi_i(a_j)x^j = 0, 1 \leq i \leq n\} \\
&= \{a : \pi_i(a_j) = 0, 0 \leq j \leq \deg\, a(x), 1 \leq i \leq n\} \\
&= \{a : p_i^{\alpha_i} \mid a_j, 0 \leq j \leq \deg\, a(x), 1 \leq i \leq n\} \\
&= \{a : k \mid a_j, 0 \leq j \leq \deg\, a(x)\} \\
&= \{0\}.
\end{aligned}$$

Hence $\Phi$ is injective. Now

$$\left| \frac{\mathbb{Z}_{/k}[x]}{(x^N - 1)\mathbb{Z}_{/k}[x]} \right| = k^N$$

and

$$\begin{aligned}
\left| \prod_{i=1}^{n} \frac{\mathbb{Z}_{/p_i^{\alpha_i}}[x]}{(x^N - 1)\mathbb{Z}_{/p_i^{\alpha_i}}[x]} \right| &= \prod_{i=1}^{n} \left| \frac{\mathbb{Z}_{/p_i^{\alpha_i}}[x]}{(x^N - 1)\mathbb{Z}_{/p_i^{\alpha_i}}[x]} \right| \\
&= \prod_{i=1}^{n} (p_i^{\alpha_i})^N \\
&= (\prod_{i=1}^{n} p_i^{\alpha_i})^N \\
&= k^N.
\end{aligned}$$

Now an injection between finite sets of the same size is a bijection and $\Phi$ is a homomorphism hence $\Phi$ is an isomorphism. ■

Martin *et.al.* were unable to produce any general results for the $\mathbb{Z}_{/p^k}$, $k > 1$, case, we quote : "no general results are available for the case of prime power $k$". They go on to say that some results can be obtained in specific cases using combinatorial methods. In chapter 5 we are able to provide some general results for the $\mathbb{Z}_{/p^k}$ case.

Martin *et.al.* also described an embedding (for symmetric rules of radius one) of the null boundary condition case on $N$ cells into the periodic boundary condition case on $2N+2$ cells and an extension of this to the case of fixed boundary conditions where the site with index $-1$ has a non-zero value (though the expression they give is incorrect). This case can be considered as the periodic boundary condition case with a constant input and will generalise to symmetric rules of any radius (where if the rule has radius $l$ then the embedding will be into the $2N+2l$ case) and any fixed boundary conditions. However, demanding that the rule be symmetrical is restrictive and, moreover, we shall generally endevour to reduce the number of cells rather than increase them throughout this thesis. For the afore-mentioned reasons we will make no use of this embedding procedure.

# Chapter 2

# Finite linear cellular automata over a commutative ring

In this chapter we consider the general case of additive cellular automata with state alphabet a finite commutative ring $R$ and finite boundary conditions, both with and without time independent inputs. We are mainly concerned with periodic boundary conditions, however we have included results for boundary conditions other than periodic and hybrids of additive cellular automata whenever we can prove such results "for free", that is whenever the proof of the result is essentially the same as that in the periodic boundary condition case.

We note that whenever a result in this chapter applies for null boundary conditions with time independent inputs then it applies for any fixed boundary conditions (see section 1.5.2) as any such system can be considered as the same cellular automata with null boundary conditions and a modified time independent input. Our goals in this chapter are twofold, firstly to provide general results that are useful and interesting in their own right and secondly to provide a toolbox for use in latter chapters where more specific choices of state alphabet are considered.

In section 2.1 we discuss some basic properties, starting in section 2.1.1 with some general remarks concerning periodic and transient behaviour and the introduction of some notation which is used throughout this thesis. We show that associated to each additive cellular automata on $N$ cells there are two ideals (submodules), the set of elements of $R_N$ ($R^N$) on cycles under the rule and the set of elements of $R_N$ ($R^N$) that evolve to zero under the rule. In section 2.1.2 we concentrate on the case of zero input and periodic boundary conditions. We show that a cellular automata rule represented by $\mathbb{T} \in R_N$ on $N$ cells is reversible on $N$ cells if and only if $\mathbb{T}$ is a unit in $R_N$ and the behaviour of configurations under the rule represented by $\mathbb{T}$ is related to the properties of the representatives of the configurations in $R_N$ (lemma 2.1.5). We also show that (theorem 2.1.1) additive cellular automata with periodic boundary conditions on $N$ cells and state alphabet a finite commutative ring $R$ cannot have cycles of length $|R_N| - 1$ (see section 1.5.1, cellular automata that can generate cycles of length $|R|^N - 1$ are candidates for pseudorandom number generators, thus additive cellular automata with periodic boundary conditions can be excluded from any search for such pseudorandom number generators).

In section 2.1.3 we consider non-zero inputs and obtain various upper bounds on orbit lengths in the system with inputs in the form of divisibility relations, for instance in lemma 2.1.13 we show that the length of the orbit that zero evolves to in the system with non-zero input $U$ must divide the orbit length of input $U$ considered as a config-

uration in the system with zero input, multiplied by the characteristic of $R$. We find these results useful in obtaining more precise results in lat er chapters.

In section 2.2 we consider the structure of the state transition graph in detail, beginning with the generalisation of theorem 1.5.2 to the non-zero input case, as a corollary we find that the number of configurations in the system with inputs which lie on cycles is the same as that in the system without inputs. In theorem 2.2.2 we show that the possible sets of elements on cycles in the system with inputs are the cosets in the quotient ring $R_N/Att(\mathbb{T})$ where $\mathbb{T}$ is the representative of the rule on $N$ cells and $Att(\mathbb{T})$ is the set of elements on cycles under $\mathbb{T}$. (For other boundary conditions *etc.* replace quotient ring with quotient module *etc.*). We give necessary and sufficient conditions for different inputs to yield the same sets of elements on cycles. In theorem 2.2.3 we show how the set of configurations on cycles in the presence of input $U$ is related to the position of $U$, considered as a configuration of the system without inputs, in the state transition graph of the system without inputs.

In section 2.3 we introduce a notion of qualitative dynamical similarity (QDS) for systems with inputs, roughly speaking the systems given by two distinct inputs are QDS if their state transition graphs "look the same" (this is made precise in section 2.3). In theorem 2.3.1 we show that the system with input $U$ is QDS to the system with zero input if and only the system with input $U$ has a fixed point and in corollary 2.3.3 we show that a necessary and sufficient condition for any input to give a system QDS to that with input zero is that the zero input system has only one fixed point (necessarily zero).

In theorem 2.3.2 we give a sufficient condition for systems with different inputs to be QDS in terms of an equivalence relation on $R_N$ considered as the set of possible inputs. In theorem 2.3.3 we show that when a certain condition is satisfied then a necessary and sufficient condition for systems with different inputs to be QDS is that the minimum orbit lengths under each system be equal. In chapter 4 we show that the condition of theorem 2.3.3 holds whenever the state alphabet is a finite field and in chapter 5 we show that the condition holds when the state alphabet is $\mathbb{Z}/m\mathbb{Z}$ for any integer $m > 1$. In chapter 6, section 6.1 we show how results for time independent inputs from this chapter can be used to obtain results for time dependent inputs when such inputs are periodic in time.

## 2.1 Basic properties

### 2.1.1 Some general remarks on periodic and transient behaviour

Many results in this chapter concern the ring $R_N$ but do not rely on any special property of $R_N$ as opposed to any finite commutative ring. The following remark is proved by examining the proofs of the relevant results:

**Remark 2.1.1** *All results in this chapter stated for the ring $R_N$ hold with $R_N$ replaced with any finite commutative ring, with the exceptions of theorem 2.1.1, lemma 2.1.6 and corollary 2.1.2.* ■

One might ask: why state results for $R_N$ if they hold more generally? The answer is simply that we are concerned with cellular automata over the finite commutative ring $R$ and hence with $R_N$ and while we will have some use for more general results, to state all our results in the more general form might obscure their relevance to cellular automata.

We shall now consider the set of elements of $R_N$ which reoccur under $\mathbb{T}_U$. Orbits are defined as usual, the forward orbit of $a \in R_N$ under $\mathbb{T}_U$ is denoted by $O_U(a)$.

**Definition 2.1.1** *$a \in R_N$ is eventually periodic under $\mathbb{T}_U$ if there are some integers $T \geq 0$ and $k \geq 1$ such that*

$$\mathbb{T}_U^{T+k}(a) = \mathbb{T}_U^T(a).$$

*If $T$ can be chosen to be zero then $a$ is periodic with period $k$.*

Thus, as usual, a cycle is the orbit of a periodic point. The prime period of a periodic point $a$ is the length of its cycle, any multiple of this is a period of $a$. We shall denote the set of distinct cycles occurring under $\mathbb{T}_U$ by $Cyc(\mathbb{T}_U)$. Given the finite number of states,

$$|R_N| = |R|^N, \tag{2.1.1}$$

all orbits are eventually periodic. We shall call the set of points that reoccur the *invariant set* of $\mathbb{T}_U$, $Att(\mathbb{T}_U)$, defined by

**Definition 2.1.2**

$$Att(\mathbb{T}_U) = \{a : a \in R_N, \mathbb{T}_U^k(a) = a, \ \textit{some } k \in \mathbf{N}_{>0}\}$$

Note that

$$Att(\mathbb{T}_U) = \bigcup_{C \in Cyc(\mathbb{T}_U)} C.$$

We shall also define $Fix(\mathbb{T}_U)$ to be that subset of $Att(\mathbb{T}_U)$ consisting of those points on cycles of length one, *i.e.* the fixed points of $\mathbb{T}_U$.

**Example 2.1.1**

Let $R = \mathbb{F}_2$, $N = 3$ and $\mathbb{T} = (x+1) + (x^3 - 1)\mathbb{F}_2[x]$. One finds that, representing $a \in \frac{\mathbb{F}_2[x]}{(x^3-1)\mathbb{F}_2[x]}$ by its canonical representative $a(x) \in \mathbb{F}_2[x]$,

$$\begin{aligned} Att(\mathbb{T}) &= \{0, 1+x, 1+x^2, x+x^2\}, \\ Fix(\mathbb{T}) &= \{0\}. \quad \blacklozenge \end{aligned}$$

When the boundary conditions are fixed rather than periodic or we have a hybrid system with either form of boundary conditions we make the obvious definitions for orbits, periodic points *etc.*, corresponding to those given above.

**Example 2.1.2**

Let $R = \mathbb{F}_2$ and $N = 3$. Consider the hybrid consisting of local rule 90 at sites 0 and 2 and local rule 150 at site 1, with periodic boundary conditions. The global rule is represented by the matrix

$$\mathbf{T} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Then one finds that $Att(\mathbf{T}) = R^N$, and

$$Fix(\mathbf{T}) = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right\} \quad \blacklozenge$$

We shall denote the cycle that $a \in R_N$ evolves to under $\mathbb{T}_U$ by $C_U(\mathbb{T}, a)$ or $C_U(a)$ when no confusion can arise. The length of $C_U(a)$ is denoted by $(\phi_a)_U$. For null boundary conditions replace $U$ with $\mathbf{U}$ *etc.*, similarly for hybrids.

**Lemma 2.1.1** *Given $R$ and $N$, and either $\mathbb{T}$ and $U$ or $\mathbf{T}$ and $\mathbf{U}$ or $\mathfrak{T}$ and $\mathbf{U}$, we have for any integer $k > 0$*

$$\text{(i)} \quad \mathbb{T}_U^k(a) = a \quad \Leftrightarrow \quad (\phi_a)_U \mid k;$$

$$\text{(ii)} \quad \mathbb{T}_{\mathbf{U}}^k(\mathbf{a}) = \mathbf{a} \quad \Leftrightarrow \quad (\phi_{\mathbf{a}})_{\mathbf{U}} \mid k;$$

$$\text{(iii)} \quad \mathfrak{T}_{\mathbf{U}}^k(\mathbf{a}) = \mathbf{a} \quad \Leftrightarrow \quad (\phi_{\mathbf{a}})_{\mathbf{U}} \mid k.$$

Proof:

We prove (i), the others are identical. That $(\phi_a)_U \mid k \Rightarrow \mathbb{T}_U^k(a) = a$ is obvious. Suppose $\mathbb{T}_U^k(a) = a$ and let $(\phi_a)_U = L$. Suppose that $L \nmid k$, then $k > L$ since $k < L$ would contradict the minimality of $L$. So $k = mL + n$ where $m \geq 0$ and $1 \leq n < L$. Then

$$\begin{aligned} & \mathbb{T}_U^{mL+n}(a) = a \\ \Rightarrow \quad & \mathbb{T}_U^{(m-1)L+n}(\mathbb{T}_U^L(a)) = a \\ & \vdots \qquad\qquad \vdots \\ \Rightarrow \quad & \mathbb{T}_U^n(a) = a \end{aligned}$$

which contradicts the minimality of $L$. ■

**Definition 2.1.3** *For given $R, N$ and $\mathbb{T}$ let $T(\mathbb{T})$ be the maximum number of time steps for any $a \in R_N$ to reach $Att(\mathbb{T})$ under $\mathbb{T}$.*

When no confusion can arise we shall write $T$ for $T(\mathbb{T})$. In terms of the state transition graph $\Gamma(\mathbb{T})$ of $\mathbb{T}$, $T$ is the maximum tree height that occurs.

**Definition 2.1.4** *For given $R, N, U$ and $\mathbb{T}$ and any $a \in Att(\mathbb{T}_U)$ let $T_U(\mathbb{T}, a)$ be the set of elements of $R_N$ not on cycles that reach $Att(\mathbb{T}_U)$ first at $a$,* together with a.

In terms of $\Gamma(\mathbb{T}_U)$, $T_U(\mathbb{T}, a)$ is the tree rooted at $a$. We make the obvious analogous definitions for fixed boundary conditions and hybrids.

**Example 2.1.3**

For example 2.1.1 one finds

$$T_0(\mathbb{T}, 0) = \{0, 1 + x + x^2\}$$

and that $T(\mathbb{T}) = 1$.

**Example 2.1.4**

Let $R = \mathbb{F}_3$, $N = 3$ and consider the rule 90 like rule, $f(a_{i-1}, a_{i+1}) = a_{i-1} + a_{i+1}$ with null boundary conditions. The global rule is represented by

$$\mathbf{T} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

One finds that

$$T_0(\mathbf{T}, \mathbf{0}) = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix} \right\} \quad \blacklozenge$$

For each $R$ and $N$ there are two ideals of $R_N$ associated to each additive cellular automata rule:

**Lemma 2.1.2** *For every $R$ and $N$ and each $\mathbb{T} \in R_N$*

(i) *$Att(\mathbb{T})$ is an ideal of $R_N$;*

(ii) *$T_0(\mathbb{T}, 0)$ is an ideal of $R_N$.*

*Similarly for null boundary conditions and hybrids with ideal of $R_N$ replaced with submodule of $R^N$.*

Proof:

This is a simple verification. ■

**Corollary 2.1.1** *For any $R$ and $N$ and $\mathbb{T} \in R_N$, $| Att(\mathbb{T}) | \mid | R_N |$ and $| T_0(\mathbb{T}, 0) | \mid | R_N |$. Similarly for null boundary conditions and hybrids.*

Proof:

This is immediate on applying Lagrange's theorem. ■

If $\mathbb{T}$ is a unit in $R_N$ then $Att(\mathbb{T}) = R_N$, if $\mathbb{T}$ is nilpotent in $R_N$ then $Att(\mathbb{T}) = \{0\}$. However if $\mathbb{T}$ is a non-nilpotent zero-divisor in $R_N$ then, as we shall see in 2.1.5 (ii), $Att(\mathbb{T})$ contains no units, also $Att(\mathbb{T}) \setminus \{0\} \neq \emptyset$ so $Att(\mathbb{T})$ is a proper ideal of $R_N$. Considering $T_0(\mathbb{T}, 0)$ we see that if $\mathbb{T}$ is nilpotent in $R_N$ then $T_0(\mathbb{T}, 0) = R_N$ and if $\mathbb{T}$ is a unit in $R_N$ then $T_0(\mathbb{T}, 0) = \{0\}$. Suppose $\mathbb{T}$ is a non-nilpotent zero-divisor in $R_N$, then $T_0(\mathbb{T}, 0)$ contains no units , again as we shall see in 2.1.5 (iii), and

$$\{0\} \subsetneq T_0(\mathbb{T}, 0) \subsetneq R_N.$$

So $T_0(\mathbb{T}, 0)$ is a proper ideal of $R_N$ and we have proved the following:

**Lemma 2.1.3** *$T_0(\mathbb{T},0)$ and $Att(\mathbb{T})$ are proper ideals of $R_N$ if and only if $\mathbb{T}$ is a non-nilpotent zero-divisor in $R_N$. Similarly for null boundary conditions and hybrids with $\mathbf{T}$ or $\mathfrak{T}$ a non-nilpotent singular matrix.* ■

Certain sub ideals of $T_0(\mathbb{T},0)$ and $Att(\mathbb{T})$ will prove useful lat er.

**Definition 2.1.5** *With given $R, N$ and $\mathbb{T}$, let $j$ be a positive integer, $0 \leq j \leq T(\mathbb{T})$, then*

$$T_0^j(\mathbb{T},0) = \{a \in R_N : \mathbb{T}^j a = 0\}.$$

*For any strictly positive integer $k$ let*

$$Cyc(\mathbb{T},k) = \{a \in Att(\mathbb{T}) : \mathbb{T}^k a = a\}.$$

The sets defined above are ideals of $R_N$ (the proof is the same as that of lemma 2.1.2) and are clearly contained in $T_0(\mathbb{T},0)$ and $Att(\mathbb{T})$ respectively. Note that $Fix(\mathbb{T}) \leq Cyc(\mathbb{T},k)$ for all $k > 0$. The same definitions are made for null boundary conditions and hybrids, the corresponding sets are then submodules. For non-zero inputs $U$ we make a similar definition, the sets are, in general, no longer ideals (submodules):

**Definition 2.1.6** *With given $R, N, \mathbb{T}$ and $U$, let $j$ be a positive integer, $0 \leq j \leq T(\mathbb{T})$, then*

$$T_0^j(\mathbb{T},U) = \{a \in R_N : \mathbb{T}_U^j(a) = 0\}.$$

*For any positive integer $k$ let*

$$Cyc(\mathbb{T}_U,k) = \{a \in Att(\mathbb{T}_U) : \mathbb{T}_U^k(a) = a\}.$$

### 2.1.2 Basic properties for $U = 0$

In this section we shall discuss the case of the system of 1.5.20 with $U = 0$, or equivalently the system defined by 1.5.17, for periodic boundary conditions. We begin with the following definition which includes the null boundary condition and hybrid cases.

**Definition 2.1.7** *For an additive cellular automata on $N$ cells with periodic boundary conditions and global rule represented by $\mathbb{T}$ let $\Pi_N(\mathbb{T})$ be the least integer satisfying*

$$\mathbb{T}^{T+\Pi_N(\mathbb{T})} = \mathbb{T}^T, \quad \forall\ T \geq T(\mathbb{T}).$$

*For an additive cellular automata on $N$ cells with null boundary conditions and global rule represented by $\mathbf{T}$ let $\Pi_N(\mathbf{T})$ be the least integer satisfying*

$$\mathbf{T}^{T+\Pi_N(\mathbf{T})} = \mathbf{T}^T.$$

*For a hybrid of linear cellular automata on $N$ cells with periodic or null boundary conditions and global rule represented by $\mathfrak{T}$ let $\Pi_N(\mathfrak{T})$ be the least integer satisfying*

$$\mathfrak{T}^{T+\Pi_N(\mathfrak{T})} = \mathfrak{T}^T.$$

For the case of periodic boundary conditions Martin *et al.* (see chapter 1, section 1.5.5) defined $\Pi_N(\mathbb{T})$ to be the length of the orbit that 1 evolves to under $\mathbb{T}$, *i.e.* $(\phi_1)_0$. It is clear that our definition is equivalent to theirs.

**Lemma 2.1.4** *For given $R, N$ and $\mathbb{T}$, all orbit lengths occurring under $\mathbb{T}$ divide $\Pi_N(\mathbb{T})$. Similarly for null boundary conditions and hybrids.*

Proof:

This follows from lemma 2.1.1 on putting $U = 0$ and $k = \Pi_N(\mathbb{T})$. ■

**Example 2.1.5**

Let $R = \mathbb{F}_2$, $N = 5$ and $\mathbb{T} = 1 + x + x^4 + (x^5 - 1)\mathbb{F}_2[x]$. Then one finds that $\mathbb{T}^2 \neq 1$ but $\mathbb{T}^3 = 1$ hence $\Pi_5(\mathbb{T}) = 3$. Thus in this case the only possible cycle lengths are 1 or 3. ♦

A cellular automata rule is reversible on $N$ cells if every configuration has a predecessor under the rule. The following result characterises those additive cellular automata that are reversible for a given $N$.

**Remark 2.1.2** *For given $R$ and $N$ the additive cellular automata with representative $\mathbb{T}$ is reversible if and only if $\mathbb{T}$ is a unit in $R_N$.*

Proof:

If $\mathbb{T}$ is reversible then every element of $R_N$ has a predecessor under $\mathbb{T}$ so 1 has a predecessor under $\mathbb{T}$ so $\mathbb{T}$ is a unit. Conversely if $\mathbb{T}$ is a unit then $\mathbb{T}R_N = R_N$ so every element of $R_N$ has a predecessor under $\mathbb{T}$ so $\mathbb{T}$ is reversible. ■

Similarly for null boundary conditions and hybrids we have that a rule (hybrid of rules) is reversible on $N$ cells if and only if $\mathbf{T}$ ($\mathfrak{T}$) is an invertible matrix.

**Example 2.1.6**

In example 2.1.5 $\mathbb{T}^3 = 1$ so $\mathbb{T}$ is a unit hence any additive cellular automata whose global rule is represented by this $\mathbb{T}$ on 5 cells is reversible on 5 cells. ♦

**Example 2.1.7**

The additive cellular automata with local rule $f(a_{i-1}, a_i) = a_{i-1} - a_i$ and periodic boundary conditions is not reversible for any $R$ and $N$.

Proof:

For any $R$ and $N$ and the local rule $f$ one has the global rule represented by

$$\mathbb{T} = x - 1 + (x^N - 1)R[x].$$

For any $R$ one has that in $R[x]$ for each $N > 1$

$$x^N - 1 = (x - 1)(x^{N-1} + x^{N-2} + \ldots + x + 1).$$

Let $a$ be the non-zero configuration $x^{N-1} + x^{N-2} + \ldots + x + 1 + (x^N - 1)R[x]$, then $\mathbb{T}a = 0$ so $\mathbb{T}$ is not a unit and the rule is not reversible. If $N = 1$ then clearly all configurations are mapped to zero in one time step. ♦

We may characterise the behaviour of rules on $N$ cells by the behaviour of their representatives as elements of $R_N$. We have already seen that a rule is reversible on $N$ cells if and only if its representative $\mathbb{T}$ is a unit in $R_N$. The next lemma is a collection of similar results.

**Lemma 2.1.5**

(i) *Suppose* $\mathbb{T} \in R_N$ *is a unit, then the units in* $R_N$ *lie on cycles of length* $\Pi_N(\mathbb{T})$ *under* $\mathbb{T}$ *and these cycles consist entirely of units.*

(ii) *Suppose* $\mathbb{T} \in R_N$ *is a zero-divisor, then any unit in* $R_N$ *has no predecessors under* $\mathbb{T}$.

(iii) *If* $R_N$ *contains non-zero nilpotent elements, then if under some* $\mathbb{T}$ *a cycle contains a non-zero nilpotent element all the elements on that cycle are nilpotent and, if* $\mathbb{T}$ *is a non-nilpotent zero-divisor, the trees rooted at nilpotent elements of* $Att(\mathbb{T})$ *(including* 0*) contain no units. The set of nilpotent elements on cycles is an ideal of* $R_N$.

Proof:

(i) $\mathbb{T}$ is a unit, let $a \in R_N$ be a unit, then $\mathbb{T}^{\Pi_N(\mathbb{T})}a = a$, if $l < \Pi_N(\mathbb{T})$ then $\mathbb{T}^l a = a$ implies that (on multiplying both sides by $a^{-1}$) $\mathbb{T}^l = 1$, contradicting the minimality

of $\Pi_N(\mathbb{T})$, hence for any unit $a$, $(\phi_a)_0 = \Pi_N(\mathbb{T})$. Let $a$ be a unit, then any element in $C_0(a)$ is of the form $\mathbb{T}^j a$ where $0 \leq j < \Pi_N(\mathbb{T})$. Then $\mathbb{T}^{\Pi_N(\mathbb{T})-j}a^{-1}$ is an inverse for $\mathbb{T}^j a$, thus any element on a cycle containing a unit is a unit.

(ii) $\mathbb{T}$ is a zero-divisor, suppose $u$ is a unit and $\mathbb{T}a = u$ for some $a \in R_N$, then $(\mathbb{T}a)u^{-1} = 1$ so $\mathbb{T}a$ is a unit, but $\mathbb{T}$ is a zero-divisor, so there is some $b \neq 0$ such that $\mathbb{T}b = 0$, hence $(\mathbb{T}a)b = 0$ so $\mathbb{T}a$ is a zero-divisor, a contradiction, hence there is no $a \in R_N$ such that $\mathbb{T}a = u$.

(iii) Suppose $a \in Att(\mathbb{T})$, $a \neq 0$ but $a^l = 0$, some integer $l > 0$. Then $(\mathbb{T}^i a)^l = \mathbb{T}^{il}a^l = 0$ for $0 \leq i < (\phi_a)_0$, so each element of $C_0(a)$ is nilpotent.

Now suppose $\mathbb{T}$ is a non-nilpotent zero-divisor, and let $a$ be any nilpotent element of $Att(\mathbb{T})$, $a^l = 0$, $l \geq 0$. Suppose $u \in R_N$ is a unit, and that $u \in T_0(\mathbb{T}, a)$, then $\mathbb{T}^t u = a$ for some $t \geq 1$, so $\mathbb{T}^{tl}u^l = 0$ so (as $u$ is a unit) we must have $\mathbb{T}^{tl} = 0$ so $\mathbb{T}$ is nilpotent, a contradiction. Thus $T_0(\mathbb{T}, a)$ contains no units if $a$ is nilpotent.

Let $\mathfrak{n}$ be the set of nilpotent elements on cycles under $\mathbb{T}$. Then $\mathfrak{n}$ is not empty as it contains 0. The sum of two nilpotent elements is a nilpotent element, by lemma A.1.2, and if $a, b \in \mathfrak{n}$ with $(\phi_a)_0 = k_1$ and $(\phi_b)_0 = k_2$, then let $k = \text{lcm}(k_1, k_2)$, then $\mathbb{T}^k(a+b) = a + b$ so $a + b \in \mathfrak{n}$. Let $a \in \mathfrak{n}$, with $a^l = 0$, $l > 0$ and $k = (\phi_a)_0$, then for any $c \in R_N$, $(ca)^l = c^l a^l = 0$ and $\mathbb{T}^k ca = \mathbb{T}^k ac = ac$ hence $ca \in \mathfrak{n}$. Thus $\mathfrak{n}$ is an ideal of $R_N$. ■

Using lemma 2.1.5 we can obtain a result about the non-occurrence of cycles of length $|R_N| - 1$ for linear cellular automata.

**Theorem 2.1.1** *An additive cellular automata over a finite commutative ring $R$ with periodic boundary conditions on $N > 1$ cells cannot have a cycle of length $|R_N| - 1$.*

Proof:

Let $\mathbb{T} \in R_N$, $N > 1$, represent an additive cellular automata, if $\mathbb{T}$ is not a unit then the number of elements on cycles is less than $|R_N| - 1$ so it suffices to consider $\mathbb{T}$ a unit. By lemma 2.1.5, (i), any unit is on a cycle under $\mathbb{T}$ consisting entirely of units, thus if there is a cycle of length $|R_N| - 1$ then all non-zero elements of $R_N$ are units so $R_N$ is a field, but for $N > 1$ the elements $x - 1 + (x^N - 1)R[x]$ and $x^{N-1} + x^{N-2} + \ldots + x + 1 + (x^N - 1)R[x]$ are non-trivial zero-divisors so $R_N$ cannot be a field, hence there can be no cycle of length $|R_N| - 1$. ■

Note that when $N = 1$ a cycle of length $|R| - 1$ will occur if and only if $R$ is a finite field and $\mathbb{T}$ is a primitive element of $R$, *i.e.* a generator of the (cyclic) group of units in $R$.

On seeing lemma 1.5.3 and corollary 1.5.1 it is natural to search for generalisations of these results to the case where $R$ is any finite commutative ring, such generalisations are easily found:

**Lemma 2.1.6** *For any finite commutative ring $R$, any integer $N > 0$ and any $\mathbb{T} \in R_N$ a configuration $a \in R_N$ has a predecessor under $\mathbb{T}^j$ if and only if $a(x) \in (x^N - 1, \mathbb{T}(x)^j)$, the ideal of $R[x]$ generated by $x^N - 1$ and $\mathbb{T}(x)^j$.*

Proof:

If $a \in R_N$ has a predecessor $b$ under $\mathbb{T}^j$ we have

$$a(x) = \mathbb{T}^j(x)b(x) - g(x)(x^N - 1)$$

for some $g(x) \in R[x]$, hence $a(x) \in (x^N - 1, \mathbb{T}^j(x))$. Conversely, if $a \in (x^N - 1, \mathbb{T}^j(x))$ then there are $e(x)$ and $f(x)$ in $R[x]$ such that

$$a(x) = \mathbb{T}^j(x)e(x) + (x^N - 1)f(x)$$

so $a = \mathbb{T}^j e$ in $R_N$, so $e = e(x) + (x^N - 1)R[x]$ is a predecessor of $a$ under $\mathbb{T}^j$. ■

**Corollary 2.1.2** *$\mathbb{T}$ is a unit in $R_N$ if and only if $(x^N - 1, \mathbb{T}(x)) = R[x]$.*

Proof:

Let $\mathbb{T}$ be a unit in $R_N$ then by lemma 2.1.6 $a(x) \in (x^N - 1, \mathbb{T}^j(x))$ for all $a \in R_N$, so $1 \in (x^N - 1, \mathbb{T}^j(x))$ so $(x^N - 1, \mathbb{T}(x)) = R[x]$. Conversely if $(x^N - 1, \mathbb{T}(x)) = R[x]$, then there are $e(x)$ and $f(x)$ in $R[x]$ such that

$$1 = \mathbb{T}(x)e(x) + (x^N - 1)f(x)$$

so in $R_N$ we have $1 = \mathbb{T}e$ hence $\mathbb{T}$ is a unit with $\mathbb{T}^{-1}$ given by $e$. ■

The following remark is sometimes useful:

**Remark 2.1.3** *For given $R, N$ and $\mathbb{T}$ and any $a \in R_N$, $\sum_{b \in C_0(a)} b$ is fixed by $\mathbb{T}$. Similarly for null boundary conditions and hybrids.*

Proof:

Let $c \in C_0(a)$, then

$$\sum_{b \in C_0(a)} b = \sum_{i=0}^{(\phi_a)_0 - 1} \mathbb{T}^i c.$$

Then

$$\mathbb{T}\sum_{b\in C_0(a)} b = \mathbb{T}\sum_{i=0}^{(\phi_a)_0-1}\mathbb{T}^i c = \sum_{i=0}^{(\phi_a)_0-1}\mathbb{T}^{i+1}c = \sum_{j=1}^{(\phi_a)_0}\mathbb{T}^j c + c = \sum_{i=0}^{(\phi_a)_0-1}\mathbb{T}^i c. \quad \blacksquare$$

### 2.1.3 Basic properties when $U \neq 0$

In this section we concentrate on systems of the form (1.5.20) (or (1.5.22)), (1.5.24) and (1.5.25), *i.e.* finite linear cellular automata (or hybrid cellular) automata with time independent inputs. We begin with a collection of mostly tedious but useful results.

We note first that the orbit of a configuration $a \in R_N$ under $\mathbb{T}_U$ can be described in terms of its orbit under $\mathbb{T}$ and the orbit of 0 under $\mathbb{T}_U$:

**Remark 2.1.4** *For given $R, N$ and $\mathbb{T}$ and each $U \in R_N$ and all $t \geq 0$*

$$\mathbb{T}_U^t(a) = \mathbb{T}^t a + \mathbb{T}_U^t(0).$$

*Similarly for null boundary conditions one has*

$$\mathbb{T}_{\mathbf{U}}^t(a) = \mathbf{T}^t\mathbf{a} + \mathbb{T}_{\mathbf{U}}^t(\mathbf{0}).$$

*and for hybrids*

$$\mathfrak{T}_{\mathbf{U}}^t(\mathbf{a}) = \mathfrak{T}^t\mathbf{a} + \mathfrak{T}_{\mathbf{U}}^t(\mathbf{0}). \quad \blacksquare$$

Note that for all $\mathbb{T} \in R_N \setminus \{0\}$ and all $U \in R_N$ one has that

$$\mathbb{T}_U^t(0) = \mathbb{T}_1^t(0)U \tag{2.1.2}$$

for each $t \geq 0$.

The next two lemmas are catalogues of easy results which will be used without reference in the rest of this chapter and those proceeding it.

**Lemma 2.1.7** *For given $R, N$ and $\mathbb{T} \in R_N$ and positive integers $t, k$ let $U, V, a, b \in R_N$, then*

(i) $\mathbb{T}_V^k(0) \pm \mathbb{T}_U^k(0) = \mathbb{T}_{V\pm U}^k(0)$;

(ii) $\mathbb{T}_U^{k+t}(0) - \mathbb{T}_U^t(0) = \mathbb{T}^t\mathbb{T}_U^k(0)$;

(iii) $\mathbb{T}_{-U}^k(0) = -\mathbb{T}_U^k(0)$;

(iv) $\mathbb{T}_V^t(\mathbb{T}_U^k(0)) = \mathbb{T}_U^{k+t}(0) + \mathbb{T}_V^t(0) - \mathbb{T}_U^t(0)$;

(v) $\mathbb{T}_V^k(a \pm b) = \mathbb{T}_V^k(a) \pm \mathbb{T}^k b = \mathbb{T}^k a + \mathbb{T}_V^k(\pm b)$;

(vi) $\mathbb{T}_{V\pm U}^k(a+b) = \mathbb{T}_V^k(a) + \mathbb{T}_{\pm U}^k(b)$.

*The obvious analogues hold for null boundary conditions and hybrids.* ■

**Lemma 2.1.8** *For given $R, N$ and $\mathbb{T} \in R_N$, let $U, V \in R_N$ and let $k \in \mathbb{N}$. Then*

(i) $\mathbb{T}_U$ *has a period $k$ orbit if and only if $\mathbb{T}_{-U}$ has a period $k$ orbit and such an orbit is of prime period $k$ for $\mathbb{T}_U$ if and only if the corresponding orbit has prime period $k$ under $\mathbb{T}_{-U}$.*

(ii) *If $\mathbb{T}_V$ and $\mathbb{T}_U$ have period $k$ orbits then $\mathbb{T}_{V+U}$ and $\mathbb{T}_{V-U}$ have period $k$ orbits (not necessarily prime).*

(iii) *If $\mathbb{T}_V$ has a period $k$ orbit but $\mathbb{T}_U$ does not then $\mathbb{T}_{V-U}$ and $\mathbb{T}_{V+U}$ do not have period $k$ orbits.*

(iv) *The obvious analogues of* (i), (ii) *and* (iii) *hold for null boundary conditions and hybrids.* ■

The equality (2.1.2) suggest that $(\phi_0)_U$ is related to $(\phi_0)_1$ for all $U \in R_N$. We have the following result.

**Lemma 2.1.9** *For given $R, N$ and $\mathbb{T}$ and any $U \in R_N$*

$$(\phi_0)_U | (\phi_0)_1.$$

*Similarly for null boundary conditions and hybrids.*

Proof:

Let $(\phi_0)_1 = L$, then

$$\mathbb{T}_1^{T+L}(0) = \mathbb{T}_1^T(0) \;\Rightarrow\; \mathbb{T}_1^{T+L}(0)U = \mathbb{T}_1^T(0)U \;\Rightarrow\; \mathbb{T}_U^{T+L}(0) = \mathbb{T}_U^T(0)$$

hence $(\phi_0)_U | (\phi_0)_1$ by lemma 2.1.1. ■

The existence or not of fixed points under $\mathbb{T}_U$ is important, as we shall see in section 2.3. The next result gives a necessary and sufficient condition for $\mathbb{T}_U$ to have a fixed point.

**Lemma 2.1.10** *For given $R, N, \mathbb{T}$ and any $U \in R_N$ there is a cycle of length 1 under $\mathbb{T}_U$ if and only if $U \in (\mathbb{T} - 1)R_N$. Moreover each element $a \in R_N$ is a fixed point of $\mathbb{T}_U$ for exactly one $U \in R_N$.*

Proof:

One has:

$$\mathbb{T}_U(a) = a \;\Leftrightarrow\; \mathbb{T}a + U = a \;\Leftrightarrow\; (\mathbb{T} - 1)a = -U \;\Leftrightarrow\; U \in (\mathbb{T} - 1)R_N.$$

Suppose that $\mathbb{T}_U(a) = a$ and that $\mathbb{T}_V(a) = a$. Then

$$-U = (\mathbb{T} - 1)a = -V \;\Rightarrow\; U = V.$$

So each $a \in R_N$ is fixed by $\mathbb{T}_U$ for at most one $U \in R_N$, but for any $a \in R_N$ let $V(a) = a - \mathbb{T}a$ then $a$ is a fixed point of $\mathbb{T}_{V(a)}$. ■

We can generalise the above to periods greater than 1:

**Lemma 2.1.11** *For given $R, N$ and any $\mathbb{T}, U, V \in R_N$ and any integer $k > 0$ we have:*

(i) $Cyc(\mathbb{T}_U, k) \neq \emptyset \;\Leftrightarrow\; \mathbb{T}_U^k(0) \in (\mathbb{T}^k - 1)R_N$.

(ii) *If $a \in R_N$ is on a period $k$ orbit under both $\mathbb{T}_U$ and $\mathbb{T}_V$ then $\mathbb{T}_{U-V}^k(0) = 0$.*

Proof:

Part (i) is similar to the first part of lemma 2.1.10, for part (ii) let $a \in R_N$ be such that $\mathbb{T}_U^k(a) = \mathbb{T}_V^k(a) = a$. Then $\mathbb{T}_U^k(0) = \mathbb{T}_V^k(0)$ hence $\mathbb{T}_{U-V}^k(0) = 0$. ■

Lemmas 2.1.10 and 2.1.11 hold for null boundary conditions and hybrids with $(\mathbb{T}^k - 1)R_N$ replaced by the image of $R^N$ under the $R$-module endomorphisms $\mathbf{T}^k - \mathbf{I}$ or $\mathfrak{T}^k - \mathbf{I}$, a submodule of $R^N$.

**Lemma 2.1.12** *For given $R, N$ and $\mathbb{T}$ let $a \in R_N$ and $d = lcm((\phi_a)_0, (\phi_0)_U)$, then*

$$(\phi_a)_U | d.$$

*Moreover one has*

$$\text{(i)} \quad (\phi_a)_U | (\phi_0)_U \;\Leftrightarrow\; (\phi_a)_0 | (\phi_0)_U;$$

$$\text{(ii)} \quad (\phi_a)_U | (\phi_a)_0 \;\Leftrightarrow\; (\phi_0)_U | (\phi_a)_0;$$

$$\text{(iii)} \quad (\phi_0)_U | (\phi_a)_U \;\Leftrightarrow\; (\phi_a)_0 | (\phi_a)_U.$$

*Similarly for null boundary conditions and hybrids.* ■

The proof of lemma 2.1.12 can be found in appendix B. Note that lemma 2.1.12, (i), implies that if $U \in R_N$ is such that $\Pi_N(\mathbb{T}) | (\phi_0)_U$ then $(\phi_a)_U | (\phi_0)_U$ for all $a \in R_N$.

For any $a \in R_N$ we can bound $(\phi_a)_U$ in terms of $\Pi_N(\mathbb{T})$ and the characteristic of $R$.

**Lemma 2.1.13** *For given $R, N$ and $\mathbb{T}$ and any $a, U \in R_N$, let $c$ be the characteristic of $R$, then*

$$(\phi_0)_U | c(\phi_U)_0 \quad \textit{and} \quad (\phi_a)_U | c\Pi_N(\mathbb{T}).$$

*Similarly for null boundary conditions and hybrids.*

Proof:

We have that

$$\begin{aligned}\mathbb{T}_U^{T+(\phi_U)_0}(0) &= (\mathbb{T}^{(\phi_U)_0-1}+\ldots+1)\mathbb{T}^T U + \mathbb{T}_U^T(0)\\ &= F + \mathbb{T}_U^T(0)\end{aligned}$$

where $F = (\mathbb{T}^{(\phi_U)_0-1}+\ldots+1)\mathbb{T}^T U$ is a fixed point of $\mathbb{T}$ by remark 2.1.3, then

$$\begin{aligned}\mathbb{T}_U^{T+2(\phi_U)_0}(0) &= 2F + \mathbb{T}_U^T(0)\\ \vdots &\quad \vdots\\ \mathbb{T}_U^{T+c(\phi_U)_0}(0) &= cF + \mathbb{T}_U^T(0)\\ &= \mathbb{T}_U^T(0),\end{aligned}$$

hence $(\phi_0)_U | c(\phi_U)_0$. In particular $(\phi_0)_1 | c\Pi_N(\mathbb{T})$ and by lemma 2.1.9 $(\phi_0)_U | (\phi_0)_1$ for all $U \in R_N$, hence for all $a \in R_N$

$$\mathbb{T}_U^{T+c\Pi_N(\mathbb{T})}(a) = \mathbb{T}^{T+c\Pi_N(\mathbb{T})}a + \mathbb{T}_U^{T+c\Pi_N(\mathbb{T})}(0) = \mathbb{T}^T a + \mathbb{T}_U^T(0) = \mathbb{T}_U^T(a),$$

hence $(\phi_a)_U | c\Pi_N(\mathbb{T})$. ■

## 2.2 Structure of the state transition graph

We begin with the generalisation of theorem 1.5.2 to allow constant inputs. First we introduce some notation. For given $R, N$ and $\mathbb{T}$ and some $U \in R_N$, let $r \in Att(\mathbb{T}_U)$, then there is a unique element in $C_U(r)$ that is a predecessor of $r$ under $\mathbb{T}_U^t$ for any positive integer $t$. Denote this element by $r^{-t}$, $r^{-t} \in C_U(r) \subseteq Att(\mathbb{T}_U)$ and $\mathbb{T}_U^t(r^{-t}) = r^0 = r$. Thus if $0 \leq s < t$ then

$$r^{-s} = \mathbb{T}_U^{t-s}(r^{-t}).$$

We shall make use of a device introduced for $U = 0$ by Martin *et al.* and define a map $\Psi_{U,r} : T_0(\mathbb{T}, 0) \longrightarrow T_U(\mathbb{T}, r)$ by

$$a \mapsto a + r^{-t} \tag{2.2.1}$$

where $t$ is the least integer such that $\mathbb{T}^t a = 0$. We make the obvious analogous definition for null boundary conditions and hybrids. The proof of the following theorem is essentially a catalogue of the properties of $\Psi_{U,r}$.

**Theorem 2.2.1** *For any one dimensional additive cellular automata represented by* $\mathbb{T}$ *over* $R$ *on* $N$ *cells, the trees rooted at each element of* $Att(\mathbb{T}_U)$ *are identical to one another and to the tree rooted at 0 under* $\mathbb{T}$ *for each* $U \in R_N$. *Similarly for null boundary conditions and hybrids.*

Proof:

We show that (a) $\Psi_{U,r}(0) = r, \mathbb{T}_U^t(\Psi_{U,r}(a)) = r$; (b) $\Psi_{U,r}$ maps configurations at height t in $T_0(\mathbb{T}, 0)$ to configurations at height t in $T_U(\mathbb{T}, r)$; (c) $\Psi_{U,r}$ is injective; (d) $\Psi_{U,r}$ maps configurations with no predecessors under $\mathbb{T}$ to configurations with no predecessors under $\mathbb{T}_U$; (e) $\Psi_{U,r}$ is surjective; (f) $\Psi_{U,r}$ preserves the time evolution structure of the tree.

(a) $\Psi_{U,r}(0) = 0 + r^0 = r$. Let $t > 0$, $\Psi_{U,r}(a) = a + r^{-t}$ then

$$\mathbb{T}_U^t(\Psi_{U,r}(a)) = \mathbb{T}^t(a + r^{-t}) + \mathbb{T}_U^t(0) = \mathbb{T}^t a + \mathbb{T}^t r^{-t} + \mathbb{T}_U^t(0) = 0 + r^0 = r.$$

Thus as $a$ ranges over all configurations in $T_0(\mathbb{T}, 0)$, $\Psi_{U,r}(a)$ ranges over all configurations in $T_U(\mathbb{T}, r)$.

(b) Suppose there is some $m \neq 0,\ m < t$ such that

$$r^{-m} = \mathbb{T}_U^s(\Psi_{U,r}(a)) = \mathbb{T}^s a + r^{s-t},\ s < t \tag{2.2.2}$$

then

$$\mathbb{T}_U^{t-s}(r^{-m}) = \mathbb{T}^{t-s}\mathbb{T}^s a + \mathbb{T}^{t-s} r^{s-t} + \mathbb{T}_U^{t-s}(0) = \mathbb{T}^t a + r^0 = r \tag{2.2.3}$$

*i.e.* $r^{t-s-m} = r$.

Let $k = |C_U(r)|$, then (2.2.3) implies that

$$t - s - m = nk,\quad n \in \mathbb{Z} \Rightarrow\ -m = s - t + nk \Rightarrow\ r^{-m} = r^{s-t+nk} = r^{s-t},$$

then (2.2.2) implies $0 = r^{-m} - r^{s-t} = \mathbb{T}^s a, s < t$, which contradicts the assumption that $t$ is the smallest positive integer such that $\mathbb{T}^s a = 0$. This together with (a) proves (b).

(c) Let $a, b \in T_0(\mathbb{T}, 0)$. If $\Psi_{U,r}(a) = \Psi_{U,r}(b)$ then $a$ and $b$ must be at the same height $t$ in $T_0(\mathbb{T}, 0)$ by (b) so

$$a + r^{-t} = b + r^{-t} \Rightarrow\ a = b,$$

hence $\Psi_{U,r}$ is injective.

(d) Let $a$ be a configuration with no predecessors under $\mathbb{T}$ that goes to 0 in $s$ time steps under $\mathbb{T}$, then for some $b \in T_U(\mathbb{T}, r)$

$$\Psi_{U,r}(a) = a + r^{-s} = b.$$

Suppose $b$ has a predecessor, $b'$, under $\mathbb{T}_U$:

$$b = \mathbb{T}_U(b') = \mathbb{T}b' + U$$

then

$$a + r^{-s} = \mathbb{T}b' + U \;\Rightarrow\; a = \mathbb{T}b' + U - r^{-s} = \mathbb{T}b' + U - \mathbb{T}r^{-s-1} - U = \mathbb{T}(b' + r^{-s-1})$$

which implies that $a$ has a predecessor, a contradiction, so $b$ has no predecessors.

(e) Let $b$ be at height $t$ in $T_U(\mathbb{T}, r)$ and suppose that $b \neq \Psi_{U,r}(a)$ for any $a \in T_0(\mathbb{T}, 0)$. There must be some minimal $s$, $0 < s \leq t$, such that

$$\mathbb{T}_U^s(b) = \Psi_{U,r}(a'), \text{ some } a' \in T_0(\mathbb{T}, 0). \tag{2.2.4}$$

If $a$ has no predecessors then, by (d), neither does $\mathbb{T}_U^s(b)$. This contradiction implies that $a$ has at least one predecessor, say $a''$, and hence

$$\begin{aligned}
\Psi_{U,r}(\mathbb{T}a'') &= \mathbb{T}_U^s(b) \\
\Rightarrow\; \mathbb{T}a'' + r^{-v} &= \mathbb{T}\mathbb{T}_U^{s-1}(b) + U,\; v = t - s \\
\Rightarrow\; 0 &= \mathbb{T}a'' + r^{-v} - \mathbb{T}\mathbb{T}_U^{s-1}(b) - U \\
\Rightarrow\; 0 &= \mathbb{T}a'' + \mathbb{T}r^{-v-1} - \mathbb{T}\mathbb{T}_U^{s-1}(b) \\
\Rightarrow\; 0 &= \mathbb{T}(a'' + r^{-v-1} - \mathbb{T}_U^{s-1}(b)) \\
\Rightarrow\; c &= a'' + r^{-v-1} - \mathbb{T}_U^{s-1}(b),
\end{aligned}$$

where $\mathbb{T}c = 0$. Thus

$$\mathbb{T}_U^{s-1}(b) = a'' - c + r^{-v-1}.$$

Now, $\mathbb{T}^{t-s+1}(a'' - c) = \mathbb{T}^{t-s+1}a'' + 0$ and $a''$ is at height $t - s + 1$ so

$$\mathbb{T}^{t-s+1}(a'' - c) = 0 \;\Rightarrow\; a'' - c + r^{-v-1} = a'' - c + r^{s-t+1} = \Psi_{U,r}(a'' - c),$$

thus

$$\mathbb{T}_U^{s-1}(b) = \Psi_{U,r}(a'' - c). \tag{2.2.5}$$

Equation (2.2.5) contradicts the minimality of $s$, thus we have for all $b \in T_U(\mathbb{T}, r)$ there is some $a \in T_0(\mathbb{T}, 0)$ such that $b = \Psi_{U,r}(a)$, hence $\Psi_r$ is surjective.

(f) Let $a \in T_0(\mathbb{T}, 0)$ be such that $\mathbb{T}^t a = 0$, then

$$\begin{aligned} \mathbb{T}_U(\Psi_{U,r}(a)) &= \mathbb{T}a + \mathbb{T}r^{-t} + U \\ &= a' + r^{-t+1}, \text{where } a' = \mathbb{T}a \\ &= \Psi_{U,r}(a') \end{aligned}$$

$$\text{so } \mathbb{T}_U(\Psi_{U,r}(a)) = \Psi_{U,r}(\mathbb{T}(a)).$$

Thus$\Psi_{U,r}$ is a bijection which preserves dynamical structure, this proves the theorem. ■

We note that the above proof can be summed up by saying that we have shown that $\Psi_{U,r}$ is a structure preserving bijection from $T_0(\mathbb{T}, 0)$ to $T_U(\mathbb{T}, r)$ for all $U \in R_N$ and each $r \in Att(\mathbb{T}_U)$. Also note that the proof of the above theorem also shows that $R_N \cong T_0(\mathbb{T}, 0) \oplus Att(\mathbb{T})$ as an $R_N$ module for each $\mathbb{T} \in R_N$.

**Corollary 2.2.1** *For given $R, N$ and $\mathbb{T} \in R_N$ and any $U \in R_N$*

$$|Att(\mathbb{T}_U)| = |Att(\mathbb{T})|.$$

*Similarly for null boundary conditions and hybrids.*

Proof:

By theorem 2.2.1 $|T_U(\mathbb{T}, r)| = |T_0(\mathbb{T}, 0)|$ for all $U \in R_N$ and each $r \in Att(\mathbb{T}_U)$. When $U = 0$ it is clear that

$$|R_N| = |T_0(\mathbb{T}, 0)||Att(\mathbb{T})|$$

and for non-zero $U$ it is clear that

$$|R_N| = |T_U(\mathbb{T}, r)||Att(\mathbb{T}_U)|$$

as the trees are all identical. Thus

$$|T_0(\mathbb{T}, 0)||Att(\mathbb{T})| = |T_U(\mathbb{T}, r)||Att(\mathbb{T}_U)| = |T_0(\mathbb{T}, 0)||Att(\mathbb{T}_U)|$$

hence $|Att(\mathbb{T}_U)| = |Att(\mathbb{T})|$. ■

Corollary 2.2.1 suggests that the distinct invariant sets occurring for $\mathbb{T}_U$ as $U$ runs through $R_N$ might be related to the quotient ring $R_N/Att(\mathbb{T})$ (or quotient module $R^N/Att(\mathbf{T})$ *etc.*). This is in fact the case.

**Theorem 2.2.2** *The distinct invariant sets that can occur for the additive cellular automata represented by* $\mathbb{T} \in R_N$ *on* $N$ *cells with constant input* $U \in R_N$ *are the elements of* $R_N/Att(\mathbb{T})$ *with*

$$Att(\mathbb{T}_U) = \alpha + Att(\mathbb{T})$$

*where* $\alpha$ *is any element of* $Att(\mathbb{T}_U)$. *Similarly for null boundary conditions and hybrids.*

Proof:

Let $\alpha \in Att(\mathbb{T}_U)$, $\alpha + Att(\mathbb{T}) = \{\alpha + b : b \in Att(\mathbb{T})\}$. For each $b \in Att(\mathbb{T})$ let $k = \text{lcm}((\phi_\alpha)_U, (\phi_b)_0)$. Then

$$\mathbb{T}_U^k(\alpha + b) = \mathbb{T}_U^k(\alpha) + \mathbb{T}^k b = \alpha + b.$$

Hence $\alpha + Att(\mathbb{T}) \subseteq Att(\mathbb{T}_U)$, but, by corollary 2.2.1, $|Att(\mathbb{T}_U)| = |Att(\mathbb{T})|$, hence $Att(\mathbb{T}_U) = \alpha + Att(\mathbb{T})$. ■

Thus the elements of $Att(\mathbb{T}_U)$ can be found from those of $Att(\mathbb{T})$ by translation by any particular element of $Att(\mathbb{T}_U)$. In practice it is often convenient to take $\alpha = \mathbb{T}_U^T(0)$. The fact that distinct cosets are disjoint tells us that if $U \neq V$ then either $Att(\mathbb{T}_U) \cap Att(\mathbb{T}_V) = \emptyset$ or $Att(\mathbb{T}_U) = Att(\mathbb{T}_V)$. Of course theorem 2.2.2 tells us nothing about the dynamical structure of $Att(\mathbb{T}_U)$.

**Corollary 2.2.2** *For given* $R, N$ *and* $\mathbb{T}$ *and any* $U, V \in R_N$ *and any* $\alpha \in Att(\mathbb{T}_U)$ *and any* $\beta \in Att(\mathbb{T}_V)$

$$Att(\mathbb{T}_U) = \alpha - \beta + Att(\mathbb{T}_V).$$

*Similarly for null boundary conditions and hybrids.*

Proof:

$Att(\mathbb{T}_U) = \alpha + Att(\mathbb{T})$ and $Att(\mathbb{T}_V) = \beta + Att(\mathbb{T})$ hence $Att(\mathbb{T}) = Att(\mathbb{T}_V) - \beta$ so $Att(\mathbb{T}_U) = \alpha - \beta + Att(\mathbb{T}_V)$. ■

There is a similar relation between $R_N/Cyc(\mathbb{T}, k)$ and $Cyc(\mathbb{T}_U, k)$ for those $U$ such that $\mathbb{T}_U$ has period $k$ orbits.

**Lemma 2.2.1** *For given* $R, N$ *and* $\mathbb{T}$ *if there is a period* $k$ *orbit under* $\mathbb{T}_U$ *with, say,* $(\phi_a)_U | k$ *for some* $a \in Att(\mathbb{T}_U)$ *then*

$$Cyc(\mathbb{T}_U, k) = a + Cyc(\mathbb{T}, k).$$

*Similarly for hybrids and null boundary conditions.*

Proof:

This is a simple verification. ■

One can easily show that if there are $a \in Att(\mathbb{T}_U)$ and $b \in Att(\mathbb{T}_V)$ such that $(\phi_a)_U|k$ and $(\phi_b)_V|k$ then

$$Cyc(\mathbb{T}_U, k) = a - b + Cyc(\mathbb{T}_V, k). \tag{2.2.6}$$

Note that these results do not say that there will be period $k$ orbits for any $k > 0$ and any $U$, one has to find a period $k$ orbit under $\mathbb{T}_U$ to apply them. Also, even if one has an $a \in Att(\mathbb{T}_U)$ with $(\phi_a)_U = k$ this does not guarantee that every element of $a + Cyc(\mathbb{T}, k)$ has prime period $k$, some elements may be on orbits whose lengths are proper divisors of $k$.

The next result gives a set of equivalent conditions for different inputs to yield the same invariant set, its proof can be found in appendix B.

**Lemma 2.2.2** *For given $R, N$ and $\mathbb{T}$ and any $U, V \in R_N$ the following statements are equivalent.*

(i) $Att(\mathbb{T}_U) \cap Att(\mathbb{T}_V) \neq \emptyset$;

(ii) $Att(\mathbb{T}_U) = Att(\mathbb{T}_V)$;

(iii) $U - V \in Att(\mathbb{T})$;

(iv) $0 \in C_{U-V}(0)$;

(v) $Att(\mathbb{T}) = Att(\mathbb{T}_{U-V})$.

*Similarly for null boundary conditions and hybrids.* ■

The following result is immediate on putting $V = 0$ in the above.

**Corollary 2.2.3** *For given $R, N$ and $\mathbb{T}$ and any $U \in R_N$ one has*

$$Att(\mathbb{T}) = Att(\mathbb{T}_U) \Leftrightarrow 0 \in C_U(0) \Leftrightarrow U \in Att(\mathbb{T})$$

*Similarly for null boundary conditions and hybrids.* ■

**Remark 2.2.1** *When $U \in Att(\mathbb{T})$, $(\phi_U)_0|(\phi_0)_U$.*

Proof:

When $U \in Att(\mathbb{T})$ one has $\mathbb{T}_U^{(\phi_0)_U}(0) = 0$ hence

$$(\mathbb{T}^{(\phi_0)_U - 1} + \ldots + \mathbb{T} + 1)U = 0,$$

So applying $\mathbb{T}_U$ to both sides of the above yields

$$\begin{aligned} \mathbb{T}(\mathbb{T}^{(\phi_0)_U-1}+\ldots+\mathbb{T}+1)U+U &= U \\ \Rightarrow \quad \mathbb{T}^{(\phi_0)_U}U+(\mathbb{T}^{(\phi_0)_U-1}+\ldots+\mathbb{T}+1)U &= U \\ \Rightarrow \quad \mathbb{T}^{(\phi_0)_U}U &= U, \end{aligned}$$

hence $(\phi_U)_0|(\phi_0)_U$. ■

**Corollary 2.2.4** *For given $R, N$ and $\mathbb{T}$ and any $U \in R_N$ there are $|Att(\mathbb{T})|-1$ elements $U' \in R_N$ such that $U' \neq U$ but $Att(\mathbb{T}_{U'}) = Att(\mathbb{T}_U)$. Similarly for null boundary conditions and hybrids.*

Proof:

By lemma 2.2.2 $Att(\mathbb{T}_U) = Att(\mathbb{T}_{U'})$ if and only if $U - U' \in Att(\mathbb{T})$. As $U'$ runs through $R_N$ there are exactly $|Att(\mathbb{T})|$ values of $U'$ such that $U - U' \in Att(\mathbb{T})$ and the result follows. ■

The next theorem relates the invariant sets for different inputs according to the positions of those inputs in the trees rooted at the elements of $Att(\mathbb{T})$ in the state transition graph for $\mathbb{T}$.

**Theorem 2.2.3** *Let $\mathbb{T}$ be a non-unit in $R_N$ and for each $r \in Att(\mathbb{T})$ let $\Psi_{0,r}$ be the structure preserving bijection defined by (2.2.1). Then*

(i) *For each $r \in Att(\mathbb{T})$ and any $U \in T_0(\mathbb{T}, 0)$*

$$Att(\mathbb{T}_U) = Att(\mathbb{T}_{\Psi_{0,r}(U)}).$$

(ii) *If $U, V \in T_0(\mathbb{T}, 0)$ and $U \neq V$ then*

$$Att(\mathbb{T}_U) \neq Att(\mathbb{T}_V).$$

(iii) *For each $r \in Att(\mathbb{T})$ and any $a \in T_0(\mathbb{T}, 0)$*

$$\Psi_{0,r}(a) + Att(\mathbb{T}) = a + Att(\mathbb{T}).$$

(iv) *If $a, b \in T_0(\mathbb{T}, 0)$ and $a \neq b$ then*

$$a + Att(\mathbb{T}) \neq b + Att(\mathbb{T}).$$

*Similarly for null boundary conditions and hybrids.*

Proof:

(i) Let $U$ be at height $t \geq 0$ in $T_0(\mathbb{T}, 0)$, let $r \in Att(\mathbb{T})$, then

$$\mathbb{T}_{U-\Psi_{0,r}(U)} = \mathbb{T}_{-r^{-t}}.$$

Now as $Att(\mathbb{T})$ is an ideal of $R_N$, $-r^{-t} \in Att(\mathbb{T})$ so by lemma 2.2.2 parts (ii) and (iii) we have $Att(\mathbb{T}_U) = Att(\mathbb{T}_{\Psi_{0,r}(U)})$.

(ii) By corollary 2.2.3 $Att(\mathbb{T}_U) = Att(\mathbb{T})$ if and only if $U \in Att(\mathbb{T})$ so there are $|Att(\mathbb{T})|$ such $U$ in $R_N$. Let $U \in T_0(\mathbb{T}, 0)$, by corollary 2.2.4 there are exactly $|Att(\mathbb{T})|$ elements of $R_N$ which have the invariant set $Att(\mathbb{T}_U)$, including $U$, and by part (i) above these elements are the $\Psi_{0,r}(U)$, $r \in Att(\mathbb{T})$. Hence if $V \in T_0(\mathbb{T}, 0)$ but $U \neq V$ then $Att(\mathbb{T}_U) \neq Att(\mathbb{T}_V)$.

(iii) Let $a$ be at height $t$ in $T_0(\mathbb{T}, 0)$, then

$$\begin{aligned} \Psi_{0,r}(a) + Att(\mathbb{T}) &= a + r^{-t} + Att(\mathbb{T}) \\ &= a + Att(\mathbb{T}) \end{aligned}$$

for each $r \in Att(\mathbb{T})$ as $r^{-t} \in Att(\mathbb{T})$.

(iv) This follows from (iii) in the same way that (ii) follows from (i) after noting that for any $a \in R_N$ there are exactly $|Att(\mathbb{T})|$ elements $b \in R_N$ (including $a$) such that $b + Att(\mathbb{T}) = a + Att(\mathbb{T})$. ■

In the light of the above theorem one can think of $T_0(\mathbb{T}, 0)$ as an "index" for the possible invariant sets, *i.e.* choosing distinct elements of $T_0(\mathbb{T}, 0)$ as inputs yields distinct invariant sets. Immediate consequences of theorem 2.2.3 are that $Att(\mathbb{T}_V) = Att(\mathbb{T}_U)$ for $U \in T_0(\mathbb{T}, 0)$ if and only if $V = \Psi_{0,r}(U)$ for some $r \in Att(\mathbb{T})$ and that $b + Att(\mathbb{T}) = a + Att(\mathbb{T})$ for some $a \in T_0(\mathbb{T}, 0)$ if and only if $b = \Psi_{0,r}(a)$ for some $r \in Att(\mathbb{T})$.

We note that, in general, for $a \in R_N$

$$a + Att(\mathbb{T}) \neq Att(\mathbb{T}_a).$$

However if $a \in Att(\mathbb{T})$ or is at height 1 then

$$a + Att(\mathbb{T}) = Att(\mathbb{T}_a).$$

To show this it suffices, by theorem 2.2.3, to show that it is true when $a \in T_0(\mathbb{T}, 0)$. This is clear when $a$ is at height 0 for then $a = 0$. When $a \in \mathbb{T}_0^1(\mathbb{T}, 0) \setminus \{0\}$ let $a + b \in a + Att(\mathbb{T})$ then

$$\mathbb{T}_a^{(\phi_b)_0}(a + b) = \mathbb{T}^{(\phi_b)_0}(b) + \mathbb{T}_a^{(\phi_b)_0}(0) = b + a,$$

which shows that $a + Att(\mathbb{T}) = Att(\mathbb{T}_a)$ as $|a + Att(\mathbb{T})| = |Att(\mathbb{T}_a)|$. In general we can show that if input $U$ is at height $t$ under $\mathbb{T}$ then $Att(\mathbb{T}_U) = a^* + Att(\mathbb{T})$ where $a^*$ is at height $t$ under $\mathbb{T}$. By theorem 2.2.3 it suffices to show this for $U \in T_0(\mathbb{T}, 0)$. Moreover we already know it is true for $0 \leq t \leq 1$. Let $U$ be at height $t > 1$ under $\mathbb{T}$. $\mathbb{T}_U^t(0) = (\mathbb{T}^{t-1} + \ldots + \mathbb{T} + 1)U$ which is clearly fixed by $\mathbb{T}_U$ so take $a^* = \mathbb{T}_U^t(0)$, now $\mathbb{T}^j\mathbb{T}_U^t(0) \neq 0$ for $0 \leq j < t$ and $\mathbb{T}^t\mathbb{T}_U^t(0) = 0$ hence $a^*$ is at height $t$ as required. Of course in general $\mathbb{T}_U^t(0) \neq U$.

## 2.3 Conditions for qualitative dynamical similarity

In this section we consider consider the question of when distinct inputs give qualitatively similar behaviour when applied with the same cellular automata rule. We first make clear what we mean by qualitatively similar behaviour.

**Definition 2.3.1** *For given $R, N$ and $\mathbb{T}$ we shall say that $Att(\mathbb{T}_U)$ and $Att(\mathbb{T}_V)$ are qualitatively dynamically similar* (QDS) *if the number of cycles of length $l$ occurring under $\mathbb{T}_U$ and the number of cycles of length $l$ occurring under $\mathbb{T}_V$ are the same. We shall say that $\mathbb{T}_U$ and $\mathbb{T}_V$ are* QDS *if $Att(\mathbb{T}_U)$ and $Att(\mathbb{T}_V)$ are* QDS. *Similarly for null boundary conditions and hybrids.*

Thus we say that the dynamical structure of $Att(\mathbb{T}_U)$ is qualitatively different from that of $Att(\mathbb{T}_V)$ if there is a cycle in $Cyc(\mathbb{T}_U)$ of a length not occurring in $Cyc(\mathbb{T}_V)$ (or vice versa) or if there are different numbers cycles of a particular length in $Cyc(\mathbb{T}_U)$ than in $Cyc(\mathbb{T}_V)$. It is clear that the relation $U \sim V$ if $\mathbb{T}_U$ and $\mathbb{T}_V$ are QDS is an equivalence relation on $R_N$ (or $R^N$). We can use the cycle set notation introduced in Chapter 1 to state definition 2.3.1 more succinctly as

$$\mathbb{T}_U \text{ and } \mathbb{T}_V \text{ are QDS } \Leftrightarrow \ \Sigma(\mathbb{T}_U) = \Sigma(\mathbb{T}_V). \tag{2.3.1}$$

The following lemma is fundamental to the rest of this section.

**Lemma 2.3.1** *Let $\phi : Att(\mathbb{T}_U) \longrightarrow Att(\mathbb{T}_V)$ be a bijection satisfying*

$$\mathbb{T}_V \circ \phi = \phi \circ \mathbb{T}_U,$$

*then $\phi$ induces a bijection $\Phi : Cyc(\mathbb{T}_U) \longrightarrow Cyc(\mathbb{T}_V)$ which preserves cycle lengths. Similarly for null boundary conditions and hybrids.*

Proof:

We show that if $\phi$ satisfies the conditions of the lemma then $\phi$ preserves orbit lengths and $\phi$ maps distinct orbits to distinct orbits. Let $b \in Att(\mathbb{T}_U)$, let $|C_U(b)| = k$ so $\mathbb{T}_U^k(b) = b$. Then

$$\mathbb{T}_V^k(\phi(b)) = \mathbb{T}_V^{k-1}(\phi(\mathbb{T}_U(b))) = \ldots = \phi(\mathbb{T}_U^k(b)) = \phi(b).$$

Hence $|\, C_V(\phi(b))\,| \;|\; k$. If $j < k$ and $\mathbb{T}_V^j(\phi(b)) = \phi(b)$ then $\phi(\mathbb{T}_U^j(b)) = \phi(b)$ and $\phi$ is a bijection so $\mathbb{T}_U^j(b) = b$ contradicting the minimality of $k$. Thus $\phi$ preserves orbit lengths. If $C_U(b_1) \neq C_U(b_2)$ then $C_U(b_1) \cap C_U(b_2) = \emptyset$ and hence the bijectivity of $\phi$ implies that distinct orbits are mapped to distinct orbits. The bijection $\Phi : Cyc(\mathbb{T}_U) \longrightarrow Cyc(\mathbb{T}_V)$ is constructed as follows: for each $C \in Cyc(\mathbb{T}_U)$ let $c \in C$, then $\Phi(C) = C_V(\phi(c))$. The above comments show that this map is well defined in the sense that it does not depend on the representative $c$ of $C$ chosen. ■

In the language of dynamical systems if there is a map $\phi$ satisfying the conditions of lemma 2.3.1 then $\mathbb{T}_U$ is conjugate to $\mathbb{T}_V$.

**Corollary 2.3.1** *If $\phi : Att(\mathbb{T}_U) \longrightarrow Att(\mathbb{T}_V)$ is a bijection satisfying*

$$\mathbb{T}_V \circ \phi = \circ \circ \mathbb{T}_U,$$

*then $\mathbb{T}_U$ and $\mathbb{T}_V$ are* QDS. *Similarly for null boundary conditions and hybrids.*

Proof:

This is immediate from lemma 2.3.1 and definition 2.3.1. ■

**Corollary 2.3.2** *If $\phi : R_N \longrightarrow R_N$ is a bijection satisfying $\mathbb{T}_V \circ \phi = \phi \circ \mathbb{T}_U$ then $\mathbb{T}_U$ and $\mathbb{T}_V$ are* QDS. *If $\phi$ is any mapping from $R_N$ to itself satisfying $\mathbb{T}_V \circ \phi = \phi \circ \mathbb{T}_U$ which when restricted to $Att(\mathbb{T}_U)$ is bijective with its image then $\mathbb{T}_U$ and $\mathbb{T}_V$ are* QDS. *Similarly for null boundary conditions and hybrids.*

Proof:

Let $\phi : R_N \longrightarrow R_N$ is a bijection satisfying $\mathbb{T}_V \circ \phi = \phi \circ \mathbb{T}_U$. Then if $b \in Att(\mathbb{T}_U)$ and $|C_U(b)| = k$ then, as in the proof of lemma 2.3.1. $\phi(b) \in Att(\mathbb{T}_V)$ as $\mathbb{T}_V^k(\phi(b)) = \phi(b)$. Thus $\phi(Att(\mathbb{T}_U)) = Att(\mathbb{T}_V)$ and $|Att(\mathbb{T}_U)| = |Att(\mathbb{T}_V)|$ and $\phi$ is a bijection hence $\phi$ satisfies the conditions of lemma 2.3.1 and the result follows from corollary 2.3.1. The second part is similar. ■

Given an additive cellular automata on $N$ cells with known behaviour we wish to know when the presence of a non-zero external input changes the qualitative dynamical behaviour.

**Theorem 2.3.1** *For given $R, N$ and $\mathbb{T}$ and any $U \in R_N$, $\mathbb{T}$ and $\mathbb{T}_U$ are* QDS *if and only if there is a cycle of length one under $\mathbb{T}_U$. Similarly for null boundary conditions and hybrids.*

Proof:

Clearly if $Fix(\mathbb{T}_U) = \emptyset$ then $\mathbb{T}_U$ and $\mathbb{T}$ are not QDS as $\mathbb{T}$ always has a fixed point. Suppose $\mathbb{T}_U$ has a fixed point $a \in R_N$. Let $\phi_a : Att(\mathbb{T}) \longrightarrow Att(\mathbb{T}_U)$, $b \mapsto a + b$. This is a bijection by theorem 2.2.2 and for all $b \in Att(\mathbb{T})$

$$\mathbb{T}_U(\phi_a(b)) = \mathbb{T}_U(a + b) = \mathbb{T}_U(a) + \mathbb{T}b = a + \mathbb{T}b = \phi_a(\mathbb{T}(b)).$$

The result now follows from corollary 2.3.1. ■

By lemma 2.1.10 any $a \in R_N$ is a fixed point of $\mathbb{T}_U$ for exactly one $U \in R_N$. We wish to know when there are inputs $U \in R_N$ such that $\mathbb{T}$ and $\mathbb{T}_U$ are not QDS.

**Corollary 2.3.3** *For given $R, N$ and $\mathbb{T}$, $\mathbb{T}$ and $\mathbb{T}_U$ are* QDS *for all $U$ if and only if $|Fix(\mathbb{T})| = 1$. When $|Fix(\mathbb{T})| > 1$ then there are $\frac{|R_N|}{|Fix(\mathbb{T})|}$ inputs $U$ such that $\mathbb{T}_U$ and $\mathbb{T}$ are* QDS *and there are $\frac{|R_N|}{|Fix(\mathbb{T})|}(|Fix(\mathbb{T})| - 1)$ inputs $U$ such that $\mathbb{T}_U$ and $\mathbb{T}$ are not* QDS. *Similarly for null boundary conditions and hybrids.*

Proof:

If $|Fix(\mathbb{T})| = 1$ then $(\mathbb{T} - 1)a \neq 0$ for any $a \in R_N \setminus \{0\}$ so $\mathbb{T} - 1$ is a unit and it follows that $(\mathbb{T} - 1)R_N = R_N$ hence by lemma 2.1.10 every input $U$ is such that $\mathbb{T}_U$ has a fixed point so by theorem 2.3.1 $\mathbb{T}$ and $\mathbb{T}_U$ are QDS. Conversely if $|Fix(\mathbb{T})| > 1$ then $(\mathbb{T} - 1)R_N \subset R_N$ and by lemma 2.1.10 any $U \in R_N \setminus (\mathbb{T} - 1)R_N$ has no fixed points and thus by theorem 2.3.1 $\mathbb{T}$ and $\mathbb{T}_U$ are not QDS.

By what we have just shown the number of inputs $U \in R_N$ such that $\mathbb{T}$ and $\mathbb{T}_U$ are QDS is $|(\mathbb{T} - 1)R_N|$. The $R_N$-module homomorphism from $R_N$ onto $(\mathbb{T} - 1)R_N$ given by $a \mapsto (\mathbb{T} - 1)a$ has kernel $Fix(\mathbb{T})$ hence by the first (module) isomorphism theorem $R_N/Fix(\mathbb{T}) \cong (\mathbb{T} - 1)R_N$ and it follows that $|(\mathbb{T} - 1)R_N| = |R_N|/|Fix(\mathbb{T})|$. The rest of the result follows by subtraction. ■

We shall denote the multiplicative group of units in $R_N$ by $U(R_N)$. We define an equivalence relation on $R_N$ as follows:

**Definition 2.3.2** *For given $R, N$ and $\mathbb{T}$ say that $U \sim_\wedge V$ for $U, V \in R_N$ if $\mathbb{T}_{V-\lambda U}$ has a fixed point for any $\lambda \in U(R_N)$.*

Note that by lemma 2.1.10 $U \sim_\wedge V$ if and only if $V - \lambda U \in (\mathbb{T} - 1)R_N$ for some $\lambda \in U(R_N)$. It remains to show that the relation $\sim_\wedge$ is an equivalence relation.

**Lemma 2.3.2** *For given $R, N$ and $\mathbb{T}$, $\sim_\wedge$ is an equivalence relation on $R_N$*

Proof:

Clearly $U \sim_\wedge U$ for all $U \in R_N$ (just take $\lambda = 1$) so $\sim_\wedge$ is reflexive. If $U \sim_\wedge V$ then $\mathbb{T}_{V-\lambda U}(a) = a$ for some $a \in R_N$ and $\lambda \in U(R_N)$. It follows that $\mathbb{T}_{\lambda U - V}(-a) = -a$ and hence that $\mathbb{T}_{U-\lambda^{-1}V}(-\lambda^{-1}a) = -\lambda^{-1}a$ and hence $V \sim_\wedge U$ so $\sim_\wedge$ is symmetric. Let $U \sim_\wedge V$ and $V \sim_\wedge W$ so there are $a, b \in R_N$ and $\lambda, \mu \in U(R_N)$ such that

$$\mathbb{T}_{V-\lambda U}(a) = a, \qquad \mathbb{T}_{V-\mu^{-1}W}(-\mu^{-1}b) = -\mu^{-1}b$$

where we have used the symmetry of $\sim_\wedge$. On subtraction and multiplication by $\mu$ one gets

$$\mathbb{T}_{W-\lambda\mu U}(\mu a + b) = \mu a + b$$

so $U \sim_\wedge W$ so $\sim_\wedge$ is transitive. ■

**Remark 2.3.1** *If $U$ and $V$ are such that $U = \lambda V$ for some unit $\lambda$ (in particular if both $U$ and $V$ are units) then $U \sim_\wedge V$.*

Proof:

If $U = \lambda V$ then $\mathbb{T}_{U-\lambda V} = \mathbb{T}_0 = \mathbb{T}$ which has a fixed point. ■

There are two important restricted cases of the $\sim_\wedge$ equivalence relation.

**Definition 2.3.3** *For given $R$ and $N$ say $U \sim_0 V$ if $U$ and $V$ are such that $V = \lambda U$ for some unit $\lambda$ and for given $R, N$ and $\mathbb{T}$ say $U \sim_1 V$ if $\mathbb{T}_{V-U}$ has a fixed point.*

**Lemma 2.3.3** *$\sim_0$ and $\sim_1$ are equivalence relations.*

Proof:

To prove that $\sim_0$ is an equivalence relation is just a matter of a straight-forward verification. For $\sim_1$ the proof is similar to (but simpler) than that of lemma 2.3.2. ■

**Lemma 2.3.4** *For given $R, N$ and $\mathbb{T}$ there are $|Fix(\mathbb{T})|$ $\sim_1$ equivalence classes, each of which has $|R_N|/|Fix(\mathbb{T})|$ members.*

Proof:

By corollary 2.3.3 there are $|R_N|/|Fix(\mathbb{T})|$ members in the $\sim_1$ class of 0, hence for given $V$ as $U$ runs through $R_N$ there will be exactly $|R_N|/|Fix(\mathbb{T})|$ inputs $U$ such that $\mathbb{T}_{V-U}$ has a fixed point so each $\sim_1$ class has $|R_N|/|Fix(\mathbb{T})|$ members and it follows that there are $|Fix(\mathbb{T})|$ classes. ■

We show in the next lemma that the $\sim_\wedge$ equivalence classes can be generated from the $\sim_0$ and $\sim_1$ equivalence classes. This is useful (especially if more than one rule is being considered) as the $\sim_0$ classes are independent of the rule $\mathbb{T}$ under consideration and the $\sim_1$ classes are simple to compute.

**Lemma 2.3.5** *For given $R, N$ and $\mathbb{T}$, let $W, U \in R_N$ then $W \sim_\wedge U$ if and only if there is some $V \in R_N$ such that $U \sim_1 V$ and $V \sim_0 W$.*

Proof:

Suppose there is some $V \in R_N$ such that $U \sim_1 V$ and $V \sim_0 W$, then $U \sim_\wedge V$ and $V \sim_\wedge W$ so $U \sim_\wedge W$. Suppose $U \sim_\wedge W$ so $W \sim_\wedge U$ so there are $a \in R_N$ and $\lambda \in U(R_N)$ such that $\mathbb{T}_{U-\lambda W}(a) = a$. Now by definition $W \sim_0 \lambda W$ and $\mathbb{T}_{U-\lambda W}(a) = a$ implies $\lambda W \sim_1 U$ so taking $V = \lambda W$ gives the result. ■

We now show that being in the same $\sim_\wedge$ equivalence class is a sufficient condition for QDS.

**Theorem 2.3.2** *For given $R, N$ and $\mathbb{T}$, if $U \sim_\wedge V$ then $\mathbb{T}_U$ and $\mathbb{T}_V$ are* QDS.

Proof:

If $U \sim_\wedge V$ then there is $a \in R_N$ and $\lambda \in U(R_N)$ such that $\mathbb{T}_{V-\lambda U}(a) = a$. Define $\phi_{\lambda,a} : R_N \longrightarrow R_N$ by $b \mapsto \lambda b + a$, as $\lambda$ is a unit this is a bijection. Using the fact that $\mathbb{T}a + V - \lambda U = a$ we have for all $b \in R_N$ that

$$\mathbb{T}_V(\phi_{\lambda,a}(b)) = \mathbb{T}\lambda b + \mathbb{T}a + V = \mathbb{T}\lambda b + \lambda U + a = \lambda(\mathbb{T}b + U) + a = \phi_{\lambda,a}(\mathbb{T}_U(b)).$$

Hence $\mathbb{T}_V \circ \phi_{\lambda,a} = \phi_{\lambda,a} \circ \mathbb{T}_U$ and so $\phi_{\lambda,a}$ satisfies the conditions of corollary 2.3.2 and the result follows. ■

**Corollary 2.3.4** *Let $U, V \in R_N$ be on the same cycle or evolve to that cycle under $\mathbb{T}$, then $\mathbb{T}_U$ and $\mathbb{T}_V$ are* QDS.

Proof:

Let $U \in R_N$, then $\mathbb{T}_{U-\mathbb{T}U}(U) = U$ so $\mathbb{T}U \sim_1 U$ and it follows that all elements of $R_N$ on or evolving to $C_0(U)$ are in the same $\sim_1$ equivalence class and the result follows from theorem 2.3.2. ■

Inputs $U$ and $V$ in distinct $\sim_\wedge$ equivalence classes can be such that $\mathbb{T}_U$ and $\mathbb{T}_V$ are QDS but being in the same $\sim_\wedge$ equivalence class guarantees qualitatively similar dynamics. Also it is clear that being in an $\sim_1$ equivalence class distinct from that of 0 guarantees qualitative dissimilarity to $\mathbb{T}_0$. By corollary 2.3.4 for given $\mathbb{T}$ all the distinct qualitative dynamical behaviours that can occur under $\mathbb{T}_U$ for some input $U$ occur for $\mathbb{T}_U$ for some $U \in Att(\mathbb{T})$.

In the case of fixed boundary conditions and hybrids these results still hold provided one replaces $U(R_N)$ with the set of non-singular $N \times N$ matrices over $R$ which commute with $\mathbf{T}$ (or $\mathfrak{T}$). Moreover any result concerning just the $\sim_1$ equivalence classes will hold for fixed boundary conditions and hybrids, in particular theorem 2.3.2 holds with $\sim_\wedge$ replaced by $\sim_1$ for then no use of multiplicative structure is made, consequently corollary 2.3.4 holds for fixed boundary conditions and hybrids since its proof only utilises the $\sim_1$ equivalence relation.

So far we have only found sufficient conditions for QDS, in the next theorem we find necessary and sufficient conditions under certain circumstances, but to do so we need the following lemma.

**Lemma 2.3.6** *Given $\mathbb{T}$ and $U$ in $R_N$ such that the minimal orbit length occurring under $\mathbb{T}_U$ is $m$ then there is an element $U^* \in R_N$ such that $U \sim_1 U^*$ and $\mathbb{T}^m_{U^*}(0) = 0$. Similarly for null boundary conditions and hybrids.*

Proof:

If $m = 1$ then $U \sim_1 0$ so take $U^* = 0$. If $m > 1$ then by (the proof of) corollary 2.3.4 there is some $\overline{U} \in Att(\mathbb{T})$ with $U \sim_1 \overline{U}$. Let $a \in R_N$ be such that $\mathbb{T}^m_{\overline{U}}(a) = a$ and let $U^* = \overline{U} - a(\mathbb{T} - 1)$ then $\overline{U} - U^* = a(\mathbb{T} - 1)$ and $\mathbb{T}_{a(\mathbb{T}-1)}(-a) = -a$ so $\overline{U} \sim_1 U^*$. Applying the orbit structure preserving map $\phi_{-a}$ we see that $\phi_{-a}(a) = 0$ and hence $\mathbb{T}^m_{U^*}(0) = 0$. The result then follows because $\sim_1$ is an equivalence relation. ■

**Theorem 2.3.3** *Suppose that for a given $U$ the minimum orbit length occurring under $\mathbb{T}_U$ is $m$ and that for any $V \in R_N$ the minimum orbit length under $\mathbb{T}_V$ divides all other orbit lengths occurring under $\mathbb{T}_V$ then, for any $V \in R_N$, $\Sigma(\mathbb{T}_U) = \Sigma(\mathbb{T}_V)$ if and only if $m$ is the minimum orbit length occurring under $\mathbb{T}_V$. Similarly for null boundary conditions and hybrids.*

Proof:

By lemma 2.3.6 we know that there is some $U^* \in R_N$ such that $U \sim_1 U^*$ where $\mathbb{T}^m_{U^*}(0) = 0$ and hence $\Sigma(\mathbb{T}_U) = \Sigma(\mathbb{T}_{U^*})$ by theorem 2.3.2. If $V$ is such that the

minimum orbit length under $\mathbb{T}_V$ is $m$ we define a map

$$\begin{aligned} \chi_a \quad &: \quad Att(\mathbb{T}_{U^*}) \longrightarrow R_N \\ & \qquad b \mapsto a + b, \end{aligned}$$

where $\mathbb{T}_V^m(a) = a$. Now, for all $b \in Att(\mathbb{T}_{U^*})$,

$$\chi_a(\mathbb{T}_{U^*}^m(b)) = \mathbb{T}^m b + \mathbb{T}_{U^*}^m(0) + a = \mathbb{T}^m b + \mathbb{T}_V^m(a) = \mathbb{T}_V^m(\chi_a(b))$$

and hence for any integer $n > 0$ one has

$$\chi_a(\mathbb{T}_{U^*}^{nm}(b)) = \mathbb{T}_V^{nm}(\chi_a(b))$$

(note that in general we do not have $\chi_a \circ \mathbb{T}_{U^*} = \mathbb{T}_V \circ \chi_a$). It follows that, as $\chi_a$ is clearly a bijection, that Im $\chi_a = Att(\mathbb{T}_V)$ and that $\chi_a$ maps points on prime period $nm$ orbits under $\mathbb{T}_{U^*}$ onto points on period $nm$ orbits under $\mathbb{T}_V$. Suppose that, under $\mathbb{T}_{U^*}$, $b$ is on an orbit of length $nm$, we show that $\chi_a(b)$ is on an orbit of length $nm$, for under the conditions of the theorem and by the proceeding remarks, $\chi_a(b)$ must be on an orbit of length $n'm$ for some integer $n' \leq n$ but if $n' < n$ then

$$\mathbb{T}_V^{n'm}(\chi_a(b)) = \chi_a(b) \;\Rightarrow\; \chi_a(\mathbb{T}_{U^*}^{n'm}(b)) = \chi_a(b) \;\Rightarrow\; \mathbb{T}_{U^*}^{n'm}(b) = b$$

contradicting the minimality of $nm$ as the orbit length of $b$ under $\mathbb{T}_{U^*}$. As $\chi_a$ is a bijection and maps points on orbits of length $nm$ under $\mathbb{T}_{U^*}$ to points on orbits of length $nm$ under $\mathbb{T}_V$ it is clear that $\Sigma(\mathbb{T}_{U^*}) = \Sigma(\mathbb{T}_V)$ and hence that $\Sigma(\mathbb{T}_U) = \Sigma(\mathbb{T}_V)$.

If the minimum orbit length occurring under $\mathbb{T}_V$ is not $m$ then clearly $\Sigma(\mathbb{T}_U) \neq \Sigma(\mathbb{T}_V)$. ■

The condition that for any $V \in R_N$ the minimum orbit length under $\mathbb{T}_V$ divides all other orbit lengths occurring under $\mathbb{T}_V$ seems somewhat restrictive at first sight, however it turns out that it often holds, for instance we shall see in chapter 4 that it is always the case when $R$ is a finite field and in chapter 5 we find that this is the case whenever $R = \mathbb{Z}/m\mathbb{Z}$, any integer $m > 1$.

We finish this chapter with the following corollary to lemma 2.3.6, concerning the case where $R_N$ (or more generally any finite commutative ring $R$, recall remark 2.1.1) is completely primary (see appendix A, completely primary means every element is either nilpotent or a unit). We find a use for the corollary in chapter 3, section 3.3.3, and note that there are similar corollaries concerning specific properties of $R_N$ and of $U$ (one such is used implicitly in the proof of theorem 3.3.6).

**Corollary 2.3.5** *Under the conditions of lemma 2.3.6 if $R_N$ is completely primary and $\mathbb{T}$ is a unit with $\mathbb{T}-1$ nilpotent and $U$ is a unit then there is a unit $U^* \in R_N$ such that $U \sim_1 U^*$ and $\mathbb{T}^m_{U^*}(0) = 0$.*

Proof:

As $\mathbb{T}$ and $U$ are units the element $\overline{U}$ defined in the proof of lemma 2.3.6 is a unit by lemma 2.1.5 and so, by the proof of lemma 2.3.6, $U \sim_1 U^*$ where $\mathbb{T}^m_{U^*}(0) = 0$ and $U^* = \overline{U} - a(\mathbb{T}-1)$ where $(\phi_a)_U = m$. Then, as $\mathbb{T}-1$ is nilpotent, $U^*$ is a unit (in a commutative finite completely primary ring if $U$ is a unit and $n$ is nilpotent then $U+n$ is a unit, as clearly $U+n$ is not nilpotent). ■

# Chapter 3

# Additive cellular automata over finite fields I

We begin this chapter by showing how, when the state alphabet $R$ is a finite field of characteristic $p$, $R_N$ can be decomposed into a direct product of completely primary rings. An immediate advantage of this procedure over that employed by Guan and He [27] is that our decomposition does not depend upon the cellular automata rule being considered (recall that the approach of Guan and He was to decompose $R^N$ into a direct sum of sub-spaces invariant under the action of a matrix representing the global rule of the cellular automata) and thus only needs to be done once even if large numbers of rules are being considered.

As we have stated before our method is a formalisation of that employed by Martin *et. al.* [3], the direct product formalism is equivalent to the technique of looking modulo a factor of $x^N - 1$ on $N$ cells used by Martin *et. al.*. However our method puts the emphasis on the algebraic structure and brings many useful features to the fore, in particular the connection between behaviour on $n$ cells, where $n$ is coprime to $p$, and behaviour on $np^r$ cells, any integer $r > 0$, is stressed, leading to strong results. Because we deal with rings and ring homomorphisms both additive and multiplicative structure is preserved and the situation is ripe for dealing with the case of additive cellular automata with time independent inputs as well as the usual, input less, case.

A further advantage of the direct product formalism and the emphasis on algebraic structure is that it allows us, in chapter 5, to extend results from the case of state alphabet $R = \mathbb{F}_p$ to the case of state alphabet $R = \mathbb{Z}_{/p^l}$ for any integer $l > 1$, using the technique of idempotent lifting.

Returning our attention to the present chapter, in theorem 3.1.1 we obtain a ring isomorphism between $R_N$ and the relevant direct product and describe how the direct product in the $N = np^r$ case is related to that in the $N = n$ case ($n$ coprime to $p$). For the rest of the chapter we concentrate on behaviour in an individual ring in the direct product, we return to the "whole" ring and cellular automata in chapter 4 where the results from chapter 3 are combined.

On $n$ cells, $n$ coprime to $p$, the factors in the direct product are all finite fields, the relevant dynamics in a finite field is discussed in section 3.2. This case is particularly simple, both with and without inputs, in particular the cycle sets in each factor consist of at most two terms.

On $np^r$ cells, the factors in the direct product are completely primary rings with non-zero nilpotent elements, in section 3.3 we describe some basic properties of these rings, in particular we show that any such ring is a (ring) extension of a finite field

occurring as a factor in the direct product for $n$ cells. In subsection 3.3.1 we describe the relevant dynamics in a ring of the above type when $U = 0$, theorems 3.3.1 and 3.3.2 completely describe the behaviour of the system in this case in terms of two quantities, one of which is completely determined by the $r = 0$ case. Theorem 3.3.3 extends the description of the system in a particular factor in the direct product from the $np^r$ cells case to the $np^{r+1}$ cells case.

In subsection 3.3.2 transient behaviour is considered for $U = 0$, by theorem 2.2.1 this suffices for $U \neq 0$ also. In subsection 3.3.3 the case of non-zero inputs $U$ is considered, we concentrate on the case where qualitatively different behaviour from the $U = 0$ case occurs, necessary and sufficient conditions for this to be so are obtained. We show in theorems 3.3.5 and 3.3.6 that, when the behaviour for non-zero $U$ is qualitatively different from that when $U$ is zero, all orbits are of the same length $p^S$ where $S$ is an integer, $S > 0$.

## 3.1 Direct product decomposition of $R_N$ when $R$ is a finite field

Our aim is to decompose $R_N$ into a direct product of simpler rings. When $R$ is a finite field this is easily accomplished. The following lemma is vital.

**Lemma 3.1.1** *Let $N = np^r$ where $p \nmid n$ then over $\mathbb{F}_{p^q}[x]$ one has*

$$x^N - 1 = \prod_{i=1}^{m} R_i(x)^{p^r}$$

*where the $R_i(x)$ are distinct irreducible polynomials.*

Proof:

First consider $x^n - 1$, this is separable over $\mathbb{F}_{p^q}[x]$ ([28] page 277) and thus has $n$ distinct roots in its splitting field extension. so

$$x^n - 1 = \prod_{i=1}^{m} R_i(x)$$

where the $R_i(x), 1 \leq i \leq m \leq n$ are distinct irreducibles. Now consider $x^N - 1$ with $N = np^r$, $r > 0$ and $p \nmid n$. Over $\mathbb{F}_{p^q}$ one has

$$x^{np^r} - 1 = (x^n - 1)^{p^r} = (\prod_{i=1}^{m} R_i(x))^{p^r} = \prod_{i=1}^{m} R_i(x)^{p^r}. \quad \blacksquare$$

**Theorem 3.1.1** *With $N = np^r$, $p \nmid n$, one has that*

$$\frac{\mathbb{F}_{p^q}[x]}{(x^N-1)\mathbb{F}_{p^q}[x]} \cong \prod_{i=1}^{m} \frac{\mathbb{F}_{p^q}[x]}{R_i(x)^{p^r}\mathbb{F}_{p^q}[x]}$$

*where $x^N - 1 = \prod_{i=1}^{m} R_i(x)^{p^r}$ is the factorisation of $x^N - 1$ described in lemma 3.1.1.*

Proof:

For $i = 1, \ldots, m$ there are homomorphisms $\theta_i : \frac{\mathbb{F}_{p^q}[x]}{(x^N-1)\mathbb{F}_{p^q}[x]} \longrightarrow \frac{\mathbb{F}_{p^q}[x]}{R_i(x)^{p^r}\mathbb{F}_{p^q}[x]}$, given by

$$a(x) + (x^N - 1)\mathbb{F}_{p^q}[x] \mapsto a(x) + R_i(x)^{p^r}\mathbb{F}_{p^q}[x].$$

Let $\Theta$ be the homomorphism induced by the $\theta_i$, $1 \leq i \leq m$,

$$\begin{aligned} \Theta : \frac{\mathbb{F}_{p^q}[x]}{(x^N-1)\mathbb{F}_{p^q}[x]} &\longrightarrow \prod_{i=1}^{m} \frac{\mathbb{F}_{p^q}[x]}{R_i(x)^{p^r}\mathbb{F}_{p^q}[x]} \\ a &\mapsto (\theta_i(a), \ldots, \theta_m(a)). \end{aligned}$$

We examine the kernel of $\Theta$:

$$\begin{aligned} \text{Ker } \Theta &= \{a : \theta_i(a) = 0. 1 \leq i \leq m\} \\ &= \{a : R_i(x)^{p^r} | a(x), 1 \leq i \leq m\}. \end{aligned}$$

Now $\mathbb{F}_{p^q}[x]$ is a unique factorisation domain, and each $R_i(x)$ is irreducible in $\mathbb{F}_{p^q}[x]$ and hence prime, thus

$$R_i(x)^{p^r} | a(x),\ 1 \leq i \leq m,\ \Rightarrow\ x^N - 1 | a(x)\ \Rightarrow\ a = 0,$$

hence Ker $\Theta = \{0\}$ and so $\Theta$ is a ring monomorphism. Now, if the degree of $R_i(x)$ is $d_i$ we have that $n = \sum_{i=1}^{m} d_i$ and hence $N = np^r = p^r \sum_{i=1}^{m} d_i$. We have

$$\left| \prod_{i=1}^{m} \frac{\mathbb{F}_{p^q}[x]}{R_i(x)^{p^r}\mathbb{F}_{p^q}[x]} \right| = \prod_{i=1}^{m} \left| \frac{\mathbb{F}_{p^q}[x]}{R_i(x)^{p^r}\mathbb{F}_{p^q}[x]} \right| = \prod_{i=1}^{m} p^{qp^r d_i} = p^{qN} = \left| \frac{\mathbb{F}_{p^q}[x]}{(x^N-1)\mathbb{F}_{p^q}[x]} \right|.$$

Thus $\Theta$ is a monomorphism between finite rings of the same cardinality and hence is surjective and so is an isomorphism. ■

**Example 3.1.1**

Let $p = 3$, $q = 1$ and $N = 11$ then

$$x^{11} - 1 = (x+2)(x^5 + 2x^3 + x^2 + 2x + 2)(x^5 + x^4 + 2x^3 + x^2 + 2)$$

hence by lemma 3.1.1

$$\begin{aligned} x^{33}-1 &= (x+2)^3(x^5+2x^3+x^2+2x+2)^3(x^5+x^4+2x^3+x^2+2)^3 \\ &= (x^3+2)(x^{15}+2x^9+x^6+2x^3+2)(x^{15}+x^{12}+2x^9+x^6+2). \end{aligned}$$

Applying theorem 3.1.1 we get

$$\frac{\mathbb{F}_3[x]}{(x^{11}-1)\mathbb{F}_3[x]} \cong \frac{\mathbb{F}_3[x]}{(x+2)\mathbb{F}_3[x]} \times \frac{\mathbb{F}_3[x]}{(x^5+2x^3+x^2+2x+2)\mathbb{F}_3[x]} \times \frac{\mathbb{F}_3[x]}{(x^5+x^4+2x^3+x^2+2)\mathbb{F}_3[x]}$$

and

$$\frac{\mathbb{F}_3[x]}{(x^{33}-1)\mathbb{F}_3[x]} \cong \frac{\mathbb{F}_3[x]}{(x^3+2)\mathbb{F}_3[x]} \times \frac{\mathbb{F}_3[x]}{(x^{15}+2x^9+x^6+2x^3+2)\mathbb{F}_3[x]} \times \frac{\mathbb{F}_3[x]}{(x^{15}+x^{12}+2x^9+x^6+2)\mathbb{F}_3[x]}.$$

♦

Given an element of $\prod_{i=1}^{m} \frac{\mathbb{F}_{p^q}[x]}{R_i(x)^{p^r}\mathbb{F}_{p^q}[x]}$ we would like to be able to "reconstruct" the unique preimage of this element under $\Theta$, the next lemma tells us how to do this.

**Lemma 3.1.2** *Let* $a \in \prod_{i=1}^{m} \frac{\mathbb{F}_{p^q}[x]}{R_i(x)^{p^r}\mathbb{F}_{p^q}[x]}$, $a = (a_1, \ldots, a_m)$, *then* $a$ *is the image under* $\Theta$ *of the element* $A \in \frac{\mathbb{F}_{p^q}[x]}{(x^N-1)\mathbb{F}_{p^q}[x]}$ *given by*

$$\begin{aligned} A = a_m &+ (a_{m-1}-a_m)g_m S_m \\ &+ (a_{m-2}-a_{m-1})g_m S_m g_{m-1} S_{m-1} \\ &\vdots \\ &+ (a_1-a_2)\prod_{i=2}^{m} g_i S_i \\ &+ (x^N-1)\mathbb{F}_{p^q}[x] \end{aligned}$$

*where the canonical representative of* $S_i$ *is* $S_i(x) = R_i(x)^{p^r}$ *for* $1 \le i \le m$ *and we have identified* $a_i = a_i(x) + S_i(x)\mathbb{F}_{p^q}[x]$ *with its canonical representative* $a_i(x)$ *and the* $g_i$ *are*

*the elements whose canonical representatives are the polynomials satisfying*

$$\begin{aligned} g_1(x)S_1(x) + g_2(x)S_2(x) &= 1 \\ g_{1,2}(x)S_1(x)S_2(x) + g_3(x)S_3(x) &= 1 \\ &\vdots \quad \vdots \\ g_{1,m-1}(x)\prod_{i=1}^{m-1} S_i(x) + g_m(x)S_m(x) &= 1 \end{aligned}$$

*which exist by the pairwise coprimeness of the* $S_i(x)$.

Proof:

The existence of the $g_i(x)$ (and of the $g_{i,j}(x)$) follows from the Chinese remainder theorem, see [29], pages $220-221$. We need to verify that $\theta_i(A) = a_i$. Clearly $\theta_m(A) = a_m$. Let $1 \leq I \leq m-1$, we can write $A$ as

$$\begin{aligned} A = a_m &+ (a_{m-1} - a_m)(1 - g_{1,m-1}\textstyle\prod_{i=1}^{m-1} S_i) \\ &+ (a_{m-2} - a_{m-1})(1 - g_{1,m-1}\textstyle\prod_{i=1}^{m-1} S_i)g_{m-1}S_{m-1} \\ &\vdots \\ &+ (a_I - a_{I+1})(1 - g_{1,m-1}\textstyle\prod_{i=1}^{m-1} S_i)\prod_{j=I+1}^{m-1} g_j S_j \\ &+ (a_{I-1} - a_I)\textstyle\prod_{i=I}^{m} g_i S_i \\ &\vdots \\ &+ (a_1 - a_2)\textstyle\prod_{i=2}^{m} g_i S_i. \end{aligned}$$

Then

$$\begin{aligned} \theta_I(A) = a_m &+ a_{m-1} - a_m \\ &+ a_{m-2} - a_{m-1} \\ &\vdots \\ &+ a_I - a_{I+1} \\ = a_I. & \end{aligned}$$

■

Note that when $r > 0$ we can find the $g_i$ from the $g_i$ in the $r = 0$ case, for on taking the $p^r$-th power of the equations

$$g_1(x)R_1(x) + g_2(x)R_2(x) = 1$$

$$\begin{aligned} g_{1,2}(x)R_1(x)R_2(x) + g_3(x)R_3(x) &= 1 \\ &\vdots \quad \vdots \\ g_{1,m-1}(x)\prod_{i=1}^{m-1} R_i(x) + g_m(x)R_m(x) &= 1 \end{aligned}$$

for the $r = 0$ case one obtains

$$\begin{aligned} g_1(x)^{p^r}R_1(x)^{p^r} + g_2(x)^{p^r}R_2(x)^{p^r} &= 1 \\ g_{1,2}(x)^{p^r}R_1(x)^{p^r}R_2(x)^{p^r} + g_3(x)^{p^r}R_3(x)^{p^r} &= 1 \\ &\vdots \quad \vdots \\ g_{1,m-1}(x)^{p^r}\prod_{i=1}^{m-1} R_i(x)^{p^r} + g_m(x)^{p^r}R_m(x)^{p^r} &= 1 \end{aligned}$$

and for $r > 0$, $S_i(x) = R_i(x)^{p^r}$, thus the $g_i$, $1 \leq i \leq m$, in the $r > 0$ case are obtained from the $g_i$, $1 \leq i \leq m$, in the $r = 0$ case by

$$g_i(x) + (x^n - 1)\mathbb{F}_{p^q}[x] \mapsto g_i(x)^{p^r} + (x^{np^r} - 1)\mathbb{F}_{p^q}[x].$$

In section 4.5 we shall see an alternative approach to "reconstruction".

## 3.2 Dynamics in a single field $\frac{\mathbb{F}_{p^q}[x]}{R(x)\mathbb{F}_{p^q}[x]}$

Throughout this section $R(x)$ is a monic, irreducible polynomial in $\mathbb{F}_{p^q}[x]$ ($p$ a prime integer, $q > 0$). The degree of $R(x)$ is $d$. Then (see appendix A, section A.4) $\frac{\mathbb{F}_{p^q}[x]}{R(x)\mathbb{F}_{p^q}[x]}$ is a field and is isomorphic to $\mathbb{F}_{p^{qd}}$. Thus we are concerned with systems with dynamics defined by (1.5.22) with $R = \mathbb{F}_{p^q}$ and $g(x) = R(x)$ and by the previous sentence may instead consider dynamics in $\mathbb{F}_{p^{q'}}$ for some $q' > q$. For an element $\mathbb{T} \neq 0$ let $O(\mathbb{T})$ be its order in $\mathbb{F}^*_{p^q}$.

The case $U = 0$ is particularly simple and is described completely by the following lemma.

**Lemma 3.2.1** *Let* $\mathbb{T} \in \mathbb{F}_{p^q}$ *then*

(i) $\mathbb{T}$ *has non-zero fixed points if and only if* $\mathbb{T} = 1$. *When* $\mathbb{T} = 1$ *all elements of* $\mathbb{F}_{p^q}$ *are fixed, when* $\mathbb{T} = 0$ *the only non-transient point is* 0.

(ii) *When* $\mathbb{T} \in \mathbb{F}_{p^q}^* \setminus \{1\}$ *then* 0 *is the unique fixed point under* $\mathbb{T}$ *and all other elements of* $\mathbb{F}_{p^q}$ *are on orbits of length* $O(\mathbb{T})$. *There are* $\frac{p^q-1}{O(\mathbb{T})}$ *such orbits.*

Proof:

(i) For any $\mathbb{T} \in \mathbb{F}_{p^q}$ and any $a \neq 0$

$$\mathbb{T}a = a \Leftrightarrow \mathbb{T}aa^{-1} = aa^{-1} \Leftrightarrow \mathbb{T} = 1.$$

The rest is completely obvious.

(ii) By definition $\mathbb{T}^{O(\mathbb{T})} = 1$ so $\mathbb{T}^{O(\mathbb{T})}a = a$ for all $a \in \mathbb{F}_{p^q}$. Suppose there is some $k < O(\mathbb{T})$ such that $\mathbb{T}^k a = a$ for some non-zero $a$. Then multipling by $a^{-1}$ gives $\mathbb{T}^k = 1$, contradicting the minimality of $O(\mathbb{T})$. As there are $p^q - 1$ non-zero elements in $\mathbb{F}_{p^q}$ the result follows. ■

Thus when $\mathbb{T} \notin \{0, 1\}$ the cycle set of $\mathbb{T}$ is

$$\Sigma(\mathbb{T}) = 1[1] + \frac{p^q - 1}{O(\mathbb{T})}[O(\mathbb{T})]. \tag{3.2.1}$$

**Example 3.2.1**

Consider $\mathbb{F}_{3^2}$ represented by $\frac{\mathbb{F}_3[x]}{(x^2+1)\mathbb{F}_3[x]}$. Let $\mathbb{T} = 1 + x + (x^2 + 1)\mathbb{F}_3[x]$ then $O(\mathbb{T}) = 8$ so one has the zero fixed point and one orbit of length 8, in cycle set notation

$$\Sigma(\mathbb{T}) = 1[1] + 1[8]. \quad \blacklozenge$$

We now consider non-zero $U$ and our first task is to determine $(\phi_0)_U$.

**Lemma 3.2.2** *Let* $\mathbb{T} \in \mathbb{F}_{p^q}$, *then for any* $U \in \mathbb{F}_{p^q}^*$

$$\begin{aligned} (\phi_0)_U &= O(\mathbb{T}) \quad \textit{if} \quad \mathbb{T} \neq 0, 1; \\ (\phi_0)_U &= p \qquad \textit{if} \quad \mathbb{T} = 1; \\ (\phi_0)_U &= 1 \qquad \textit{if} \quad \mathbb{T} = 0. \end{aligned}$$

Proof:

If $\mathbb{T} \neq 1$ then, by remark 2.1.3, $\mathbb{T}_1^{O(\mathbb{T})}(0)$ is fixed by $\mathbb{T}$ and hence $\mathbb{T}_1^{O(\mathbb{T})}(0) = 0$ by lemma 3.2.1. Thus for any $U \in \mathbb{F}_{p^q}$ one has that $\mathbb{T}_U^{O(\mathbb{T})}(0) = 0$ and hence $(\phi_0)_U | O(\mathbb{T})$ but, by remark 2.2.1, $O(\mathbb{T}) = (\phi_U)_0 | (\phi_0)_U$ hence $(\phi_0)_U = O(\mathbb{T})$.

Now suppose $\mathbb{T} = 1$ and $U \neq 0$ so $(\phi_U)_0 = 1$ and $(\phi_0)_U | p$ by lemma 2.1.13, hence, as $\mathbb{T}_U(0) = U \neq 0$, $(\phi_0)_U \neq 1$ so $(\phi_0)_U = p$. When $\mathbb{T} = 0$ it is clear that $U$ is a fixed point under $\mathbb{T}_U$. ■

**Lemma 3.2.3** *Let $\mathbb{T} \in \mathbb{F}_{p^q}$ and $U \in \mathbb{F}_{p^q}^*$ then*

(i) *If $\mathbb{T} = 0$ the only non-transient point is $U$ which is a fixed point.*

(ii) *If $\mathbb{T} = 1$ then every point is periodic with prime period $p$ under $\mathbb{T}_U$.*

(iii) *If $\mathbb{T} \neq 0$ and $\mathbb{T} \neq 1$ then $\mathbb{T}$ has a unique fixed point $a^* \neq 0$ given by*

$$a^* = -(\mathbb{T} - 1)^{-1} U.$$

*All other points are periodic with prime period $O(\mathbb{T})$.*

Proof:

(i) This is clear. (ii) $(1_U)^p(a) = a + pU = a$ for any $a \in \mathbb{F}_{p^q}$. If $(1_U)^L(a) = a$ for some $0 < L < p$ then one has $a + LU = a$ hence $LU = 0$ hence $U = 0$. (iii) Let $0 < L < O(\mathbb{T})$ and suppose that, for some $a^* \neq 0$, one has $\mathbb{T}_U^L(a^*) = a^*$ then

$$\mathbb{T}^L a^* + \mathbb{T}_U^L(0) = a^* \;\Rightarrow\; (\mathbb{T}^L - 1)a^* = -\mathbb{T}_U^L(0) \;\Rightarrow\; a^* = -(\mathbb{T}^L - 1)^{-1}\mathbb{T}_U^L(0),$$

a unique solution. There cannot be only one point on an orbit of prime period $L$ if $L > 1$ so $a^*$ must be a fixed point and the result follows on putting $L = 1$. For $b \in \mathbb{F}_{p^q}$, $b \neq a^*$, we have, by lemma's 3.2.1 and 3.2.2, that $\mathbb{T}_U^{O(\mathbb{T})}(b) = b$ and by the above $b$ cannot have a period less than $O(\mathbb{T})$. ■

Thus, as in the $U = 0$ case, one has for $\mathbb{T} \notin \{0, 1\}$ and $U \in \mathbb{F}_{p^q}^*$ that

$$\Sigma(\mathbb{T}_U) = 1[1] + \frac{p^q - 1}{O(\mathbb{T})}[O(\mathbb{T})].$$

**Example 3.2.2**

Let $p = 3, q = 1$, let

$$\begin{aligned} \mathbb{T} &= x^4 + x^3 + 1 + (x^5 + 2x^3 + x^2 + 2x + 2)\mathbb{F}_3[x], \\ \mathbb{T} &\in \frac{\mathbb{F}_3[x]}{(x^5 + 2x^3 + x^2 + 2x + 2)\mathbb{F}_3[x]} \cong \mathbb{F}_{3^5}. \end{aligned}$$

Then $O(\mathbb{T}) = 121$ and by lemma 3.2.3 we have, for all $U \in \frac{\mathbb{F}_3[x]}{(x^5+2x^3+x^2+2x+2)\mathbb{F}_3[x]}$,

$$\Sigma(\mathbb{T}_U) = 1[1] + \frac{3^5 - 1}{121}[121] = 1[1] + 2[121].$$

Now suppose $p = 3, q = 2$, the polynomial $x^5 + 2x^3 + x^2 + 2x + 2$ remains irreducible over $\mathbb{F}_9$. We represent $\mathbb{F}_9$ using $\frac{\mathbb{F}_3[x]}{(x^2+x+2)\mathbb{F}_3[x]}$. Let $a$ be a root of $x^2 + x + 2$, let

$$\mathbb{T} = x^3 + a + (x^5 + 2x^3 + x^2 + 2x + 2)\frac{\mathbb{F}_3[x]}{(x^2 + x + 2)\mathbb{F}_3[x]}.$$

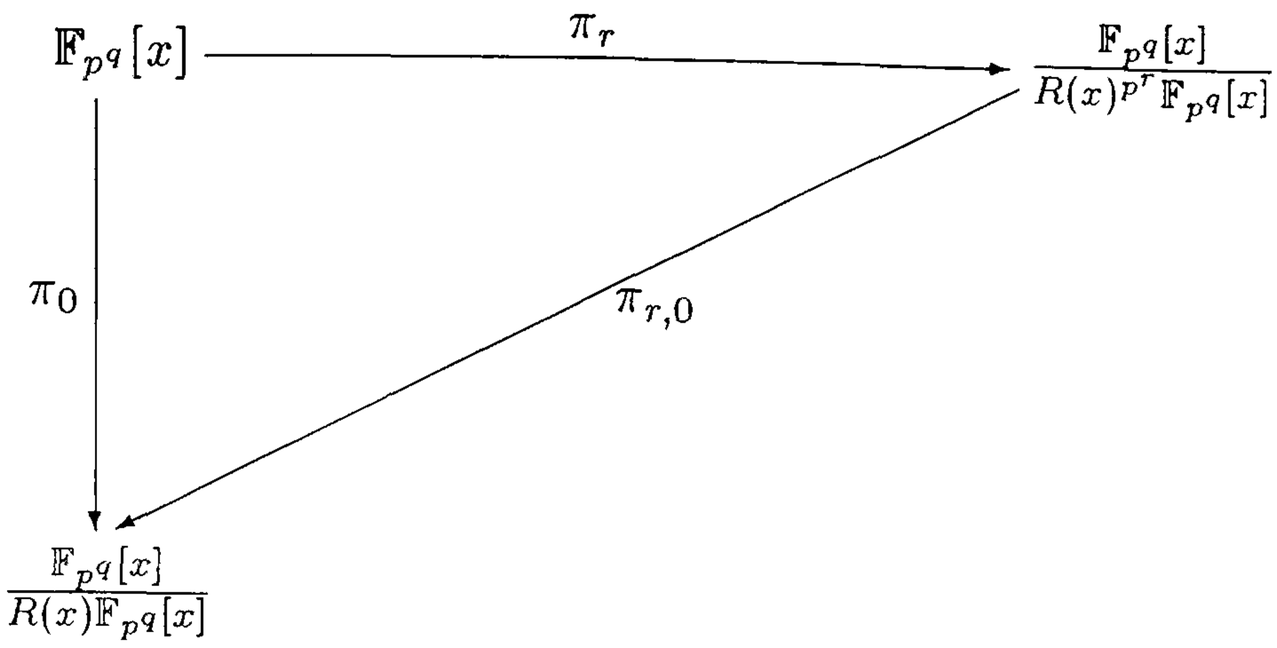


Figure 3.1: $\pi_{r,0} \circ \pi_r = \pi_0$.

One finds that $O(\mathbb{T}) = 7381$ and so for all $U$ one has that

$$\Sigma(\mathbb{T}_U) = 1[1] + \frac{3^{2.5}-1}{7381}[7381] = 1[1] + 8[7381]. \quad \blacklozenge$$

## 3.3 Dynamics in a single ring $\frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$, $r > 0$

We first deduce some properties of these rings. Let $d$ be the degree of $R(x)$. We shall denote the natural homomorphism from $\mathbb{F}_{pq}[x]$ onto $\frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$ by $\pi_r$ for any $r \in \mathbb{N}$. By the factor theorem (theorem A.1.1) there is a unique ring homomorphism $\pi_{r,0} : \frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]} \longrightarrow \frac{\mathbb{F}_{pq}[x]}{R(x)\mathbb{F}_{pq}[x]}$ satisfying $(\pi_{r,0} \circ \pi_r)(a) = \pi_0(a)$ for all $a \in \mathbb{F}_{pq}[x]$ (see figure 3.1). The kernel of $\pi_{r,0}$ consists of those elements $a(x) + R(x)^{p^r}\mathbb{F}_{pq}[x]$ such that $R(x)|a(x)$ and is thus clearly a nil ideal and (by the first isomorphism theorem)

$$\frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]} \Big/ \text{Ker } \pi_{r,0} \cong \frac{\mathbb{F}_{pq}[x]}{R(x)\mathbb{F}_{pq}[x]}, \tag{3.3.1}$$

hence Ker $\pi_{r,0}$ is a maximal ideal, in particular it is maximal amongst ideals consisting of nilpotent elements, hence we have proved:

**Lemma 3.3.1** *An element $\mathbb{T} \in \frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$ is nilpotent if and only if $R(x)|\mathbb{T}(x)$.* ■

**Lemma 3.3.2** *The ring $\frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$ is completely primary.*

Proof:

We have to show that every element of $\frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$ is either nilpotent or a unit. Let $\mathbb{T} \in \frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]} \setminus$ Ker $\pi_{r,0}$, then $\pi_{r,0}(\mathbb{T}) = \hat{\mathbb{T}}$, a unit. Let $L$ be the order of $\hat{\mathbb{T}}$ in the group of units of $\frac{\mathbb{F}_{pq}[x]}{R(x)\mathbb{F}_{pq}[x]}$ so that $\hat{\mathbb{T}}^L = 1$, it follows that $\mathbb{T}^L = 1 + \mathbb{T}_n$ where $\mathbb{T}_n \in$ Ker $\pi_{r,0}$, hence $\mathbb{T}^{Lp^r} = 1$ hence $\mathbb{T}$ is a unit and the result is proved. ■

We shall denote the group of units in $\frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$ by $U_{pq}(R, r)$.

**Lemma 3.3.3** *For given $p, q$ and $R(x)$ and $r$ one has*

$$\begin{aligned} |\text{Ker } \pi_{r,0}| &= p^{qd(p^r-1)}; \\ |U_{pq}(R,r)| &= p^{qd(p^r-1)}(p^{qd}-1). \end{aligned}$$

Proof:

That $|\text{Ker } \pi_{r,0}| = p^{qd(p^r-1)}$ follows from (3.3.1) by counting the numbers of elements in $\frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$ and $\frac{\mathbb{F}_{pq}[x]}{R(x)\mathbb{F}_{pq}[x]}$. The rest follows by subtraction. ■

We note that there is a ring homomorphism $\Phi : \frac{\mathbb{F}_{pq}[x]}{R(x)\mathbb{F}_{pq}[x]} \longrightarrow \frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$ given by

$$a(x) + R(x)\mathbb{F}_{pq}[x] \mapsto a(x)^{p^r} + R(x)^{p^r}\mathbb{F}_{pq}[x],$$

induced by the ring monomorphism $a(x) \mapsto a(x)^{p^r}$ on $\mathbb{F}_{pq}[x]$. Clearly Ker $\Phi = \{0\}$ hence $\Phi$ is a ring monomorphism, with image the subring of $\frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$ generated as a vector space over $\mathbb{F}_{pq}$ by the elements $1 + R(x)^{p^r}\mathbb{F}_{pq}[x]$, $x^{p^r} + R(x)^{p^r}\mathbb{F}_{pq}[x]$, ..., $x^{(d-1)p^r} + R(x)^{p^r}\mathbb{F}_{pq}[x]$. we shall denote this subring by $< 1, x^{p^r}, \ldots, x^{(d-1)p^r} >$. Thus $\frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$ can be regarded as a (ring) extension of $\frac{\mathbb{F}_{pq}[x]}{R(x)\mathbb{F}_{pq}[x]}$ or as an $\frac{\mathbb{F}_{pq}[x]}{R(x)\mathbb{F}_{pq}[x]}$−algebra if one so wishes.

### 3.3.1 Dynamics in $\frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$ when $U = 0$

As usual we let $\Pi(\mathbb{T})$ denote the length of the orbit that 1 evolves to under $\mathbb{T}$. It is clear that $(\phi_a)_0|\Pi(\mathbb{T})$ for all $a \in \frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$.

**Lemma 3.3.4** *Suppose $\mathbb{T} \in \frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$ is a unit, then $\mathbb{T}$ has a non-trivial period $l$ orbit, $l \geq 1$, if and only if $\mathbb{T}^l - 1$ is nilpotent.*

Proof:

Suppose $\mathbb{T}$ has a period $l$ orbit, $l \geq 1$, and that $a \neq 0$ is on this orbit hence

$$\mathbb{T}^l a = a \quad \Rightarrow \quad (\mathbb{T}^l - 1)a = 0$$

thus if $a$ is a unit then $\mathbb{T}^l - 1 = 0$ and if $a$ is not a unit then $\mathbb{T}^l - 1$ is a zero-divisor and hence nilpotent by lemma 3.3.1. If $\mathbb{T}^l - 1$ is nilpotent, $l \geq 0$, then either $\mathbb{T}^l = 1$ and all elements of $\frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^r}\mathbb{F}_{p^q}[x]}$ are on period $l$ orbits or $\mathbb{T}^l - 1$ is a zero-divisor hence there is some $a \neq 0$ such that $(\mathbb{T}^l - 1)a = 0$ hence $\mathbb{T}^l a = a$ and $a$ is on a period $l$ orbit. ■

Note that the number of units $\mathbb{T}$ with non-zero fixed points is $|\text{Ker } \pi_{r,0}|$ as, by remark A.1.1, if $\mathbb{T} - 1$ is nilpotent then $1 - (\mathbb{T} - 1) = -\mathbb{T}$ is a unit and if $\mathbb{T}$ is a unit with non-zero fixed points then $\mathbb{T} - 1$ is nilpotent. The proof of the following result can be found in appendix B.

**Lemma 3.3.5** *Let* $\mathbb{T} \in \frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^r}\mathbb{F}_{p^q}[x]}$, $\mathbb{T}$ *a unit, then*

(i) *If* $a$ *is a unit then* $a$ *is on an orbit of length* $\Pi(\mathbb{T})$ *under* $\mathbb{T}$.

(ii) *If* $a, b \in$ Ker $\pi_{r,0}$ *then if* $(\phi_a)_0 \neq (\phi_b)_0$ *then either* $(\phi_a)_0 | (\phi_b)_0$ *or* $(\phi_b)_0 | (\phi_a)_0$. ■

If $\mathbb{T} \in U_{p^q}(R, r)$ we wish to know what the minimal orbit length that occurs for a non-zero element of $\frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^r}\mathbb{F}_{p^q}[x]}$ under $\mathbb{T}$ is. If this minimal orbit length is less than $\Pi(\mathbb{T})$ then by lemma 3.3.5 the elements of such an orbit must be nilpotent. Denote this minimal orbit length by $L(\mathbb{T})$.

**Lemma 3.3.6** *Let* $\mathbb{T} \in U_{p^q}(R, r)$ *then* $L(\mathbb{T})$ *is equal to the order of* $\pi_{r,0}(\mathbb{T})$ *in* $\frac{\mathbb{F}_{p^q}[x]}{R(x)\mathbb{F}_{p^q}[x]}$.

Proof:

Let $L$ be the order of $\pi_{r,0}(\mathbb{T})$ in $\frac{\mathbb{F}_{p^q}[x]}{R(x)\mathbb{F}_{p^q}[x]}$ so that $\pi_{r,0}(\mathbb{T})^L = 1$, $L$ minimal, hence $\mathbb{T}^L - 1$ is in Ker $\pi_{r,0}$ so $\mathbb{T}$ has a period $L$ orbit by lemma 3.3.4. Now suppose that $\mathbb{T}^k - 1$ is nilpotent for some integer $k < L$, then applying $\pi_{r,0}$ shows that $\pi_{r,0}(\mathbb{T})^k = 1$, contradicting the minimality of $L$. ■

**Definition 3.3.1** *Let* $\mathcal{I} : \frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^r}\mathbb{F}_{p^q}[x]} \longrightarrow \{0, 1, \ldots, p^r\}$ *be the map given by*

$$\begin{aligned} a &\mapsto i \text{ if } R(x)^i | a(x) \text{ but } R(x)^{i+1} \nmid a(x),\ a \neq 0, \\ 0 &\mapsto p^r. \end{aligned}$$

**Theorem 3.3.1** *When* $\mathbb{T} \in U_{p^q}(R, r)$ *the orbits that can occur under* $\mathbb{T}$ *are of lengths* $1, L(\mathbb{T}), L(\mathbb{T})p, \ldots, L(\mathbb{T})p^{S(\mathbb{T})} = \Pi(\mathbb{T})$ *where*

$$S = \lceil s \rceil, \ s = r - \log_p(\mathcal{I}(\mathbb{T}^{L(\mathbb{T})} - 1)).$$

*Explicitly* $S = r - n$ *for* $p^n \leq \mathcal{I}(\mathbb{T}^{L(\mathbb{T})} - 1) < p^{n+1}$ *and* $S = 0$ *for* $\mathcal{I}(\mathbb{T}^{L(\mathbb{T})} - 1) = p^r$.

Proof:

Zero is always a fixed point. We look at the orbits of the nilpotent elements of $\frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$. By lemma 3.3.4 $\mathbb{T}^{L(\mathbb{T})} = 1 + \mathbb{T}_n$ where $\mathbb{T}_n$ is nilpotent with $\mathcal{I}(\mathbb{T}_n) = \mathcal{I}(\mathbb{T}^{L(\mathbb{T})} - 1) = I > 0$. By lemma 3.3.5, (ii), if any nilpotent element $b$ is on an orbit of length $(\phi_b)_0 > L(\mathbb{T})$ then $L(\mathbb{T})|(\phi_b)_0$. Thus any non-zero element is on an orbit of length $L(\mathbb{T})k$ for some $k \geq 1$. Now

$$\mathbb{T}^{L(\mathbb{T})k} = (1 + \mathbb{T}_n)^k = 1 + \sum_{u=1}^{k} \binom{k}{u} \mathbb{T}_n^u$$

and in particular

$$\mathbb{T}^{L(\mathbb{T})p^i} = 1 + \mathbb{T}_n^{p^i}, \ i \geq 1.$$

Let $a \in \text{Ker } \pi_{r,0}$ such that $a(x) = \alpha(x)R(x)^\beta$ where $R(x) \nmid \alpha(x)$ and $p^r > \beta > 0$. Let $i$ be such that

$$\begin{aligned} \beta + Ip^{i-1} &< p^r \\ \beta + Ip^i &\geq p^r \end{aligned}$$

so $\mathbb{T}^{L(\mathbb{T})p^{i-n}}a \neq a$ for $1 \leq n \leq i$ and $\mathbb{T}^{L(\mathbb{T})p^i}a = a$. Thus $L(\mathbb{T})|(\phi_a)_0|L(\mathbb{T})p^i$ so $(\phi_a)_0$ must be of the form $L(\mathbb{T})p^j, j \leq i$ but we cannot have $j < i$ by the above so $(\phi_a)_0 = L(\mathbb{T})p^i$. Thus all non-zero nilpotent elements are on orbits of lengths $L(\mathbb{T})p^i, 0 \leq i \leq S$, for some positive integer $S$. We claim $S$ is the least integer such that $Ip^S \geq p^r$, for then $\mathbb{T}^{L(\mathbb{T})p^S} - 1 = 0$ so $\Pi(\mathbb{T})|L(\mathbb{T})p^S$ but $L(\mathbb{T})p^S$ is an orbit length that occurs for some nilpotent elements, namely those with $1 \leq \mathcal{I}(a) \leq p^r - Ip^{S-1} - 1$, hence $L(\mathbb{T})p^S|\Pi(\mathbb{T})$ and so $L(\mathbb{T})p^S = \Pi(\mathbb{T})$ (and so the units are on orbits of length $L(\mathbb{T})p^S$). It remains to determine $S$. Let $s \in \mathbb{R}$ be the least number such that $Ip^s = p^r$ so $p^s = p^r/I$. Taking logarithms to the base $p$ yields

$$s = r - \log_p(I)$$

and clearly $S = \lceil s \rceil$. The last part of the theorem follows on examination of $\log_p(I)$ as $I$ takes on its possible values. ■

Note the use of lemma 3.3.5, (ii), in the proof of theorem 3.3.1, the theorem can be proved without the use of lemma 3.3.5 but the proof is longer (and uglier).

Note that theorem 3.3.1 holds for $r = 0$ for in that case

$$\mathcal{I}(\mathbb{T}^{O(\mathbb{T})} - 1) = \mathcal{I}(1 - 1) = \mathcal{I}(0) = p^0 = 1$$

and so $S = 0 - \log_p 1 = 0$ and we get orbit lengths 1 and $O(\mathbb{T})$.

We now know the orbit lengths that can occur under $\mathbb{T}$, our next task is to count the number of orbits of a given length. It is evident from the proof of theorem 3.3.1 that the nilpotent elements $A$ on orbits of length $Lp^e$ are those satisfying

$$\begin{aligned} \mathcal{I}(\mathbb{T}^L - 1)p^e + \mathcal{I}(A) &\geq p^r, \\ \mathcal{I}(\mathbb{T}^L - 1)p^{e-1} + \mathcal{I}(A) &< p^r, \end{aligned}$$

thus to count the number of orbits of a given length it is useful to know exactly how many nilpotent elements have canonical representatives that are divisible by a particular power of $R(x)$ and no higher power of $R(x)$, to this end we make the following definitions.

**Definition 3.3.2**

$$\begin{aligned} A(l) &= \{a(x) \in \mathbb{F}_{p^q}[x] : \deg a(x) \leq l, a \neq 0\}; \\ \mathcal{D}_R(l,s) &= \{a(x) \in \mathbb{F}_{p^q}[x] : \deg a(x) \leq l, R^s(x) \mid a(x), \\ &\qquad R^{s+1}(x) \nmid a(x)\}, \ l \geq d, s \geq 0. \end{aligned}$$

We shall want the following properties of the sets defined in 3.3.2, the proof can be found in appendix B.

**Lemma 3.3.7** *We have, for suitable $l$ and $s$, that*

(i) $\mid A(l) \mid = p^{q(l+1)} - 1$.

(ii) $\mathcal{D}_R(l,s) = R(x)^s A(l - sd) \setminus R(x)^{s+1} A(l - (s+1)d)$.

(iii) $\mid \mathcal{D}_R(l,s) \mid = p^{q(l-sd-d+1)}(p^{qd} - 1)$ *and in particular*

$$\mid \mathcal{D}_R(p^r d - 1, s) \mid = p^{(p^r - s - 1)qd}(p^{qd} - 1). \quad \blacksquare$$

Note that for any positive integers $n_1$ and $n_2$ with $n_1 \neq n_2$one has $\mathcal{D}_R(l, n_1) \cap \mathcal{D}_R(l, n_2) = \emptyset$, hence for any finite set of positive integers indexed by $I \subset \mathbb{N}$

$$\left| \bigcup_{i \in I} \mathcal{D}_R(l, n_i) \right| = \sum_{i \in I} |\mathcal{D}_R(l, n_i)|. \tag{3.3.2}$$

For the sake of brevity one can identify $\mathcal{D}_R(p^r d - 1, n)$ with the set

$$\{a(x) + R(x)^{p^r}\mathbb{F}_{p^q}[x] : a(x) \in \mathcal{D}_R(p^r d - 1, n)\} \subset \frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^r}\mathbb{F}_{p^q}[x]}.$$

In particular one can identify $\mathcal{D}_R(p^r d - 1, 0)$ with $U_{p^q}(R, r)$ as $\mathcal{D}_R(p^r d - 1, 0)$ is the set of polynomials in $\mathbb{F}_{p^q}[x]$ of degree less than or equal to $p^r d - 1$ not divisible by $R(x)$ as these are the canonical representatives of the elements of $U_{p^q}(R, r)$. The meaning of $\mathcal{D}_R(p^r d - 1, n)$ should be clear from context.

Using definition 3.3.2 and lemma 3.3.7 we can partition $\frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^r}\mathbb{F}_{p^q}[x]}$ into a disjoint union of subsets with the property that all the elements in a particular subset are on orbits of a particular length and the elements of such a subset are all the elements on orbits of that length.

**Lemma 3.3.8** *The elements of* $\frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^r}\mathbb{F}_{p^q}[x]}$ *on prime period* $L(\mathbb{T})p^e$ *orbits,* $0 < e < S$, *are the elements of*

$$\bigcup_{i \,=\, p^r - \mathcal{I}(\mathbb{T}^{L(\mathbb{T})}-1)p^e}^{p^r - \mathcal{I}(\mathbb{T}^{L(\mathbb{T})}-1)p^{e-1}-1} \mathcal{D}_R(p^r d - 1, i)$$

*whilst those on orbits of length* $L(\mathbb{T})$ *are the elements of*

$$\bigcup_{i \,=\, p^r - \mathcal{I}(\mathbb{T}^{L(\mathbb{T})}-1)}^{p^r - 1} \mathcal{D}_R(p^r d - 1, i)$$

*and those on orbits of length* $\Pi(\mathbb{T}) = L(\mathbb{T})p^S$ *are the elements of*

$$\bigcup_{i \,=\, 0}^{p^r - \mathcal{I}(\mathbb{T}^{L(\mathbb{T})}-1)p^{S-1}-1} \mathcal{D}_R(p^r d - 1, i).$$

Proof:

Suppose first that $0 < e < S$. Elements on orbits of length $L(\mathbb{T})p^e$ must be nilpotent. Let $a \in \text{Ker } \pi_{r,0} \setminus \{0\}$, for $a$ to be on an orbit of length $L(\mathbb{T})p^e$ we require that

$$\begin{aligned} \mathcal{I}(\mathbb{T}^{L(\mathbb{T})} - 1)p^e + \mathcal{I}(a) &\geq p^r \text{ and} \\ \mathcal{I}(\mathbb{T}^{L(\mathbb{T})} - 1)p^{e-1} + \mathcal{I}(a) &< p^r \end{aligned}$$

so that

$$p^r - \mathcal{I}(\mathbb{T}^{L(\mathbb{T})} - 1)p^{e-1} > \mathcal{I}(a) \geq p^r - \mathcal{I}(\mathbb{T}^{L(\mathbb{T})} - 1)p^e$$

and the first part follows. For $e = 0$ we require

$$\begin{aligned} \mathcal{I}(\mathbb{T}^{L(\mathbb{T})} - 1) + \mathcal{I}(a) &\geq p^r \text{ and} \\ \mathcal{I}(a) &< p^r \end{aligned}$$

and the second part follows. For nilpotent elements on orbits of length $\mathcal{I}(\mathbb{T}^{L(\mathbb{T})} - 1)p^S$ we have

$$1 \leq \mathcal{I}(a) < p^r - \mathcal{I}(\mathbb{T}^{L(\mathbb{T})} - 1)p^{S-1}$$

and allow $\mathcal{I}(a) = 0$ to include the units and the last part follows. ■

The next result enables us to count the number of elements of $\frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^r}\mathbb{F}_{p^q}[x]}$ on an orbit of a given length.

**Lemma 3.3.9** *For positive integers $s_1, s_2$ with $p^r - 1 > s_2 > s_1$ we have that*

$$\left| \bigcup_{i=s_1}^{s_2} \mathcal{D}_R(p^r d - 1, i) \right| = p^{(p^r - s_1)qd} - p^{(p^r - s_2 - 1)qd}.$$

Proof:

This is easily verified using (3.3.2) and lemma 3.3.7. ■

We can now obtain the cycle set of any $\mathbb{T} \in U_{p^q}(R, r)$, the proof of the following theorem follows immediately from lemmas 3.3.8 and 3.3.9. Of course if $\mathbb{T} = 1$ then $\Sigma(\mathbb{T}) = p^{qdp^r}[1]$ and so we exclude this trivial case.

**Theorem 3.3.2** *When $\mathbb{T}$ is a unit, $\mathbb{T} \neq 1$, with $I = \mathcal{I}(\mathbb{T}^{L(\mathbb{T})} - 1)$ and $S$ as defined earlier, the cycle set for $\mathbb{T}$ is, when $S > 0$:*

$$\begin{aligned} \Sigma(\mathbb{T}) &= 1[1] + \frac{p^{Iqd} - 1}{L(\mathbb{T})}[L(\mathbb{T})] + \\ &\sum_{j=1}^{S-1} \frac{p^{Iqdp^j} - p^{Iqdp^{j-1}}}{L(\mathbb{T})p^j}[L(\mathbb{T})p^j] + \frac{p^{p^r qd} - p^{Ip^{S-1}qd}}{L(\mathbb{T})p^S}[L(\mathbb{T})p^S], \end{aligned}$$

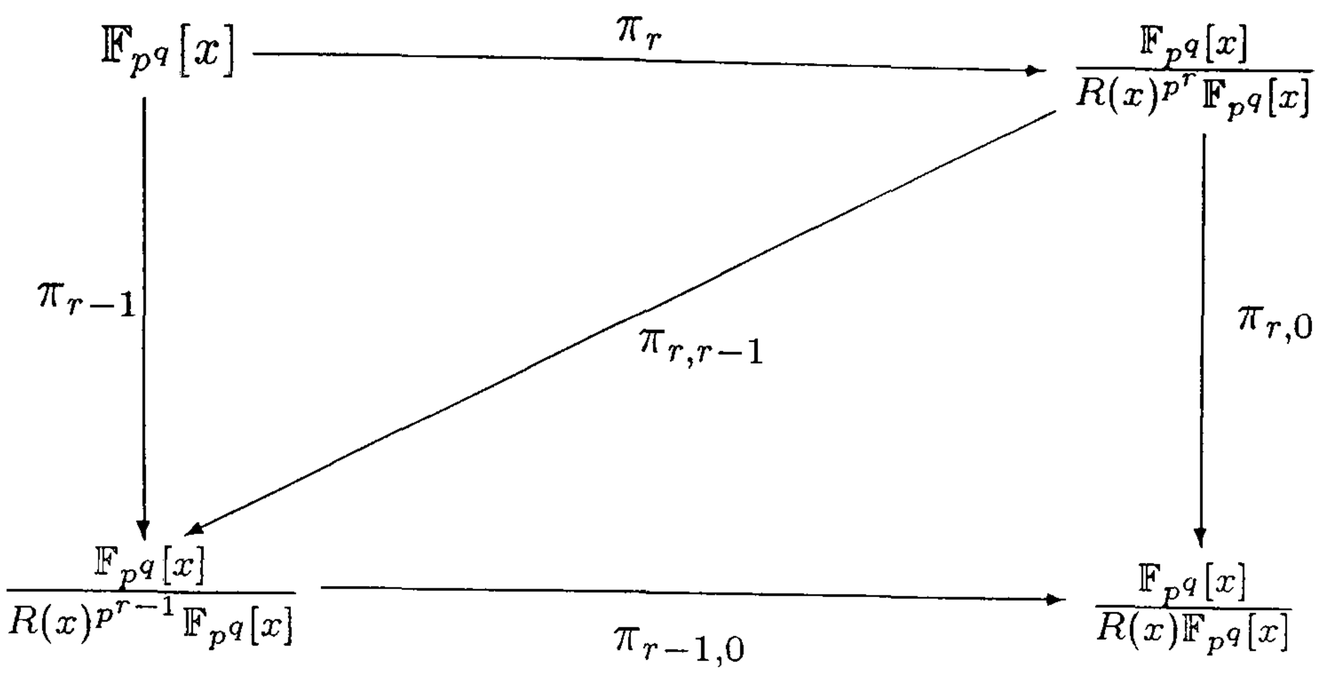


Figure 3.2: This diagram commutes.

*When $S = 0$ one has*

$$\Sigma(\mathbb{T}) = 1[1] + \frac{p^{Iqd} - 1}{L(\mathbb{T})}[L(\mathbb{T})]. \quad \blacksquare$$

Theorem 3.3.2 holds for $r = 0$ for in that case, as noted earlier, $S = 0$ and we regain equation 3.2.1.

From theorem 3.3.2 we see that $\Sigma(\mathbb{T})$ is completely determined by knowledge of $L(\mathbb{T})$ and hence $\mathcal{I}(\mathbb{T}^{L(\mathbb{T})} - 1)$. We now establish some connections between behaviour in $\frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$ and in $\frac{\mathbb{F}_{pq}[x]}{R(x)^{p^{r-1}}\mathbb{F}_{pq}[x]}$.

**Remark 3.3.1** *By the factor theorem (theorem A.1.1), for each $r > 1$, there is a unique ring homomorphism*

$$\pi_{r,r-1} : \frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]} \longrightarrow \frac{\mathbb{F}_{pq}[x]}{R(x)^{p^{r-1}}\mathbb{F}_{pq}[x]}$$

*such that figure 3.2 commutes, where $\pi_r$ and $\pi_{r-1}$ are the natural projections. $\pi_{r,r-1}$ satisfies*

$$\pi_{r,r-1}(\alpha(x) + R(x)^{p^r}\mathbb{F}_{pq}[x]) = \pi_{r-1}(\alpha(x)).$$

Proof:

It follows from the factor theorem A.1.1, on putting $f = \pi_{r-1}$ and $\pi = \pi_r$, that the upper triangle commutes. It is a simple matter to verify that the rest of figure 3.2 commutes, in particular $\pi_{r,0} = \pi_{r-1,0} \circ \pi_{r,r-1}$. $\blacksquare$

More generally there are homomorphisms

$$\pi_{r,r-j} : \frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]} \longrightarrow \frac{\mathbb{F}_{pq}[x]}{R(x)^{p^{r-j}}\mathbb{F}_{pq}[x]}, \quad 0 < j \leq r.$$

These homomorphisms commute, *i.e.*

$$\pi_{r-j,r-j-k} \circ \pi_{r,r-j} = \pi_{r,r-j-k}, \quad 0 < j \leq r, 0 < k \leq r-j.$$

We can now relate the relevant properties of $\mathbb{T} \in \frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$ and $\pi_{r,r-1}(\mathbb{T})$.

**Lemma 3.3.10** *Let* $\mathbb{T} \in \frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$ *and let* $\mathbb{T}' \in \frac{\mathbb{F}_{pq}[x]}{R(x)^{p^{r-1}}\mathbb{F}_{pq}[x]}$, *where* $\mathbb{T}' = \pi_{r,r-1}(\mathbb{T})$.

*Then*

(i) *For* $\mathbb{T}$ *and* $\mathbb{T}'$ *units,* $L(\mathbb{T}) = L(\mathbb{T}')$.

(ii) $\mathbb{T} \in \text{Ker } \pi_{r,0} \Leftrightarrow \mathbb{T}' \in \text{Ker } \pi_{r-1,0}$.

(iii) *If* $\mathbb{T} \in \text{Ker } \pi_{r,0}$ *and* $\mathcal{I}(\mathbb{T}) < p^{r-1}$ *then*

$$\mathcal{I}(\mathbb{T}') = \mathcal{I}(\mathbb{T})$$

*but if* $\mathcal{I}(\mathbb{T}) \geq p^{r-1}$ *then*

$$\mathcal{I}(\mathbb{T}') = p^{r-1}.$$

(iv) *For* $\mathbb{T}$ *and* $\mathbb{T}'$ *units let* $\Pi(\mathbb{T}) = L(\mathbb{T})p^{S_{\mathbb{T}}}$ *and* $\Pi(\mathbb{T}') = L(\mathbb{T}\,)p^{S_{\mathbb{T}'}}$, *then*

$$S_{\mathbb{T}'} = S_{\mathbb{T}} - 1,$$

*unless* $S_{\mathbb{T}} = 0$ *in which case* $S_{\mathbb{T}'} = 0$.

Proof:

(i) as $\pi_{r,0} = \pi_{r-1,0} \circ \pi_{r,r-1}$, we have $O(\mathbb{T}) = O(\mathbb{T}')$ so $L(\mathbb{T}) = L(\mathbb{T}')$.

(ii) If $\mathbb{T} \in \text{Ker } \pi_{r,0}$ then $\mathbb{T}'$ is nilpotent as the homomorphic image of a nilpotent element must be nilpotent. If $\mathbb{T}'$ is nilpotent then $\mathbb{T}$ is a preimage of $\mathbb{T}'$ under $\pi_{r,r-1}$ so $\mathbb{T} = \mathbb{T}' + \mathbb{T}''$ where $\pi_{r,r-1}(\mathbb{T}'') = 0$ so $R^{p^{r-1}}(x) | \mathbb{T}''(x)$ so $R(x) | \mathbb{T}(x)$ so $\mathbb{T}$ is nilpotent.

(iii) Let $\mathbb{T} \in \text{Ker } \pi_{r,0}$ with $I = \mathcal{I}(\mathbb{T}) < p^{r-1}$ so $\mathbb{T} = \alpha R^I = \alpha(x)R(x)^I + R(x)^{p^r}\mathbb{F}_{pq}[x]$ where $R(x) \nmid \alpha(x)$. Then

$$\begin{aligned} \mathbb{T}' &= \pi_{r,r-1}(\mathbb{T}) \\ &= \pi_{r,r-1}(\alpha)\pi_{r,r-1}(R^I). \end{aligned}$$

$R(x) \nmid \alpha(x)$ and $I < p^{r-1}$ imply that $R(x) \nmid \pi_{r,r-1}(\alpha)(x)$ and $R(x)^I | \pi_{r,r-1}(R^I)(x)$ hence $\mathcal{I}(\mathbb{T}') = I$. If $I = \mathcal{I}(\mathbb{T}) \geq p^{r-1}$ then

$$\mathbb{T}' = \pi_{r,r-1}(\mathbb{T}^{L(\mathbb{T})} - 1) = 0$$

so by definition $\mathcal{I}(\mathbb{T}') = p^{r-1}$.

(iv) For $\mathcal{I}(\mathbb{T}^{L(\mathbb{T})} - 1) < p^{r-1}$ we have, by parts (i) and (iii), for $S_{\mathbb{T}} \neq 0$

$$\begin{aligned} S_{\mathbb{T}'} &= \lceil r - 1 - \log_p(\mathcal{I}(\mathbb{T}'^{L(\mathbb{T})} - 1)) \rceil \\ &= \lceil r - \log_p(\mathcal{I}(\mathbb{T}^{L(\mathbb{T})} - 1)) \rceil - 1 \\ &= S_{\mathbb{T}} - 1. \end{aligned}$$

When $I = \mathcal{I}(\mathbb{T}^{L(\mathbb{T})} - 1) \geq p^{r-1}$ one has by theorem 3.3.1 that $S_{\mathbb{T}} = 1$. Then, by part (iii), one has

$$\begin{aligned} S_{\mathbb{T}'} &= \lceil r - 1 - \log_p(p^{r-1}) \rceil \\ &= 0 \\ &= S_{\mathbb{T}} - 1. \end{aligned}$$

When $S_{\mathbb{T}} = 0$ one has $\mathcal{I}(\mathbb{T}^{L} - 1) = p^r$ and so by part (iii) it follows that $\mathcal{I}(\mathbb{T}'^{L} - 1) = p^{r-1}$, hence $S_{\mathbb{T}'} = 0$. ■

**Theorem 3.3.3** *Let* $\mathbb{T} \in \frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$ *and let* $\mathbb{T}' \in \frac{\mathbb{F}_{pq}[x]}{R(x)^{p^{r-1}}\mathbb{F}_{pq}[x]}$, *where* $r \geq 1$ *and* $\mathbb{T}' = \pi_{r,r-1}(\mathbb{T})$. *Then with* $I = \mathcal{I}(\mathbb{T}^{L(\mathbb{T})} - 1)$ *and* $S = S_{\mathbb{T}}$ *one has that*

$$\Sigma(\mathbb{T}) = \Sigma(\mathbb{T}') + \frac{p^{qdIp^{S-1}} - p^{qdp^{r-1}}}{L(\mathbb{T})p^{S-1}}[L(\mathbb{T})p^{S-1}] + \frac{p^{qdp^r} - p^{qdIp^{S-1}}}{L(\mathbb{T})p^S}[L(\mathbb{T})p^S]$$

*unless* $I$ *is a power of* $p$ *when*

$$\Sigma(\mathbb{T}) = \Sigma(\mathbb{T}') + \frac{p^{qdp^r} - p^{qdp^{r-1}}}{L(\mathbb{T})p^S}[L(\mathbb{T})p^S].$$

Proof:

We know from lemma 3.3.10 that $L(\mathbb{T}') = L(\mathbb{T})$. When $\mathcal{I}(\mathbb{T}'^{L(\mathbb{T})} - 1) = I$ then, by lemma 3.3.10, $I < p^{r-1}$ and $S_{\mathbb{T}'} = S - 1$ and one has

$$\begin{aligned} \Sigma(\mathbb{T}') &= 1[1] + \frac{p^{qdI} - 1}{L(\mathbb{T})}[L(\mathbb{T})] + \sum_{j=1}^{S-2} \frac{p^{qdIp^j} - p^{qdIp^{j-1}}}{L(\mathbb{T})p^j}[L(\mathbb{T})p^j] + \\ &\quad \frac{p^{qdp^{r-1}} - p^{qdIp^{S-2}}}{L(\mathbb{T})p^{S-1}}[L(\mathbb{T})p^{S-1}] \end{aligned}$$

and

$$\begin{aligned}\Sigma(\mathbb{T}) &= 1[1]+\frac{p^{qdI}-1}{L(\mathbb{T})}[L(\mathbb{T})]+\sum_{j=1}^{S-1}\frac{p^{qdIp^j}-p^{qdIp^{j-1}}}{L(\mathbb{T})p^j}[L(\mathbb{T})p^j]+\\ &\quad \frac{p^{qdp^r}-p^{qdIp^{S-1}}}{L(\mathbb{T})p^S}[L(\mathbb{T})p^S]\\ &= 1[1]+\frac{p^{qdI}-1}{L(\mathbb{T})}[L(\mathbb{T})]+\sum_{j=1}^{S-2}\frac{p^{qdIp^j}-p^{qdIp^{j-1}}}{L(\mathbb{T})p^j}[L(\mathbb{T})p^j]+\\ &\quad \frac{p^{qdIp^{S-1}}-p^{qdIp^{S-2}}}{L(\mathbb{T})p^{S-1}}[L(\mathbb{T})p^{S-1}]+\frac{p^{qdp^r}-p^{qdIp^{S-1}}}{L(\mathbb{T})p^S}[L(\mathbb{T})p^S]\\ &= \Sigma(\mathbb{T}')-\frac{p^{qdp^{r-1}}-p^{qdIp^{S-2}}}{L(\mathbb{T})p^{S-1}}[L(\mathbb{T})p^{S-1}]+\\ &\quad \frac{p^{qdIp^{S-1}}-p^{qdIp^{S-2}}}{L(\mathbb{T})p^{S-1}}[L(\mathbb{T})p^{S-1}]+\frac{p^{qdp^r}-p^{qdIp^{S-1}}}{L(\mathbb{T})p^S}[L(\mathbb{T})p^S].\end{aligned}$$

The terms in $[L(\mathbb{T})p^{S-1}]$ add to give $\frac{p^{qdIp^{S-1}}-p^{qdp^{r-1}}}{L(\mathbb{T})p^{S-1}}[L(\mathbb{T})p^{S-1}]$.

If $I=p^m$ where $0<m<r-1$ then

$$S=s=r-\log_p(p^m)=r-m$$

so

$$p^{qdIp^{S-1}}-p^{qdp^{r-1}}=p^{qdp^{m+r-m-1}}-p^{qdp^{r-1}}=0.$$

If $I\geq p^{r-1}$ there are three cases, but in all cases one has $\mathcal{I}(\mathbb{T}'^{L(\mathbb{T})}-1)=p^{r-1}$ and hence $S_{\mathbb{T}'}=0$ and so

$$\Sigma(\mathbb{T}')=1[1]+\frac{p^{p^{r-1}qd}-1}{L(\mathbb{T})}[L(\mathbb{T})].$$

Firstly suppose that $I=p^r$ then $S=0$ and

$$\begin{aligned}\Sigma(\mathbb{T}) &= 1[1]+\frac{p^{p^rqd}-1}{L(\mathbb{T})}[L(\mathbb{T})]\\ &= 1[1]+\frac{p^{p^{r-1}qd}-1}{L(\mathbb{T})}[L(\mathbb{T})]+\frac{p^{p^rqd}-p^{p^{r-1}qd}}{L(\mathbb{T})}[L(\mathbb{T})]\\ &= \Sigma(\mathbb{T}')+\frac{p^{p^rqd}-p^{p^{r-1}qd}}{L(\mathbb{T})}[L(\mathbb{T})].\end{aligned}$$

Secondly suppose that $I = p^{r-1}$, then $S = 1$ and

$$\begin{aligned}\Sigma(\mathbb{T}) &= 1[1] + \frac{p^{p^{r-1}qd} - 1}{L(\mathbb{T})}[L(\mathbb{T})] + \frac{p^{p^r qd} - p^{p^{r-1}qd}}{pL(\mathbb{T})}[pL(\mathbb{T})] \\ &= \Sigma(\mathbb{T}') + \frac{p^{p^r qd} - p^{p^{r-1}qd}}{pL(\mathbb{T})}[pL(\mathbb{T})].\end{aligned}$$

Thirdly suppose that $I = p^{r-1} + v$, $0 < v < p^{r-1}(p-1)$, then $S = 1$ and

$$\begin{aligned}\Sigma(\mathbb{T}) &= 1[1] + \frac{p^{(p^{r-1}+v)qd} - 1}{L(\mathbb{T})}[L(\mathbb{T})] + \frac{p^{p^r qd} - p^{(p^{r-1}+v)qd}}{pL(\mathbb{T})}[pL(\mathbb{T})] \\ &= 1[1] + \frac{p^{(p^{r-1})qd} - 1}{L(\mathbb{T})}[L(\mathbb{T})] + \frac{p^{(p^{r-1}+v)qd} - p^{p^{r-1}qd}}{L(\mathbb{T})}[L(\mathbb{T})] \\ &\quad + \frac{p^{p^r qd} - p^{(p^{r-1}+v)qd}}{pL(\mathbb{T})}[pL(\mathbb{T})] \\ &= \Sigma(\mathbb{T}') + \frac{p^{(p^{r-1}+v)qd} - p^{p^{r-1}qd}}{L(\mathbb{T})}[L(\mathbb{T})] + \frac{p^{p^r qd} - p^{(p^{r-1}+v)qd}}{pL(\mathbb{T})}[pL(\mathbb{T})],\end{aligned}$$

which is of the required form. ■

We conclude this section with a lemma that will be very useful in chapter 4.

**Lemma 3.3.11** *Let* $\{\mathbb{T}_i\}_{i\in\mathbb{N}}$ *be such that* $\mathbb{T}_i \in \frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^i}\mathbb{F}_{p^q}[x]}$ *and* $\pi_{i+1,i}(\mathbb{T}_{i+1}) = \mathbb{T}_i$ *for all* $i \in \mathbb{N}$, *then*

(i) *If* $\mathbb{T}_0$ *is non-zero then* $\mathbb{T}_i$ *is a unit for all* $i \in \mathbb{N}$ *and* $L(\mathbb{T}_i) = L(\mathbb{T}_0) = O(\mathbb{T}_0)$ *for all* $i \in \mathbb{N}$.

(ii) *If* $\mathbb{T}_0 = 0$ *then* $\mathbb{T}_i$ *is nilpotent for all* $i \in \mathbb{N}$.

(iii) *If* $\mathbb{T}_0 = 0$ *and there is some integer* $j > 0$ *such that* $\mathbb{T}_j \neq 0$ *then*

$$\mathcal{I}(\mathbb{T}_{j+n}) = \mathcal{I}(\mathbb{T}_j) \quad \textit{for all } n \geq 0.$$

(iv) *If* $\mathbb{T}_0 \neq 0$ *and there is some integer* $j > 0$ *such that* $\mathbb{T}_j^{L(\mathbb{T}_0)} - 1 \neq 0$ *then* $S_{\mathbb{T}_j+n} = n + S_{\mathbb{T}_j}$ *for all* $n \in \mathbb{N}$.

Proof:

(i) Follows from lemma 3.3.10, (i).

(ii) Follows from lemma 3.3.10, (ii).

(iii) Suppose $\mathbb{T}_j \neq 0$ for some $j > 0$, then by lemma 3.3.10, (iii), $\mathcal{I}(\mathbb{T}_{j+1}) = \mathcal{I}(\mathbb{T}_j)$

unless $\mathcal{I}(\mathbb{T}_{j+1}) \geq p^j$ but in that case $\mathbb{T}_j = 0$, a contradiction. The result now follows by induction.

(iv) Follows from part (iii) and lemma 3.3.10, (iv). ■

We shall see in chapter 4, lemma 4.2.4, that when the set $\{\mathbb{T}_i\}_{i\in\mathbb{N}}$ described in lemma 3.3.11 corresponds to an additive cellular automata rule then the conditions of parts (iii) and (iv), *i.e.* that there is some integer $j > 0$ such that $\mathbb{T}_j \neq 0$ or $\mathbb{T}_j^{L(\mathbb{T}_j)} - 1 \neq 0$, are always satisfied. This makes the application of theorem 3.3.3 easy for $i > j$ as then, with $L = L(\mathbb{T}_0)$, $\mathcal{I}(\mathbb{T}_i^L - 1) = \mathcal{I}(\mathbb{T}_j^L - 1)$ if $\mathbb{T}_0$ (and hence $\mathbb{T}_i$ for all $i \in \mathbb{N}$) is a unit and so one does not need to recompute $\mathcal{I}(\mathbb{T}_i^L - 1)$ as $i$ increases and one can just "turn the handle" and add cycle terms repeatedly to obtain the cycle set for $\mathbb{T}_i$ for any $i > j$.

### 3.3.2 Transient structure for nilpotent $\mathbb{T}$

When $r > 0$ the transient structure under non-zero, nilpotent $\mathbb{T}$ is non-trivial. Note that the results in this section hold for $r = 0$, for instance in lemma 3.3.12, for if $\mathcal{I}(\mathbb{T}) > 0$ and $r = 0$ then $\mathbb{T} = 0$.

**Lemma 3.3.12** *Let $\mathbb{T} \in \mathcal{D}_R(p^r d - 1, I), I > 0$ then the tree height under $\mathbb{T}$ is $T = \lceil p^r/I \rceil$, the least integer such that $TI \geq p^r$. If $I = 1$ then $T = p^r$ and the leaves are the units. If $I > 1$ the leaves are the elements of*

$$\bigcup_{0\leq I_a<I} \mathcal{D}_R(p^r d - 1, I_a)$$

*and the elements at height $t$ in the tree are the elements of*

$$\bigcup_{I_a=p^r-tI}^{p^r-(t-1)I-1} \mathcal{D}_R(p^r d - 1, I_a).$$

Proof:

We have $\mathbb{T} = \alpha R^I$ where $R(x) \nmid \alpha(x)$. Clearly $\mathbb{T}^T = 0$ if and only if $IT \geq p^r$ so $T = \lceil p^r/I \rceil$. By lemma 2.1.5, (ii) the units are leaves. If $I = 1$ let $a \neq 0$ be nilpotent, $a\beta R^J$, where $R(x) \nmid \beta(x)$ and $J \geq 1$, then

$$\mathbb{T}^J \beta(\alpha^{-1})^J = a$$

so $a$ is the predecessor after $J$ time steps of a unit, clearly in this case $T = p^r$. If $I > 1$, if $a = \beta R^{I_a}$ where $0 < I_a < I$ and $R(x) \nmid \beta(x)$ then $a$ has no predecessor under $\mathbb{T}$, for assume there is some $b$ with $\mathbb{T}b = a$ then $\alpha R^I b = \beta R^{I_a}$ but $I_a < I$ and by examining this in $\mathbb{F}_{pq}[x]$ one obtains a contradiction in the usual manner. If $I_a \geq I$ then $a$ has a predecessor by the same argument as used when $I = 1$. Thus the elements without predecessors are the units and those nilpotent $a$ with $I_a < I$, i.e. the elements of

$$\bigcup_{0 \leq I_a < I} \mathcal{D}_R(p^r d - 1, I_a).$$

Finally, suppose that $\mathbb{T}^t a = 0$ but $\mathbb{T}^{t-1} a \neq 0$, then one must have that $tI + I_a \geq p^r$ but $(t-1)I + I_a < p^r$, hence

$$p^r - tI \leq I_a < p^r - (t-1)I$$

and the desired result follows. ■

Applying lemma 3.3.9 to lemma 3.3.12 we see that the number of leaves is

$$p^{(p^r - I)qd}(p^{Iqd} - 1), \tag{3.3.3}$$

the number of leaves that are not units is

$$p^{(p^r - I)qd}(p^{(I-1)qd} - 1), \tag{3.3.4}$$

and the number of elements at height t is

$$p^{(t-1)Iqd}(p^{Iqd} - 1). \tag{3.3.5}$$

Note that when $I > 1$ not all the leaves need be at the maximum height.

**Example 3.3.1**

If $I = p^r - 1$ then the only non-zero elements with predecessors are those of the form $\beta R^{p^r - 1}$, $R \nmid \beta$. The units are at height 2 and the non-units of the form $\gamma R^{p^r - 1 - j}$, $p^r - 1 > j > 0$, $R \nmid \gamma$, are at height 1. ♦

Note that any $a \in \frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$ can be written as $\beta R^{I_a}$ for some unit $\beta$ and $p^r - 1 \geq I_a \geq 0$.

We now know the numbers of elements at given heights, however this is not sufficient to completely characterise the state transition graph, we also need information on the in-degrees of the vertices, to this end we need the following, somewhat technical, lemma, whose proof can be found in appendix B, section B.2.

**Lemma 3.3.13** *Let* $\mathbb{T} \in \mathcal{D}_R(p^r d - 1, I), I > 0$. *Let* $\beta_1, \beta_2 \in U_{p^q}(R, r)$, *then for* $I_a \geq 0$ *and* $L > 0$

$$0 \neq \mathbb{T}^L \beta_1 R^{I_a} = \mathbb{T}^L \beta_2 R^{I_a} \Leftrightarrow R(x)^{p^r - LI - I_a} \mid \beta_1(x) - \beta_2(x)$$

*and if* $I_a \neq I_{a'}$ *for* $IL + I_a < p^r$, $IL + I_{a'} < p^r$ *then* $\mathbb{T}^L \beta_1 R^{I_a} \neq \mathbb{T}^L \beta_2 R^{I_{a'}}$. ■

**Corollary 3.3.1** *If* $a$ *is a unit and* $b$ *is nilpotent then* $\mathbb{T}a \neq \mathbb{T}b$.

Proof:

If $a$ is a unit then $I_a = \mathcal{I}(a) = 0$ but if $b$ is nilpotent then $I_b > 0$ hence the result follows from lemma 3.3.13. ■

We can now use lemma 3.3.13 and corollary 3.3.1 to find the in-degrees of all vertices in the state transition diagram.

**Theorem 3.3.4** *When* $\mathbb{T}$ *is nilpotent the in-degree of every vertex apart from zero in the state transition graph is* $p^{Iqd}$ *while that of zero is* $p^{Iqd} - 1$, *where* $I = \mathcal{I}(\mathbb{T})$.

Proof:

By corollary 3.3.1 all the predecessors of a particular element are either units or nilpotent but not a mixture of both. Suppose first that $a$ and $b$ are units with $\mathbb{T}a = \mathbb{T}b$ ($\neq 0$ as $a, b$ are units), then by lemma 3.3.13 we must have $R(x)^{p^r - I} | a(x) - b(x)$ so

$$a - b = \alpha \in \bigcup_{i=p^r-I}^{p^r-1} \mathcal{D}_R(p^r d - 1, i).$$

Fix $a$, then all such $b$ are of the form $b = a + \alpha$, so (including $a$) the number of predecessors of $\mathbb{T}a$ is

$$\left| \bigcup_{i=p^r-I}^{p^r-1} \mathcal{D}_R(p^r d - 1, i) \right| + 1.$$

Now using lemma 3.3.9 gives the number of predecessors as

$$p^{(p^r - p^r + I)qd} - p^{(p^r - p^r + 1 - 1)qd} + 1 = p^{Iqd}.$$

For $a$ and $b$ nilpotent and $\mathbb{T}a = \mathbb{T}b \neq 0$ we must have, by lemma 3.3.13, that $\mathcal{I}(a) = \mathcal{I}(b) = I_a$, so $a = a' R^{I_a}$ and $b = b' R^{I_a}$ for some $a', b'$ with $R(x) \nmid a'(x)$ and

$R(x) \nmid b'(x)$ and, again by lemma 3.3.13, $R(x)^{p^r-LI-I_a} | a'(x) - b'(x)$. Thus $b' = a' + \alpha$ where

$$\alpha \in \bigcup_{i=p^r-I-I_a}^{p^r-1} \mathcal{D}_R(p^r d - 1, i).$$

However if we are to avoid counting the same element more than once we need to ensure that $b'$ is such that deg $b(x) < p^r d - 1$ so deg $b'(x) < p^r d - 1 - dI_a$. Fixing $a'$, we can do this by restricting deg $\alpha(x)$ to be less than or equal to $p^r d - 1 - dI_a$ so

$$\alpha \in \bigcup_{i=p^r-I-I_a}^{p^r-1-I_a} \mathcal{D}_R((p^r - I_a)d - 1, i)$$

where the upper limit on $i$ is necessary as there cannot be elements $\alpha$ such that deg $\alpha(x)$ is $p^r d - I_a d - 1$ with $\alpha(x)$ divisible by $R(x)^{p^r-I_a}$ since the degree of that element is $p^r d - I_a d > p^r d - I_a d - 1$. Therefore, including $a$ itself, one finds that the number of predecessors of $\mathbb{T}a$ is

$$\left| \bigcup_{i=p^r-I-I_a}^{p^r-1-I_a} \mathcal{D}_R((p^r - I_a)d - 1, i) \right| + 1.$$

On employing a similar argument to that used in the proof of lemma 3.3.9 one finds that this number is

$$\sum_{i=p^r-I-I_a}^{p^r-1-I_a} \left( p^{(p^r-I_a-i)qd} - p^{(p^r-I_a-i-1)qd} \right) + 1 = p^{Iqd} - 1 + 1 = p^{Iqd}.$$

By the remarks following lemma 3.3.12 (equation 3.3.5 with $t = 1$) the number of non-zero predecessors of zero is $p^{Iqd} - 1$. ■

### 3.3.3 Dynamics in $\frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^r}\mathbb{F}_{p^q}[x]}$ when $U \neq 0$

We now consider the affine case $\mathbb{T}_U : \frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^r}\mathbb{F}_{p^q}[x]} \longrightarrow \frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^r}\mathbb{F}_{p^q}[x]}$, $a \mapsto \mathbb{T}a + U$. We know from corollary 2.3.3 that $\mathbb{T}_U$ can give qualitatively different dynamics from $\mathbb{T}$ for some input $U$ if and only if $\mathbb{T}$ has non-zero fixed points. When $\mathbb{T}_U$ has a fixed point we can apply results from chapter 2 to obtain the precise behaviour under $\mathbb{T}_U$ (as opposed to qualitative behaviour) if we know a fixed point of $\mathbb{T}_U$, thus we concentrate on the case

of qualitatively different behaviour from $\mathbb{T}$ in this section. Of course by theorem 2.2.1 we need only consider periodic behaviour. When $\mathbb{T}$ has non-zero fixed points $\mathbb{T}-1$ is nilpotent by lemma 3.3.4 and $L(\mathbb{T})=1$.

**Lemma 3.3.14** *If* $\mathbb{T} \in \frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^r}\mathbb{F}_{p^q}[x]}$ *has a non-zero fixed point then* $\mathbb{T}_U$ *has a fixed point if and only if* $U$ *is nilpotent and* $\mathcal{I}(\mathbb{T}-1) \leq \mathcal{I}(U)$. *If* $\mathbb{T}$ *has only the zero fixed point then, for each* $U \in \frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^r}\mathbb{F}_{p^q}[x]}$, $\mathbb{T}_U$ *has unique fixed point,* $-(\mathbb{T}-1)^{-1}U$. *If* $\mathbb{T}$ *is nilpotent then, for each* $U \in \frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^r}\mathbb{F}_{p^q}[x]}$, $\mathbb{T}_U$ *has the unique fixed point*

$$(\mathbb{T}^{T-1}+\ldots+\mathbb{T}+1)U,$$

*where* $T$ *is the maximum tree height occurring under* $\mathbb{T}$.

Proof:

If $\mathbb{T}$ has a non-zero fixed point then by Lemma 3.3.4 we have that $\mathbb{T}-1$ is nilpotent. Let $a$ be a fixed point of $\mathbb{T}_U$ then

$$\mathbb{T}a+U=a \;\Rightarrow\; U=-(\mathbb{T}-1)a$$

hence $U$ is nilpotent and clearly $\mathcal{I}(U) \geq \mathcal{I}(\mathbb{T}-1)$.

Conversely suppose $U$ is nilpotent and $\mathcal{I}(\mathbb{T}-1) \geq \mathcal{I}(U)$. Suppose $I_U = \mathcal{I}(U) = \mathcal{I}(\mathbb{T}-1)+J$, $J \in \mathbb{N}$. Then there are $\alpha(x), \beta(x) \in \mathbb{F}_{p^q}[x]$ such that

$$\begin{aligned} \mathbb{T}-1 &= \alpha(x)R(x)^{\mathcal{I}(\mathbb{T}-1)} + R(x)^{p^r}\mathbb{F}_{p^q}[x],\ R(x) \nmid \alpha(x) \\ -U &= \beta(x)R(x)^{I_U} + R(x)^{p^r}\mathbb{F}_{p^q}[x],\ R(x) \nmid \beta(x). \end{aligned}$$

As $R(x) \nmid \alpha(x)$, $\alpha^{-1}$ exists, so let $a = \alpha^{-1}\beta R^J$, then

$$(\mathbb{T}-1)a = \alpha R^{\mathcal{I}(\mathbb{T}-1)}\alpha^{-1}\beta R^J = \beta R^{I_U} = -U$$

so $a$ is a fixed point of $\mathbb{T}_U$. Now suppose that $\mathbb{T}$ is a unit but has only the zero fixed point, by lemma 3.3.4 this is equivalent to saying that $\mathbb{T}-1$ is a unit and thus $(\mathbb{T}-1)^{-1}$ exists, hence

$$\mathbb{T}a+U=a \;\Leftrightarrow\; (\mathbb{T}-1)a=-U \;\Leftrightarrow\; a=-(\mathbb{T}-1)^{-1}U.$$

When $\mathbb{T}$ is nilpotent with maximum tree height $T$ we have $\mathbb{T}^T a = 0$ for all $a \in \frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^r}\mathbb{F}_{p^q}[x]}$ so for any $U$ one has

$$\mathbb{T}_U((\mathbb{T}^{T-1}+\ldots+\mathbb{T}+1)U) = (\mathbb{T}^T+\ldots+\mathbb{T})U+U = (\mathbb{T}^{T-1}+\ldots+\mathbb{T}+1)U,$$

thus $(\mathbb{T}^{T-1}+\ldots+\mathbb{T}+1)U$ is a fixed point and is unique by corollary 2.3.3. ■

Note (the proof of) lemma 3.3.14 tells us how to construct fixed points for $\mathbb{T}_U$ when $\mathbb{T}$ and $\mathbb{T}_U$ are QDS. Summarising the rest of the content of lemma 3.3.14 we have that when $\mathbb{T}$ has a non-zero fixed point then all units and any nilpotent $U$ with $\mathcal{I}(U) < \mathcal{I}(\mathbb{T}-1)$ give $\Sigma(\mathbb{T}_U) \neq \Sigma(\mathbb{T})$. We shall need the following lemma.

**Lemma 3.3.15** *For any integer* $e > 0$

$$\mathbb{T}_U^{p^e}(0) = (\mathbb{T}-1)^{p^e-1}U$$

Proof:

In $\frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$ one has $\mathbb{T}_U^{p^e}(0) = (\mathbb{T}^{p^e-1}+\ldots+\mathbb{T}+1)U = \mathbb{T}_1^{p^e}(0)U$, in $\mathbb{F}_{pq}[x]$ one has

$$(\mathbb{T}(x)-1)^{p^e} = \mathbb{T}(x)^{p^e}-1 = (\mathbb{T}(x)-1)(\mathbb{T}(x)^{p^e-1}+\ldots+\mathbb{T}(x)+1).$$

Thus $(\mathbb{T}_1^{p^e}(0))(x) = \frac{(\mathbb{T}(x)-1)^{p^e}}{\mathbb{T}(x)-1} = (\mathbb{T}(x)-1)^{p^e-1}$, where $(\mathbb{T}_1^{p^e}(0))(x)$ is the canonical representative of $\mathbb{T}_1^{p^e}(0)$, and the result follows. ■

As in the $r = 0$ case our first task is to determine $(\phi_0)_U$.

**Lemma 3.3.16** *For any unit* $\mathbb{T}$ *and any* $U \in \frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$*:*

$$\begin{aligned}(\phi_0)_U &= (\phi_U)_0 \text{ if } \mathbb{T}_U^{(\phi_U)_0}(0) = 0,\\ (\phi_0)_U &= p(\phi_U)_0 \text{ if } \mathbb{T}_U^{(\phi_U)_0}(0) \neq 0.\end{aligned}$$

Proof:

If $\mathbb{T}_U^{(\phi_U)_0}(0) = 0$ then clearly $(\phi_0)_U|(\phi_U)_0$ but by remark 2.2.1 $(\phi_U)_0|(\phi_0)_U$ hence $(\phi_0)_U = (\phi_U)_0$.

Now suppose that $\mathbb{T}_U^{(\phi_U)_0}(0) = F$, a non-zero fixed point of $\mathbb{T}$ then, by lemma 2.1.13, $(\phi_0)_U|p(\phi_U)_0$ and by remark 2.2.1 $(\phi_U)_0|(\phi_0)_U$ hence, as $\mathbb{T}_U^{(\phi_U)_0}(0) \neq 0$, we must have $(\phi_0)_U = p(\phi_U)_0$ ■

We now consider unit $\mathbb{T}$ with non-zero fixed points and input $U$ a unit. to obtain the cycle set in this case we need the following lemma.

**Lemma 3.3.17** *Let* $\mathbb{T}$ *be a unit with a non-zero fixed point, let* $U$ *be a unit and* $\Pi(\mathbb{T}) = p^S$*. Then, with* $I = \mathcal{I}(\mathbb{T}-1)$, $(\phi_0)_U = \Pi(\mathbb{T})$ *if* $I(p^S-1) \geq p^r$ *and* $(\phi_0)_U = p\Pi(\mathbb{T})$ *if* $I(p^S-1) < p^r$.

Proof:

As $U$ is a unit $(\phi_U)_0 = p^S$. $\mathbb{T} - 1 = \alpha R^I$ where $R(x) \nmid \alpha(x)$. By lemma 3.3.15 one has $\mathbb{T}_U^{p^S}(0) = \alpha R^{I(p^S-1)}U$, which is zero if and only if $I(p^S - 1) \geq p^r$. Thus if $I(p^S - 1) \geq p^r$ then by lemma 3.3.16 $(\phi_0)_U = \Pi(\mathbb{T}) = p^S$ and if $I(p^S - 1) < p^r$ then by lemma 3.3.16 $(\phi_0)_U = p\Pi(\mathbb{T}) = p^{S+1}$. ■

We can now obtain the cycle set of $\mathbb{T}_U$ when $\mathbb{T}$ has non-zero fixed points and $U$ is a unit. When $\mathbb{T} = 1$ ($\Leftrightarrow$ $\mathcal{I}(\mathbb{T} - 1) = p^r$) all points are on cycles of length $p$ under $\mathbb{T}_U$ for any $U \neq 0$ by the same argument as used in lemma 3.2.3, (ii), thus we may exclude the case $\mathbb{T} = 1$ or equivalently $\mathcal{I}(\mathbb{T} - 1) = p^r$.

**Theorem 3.3.5** *When $\mathbb{T} \neq 1$ is a unit with non-zero fixed points and $\mathcal{I}(\mathbb{T} - 1) = I$ and $U$ is a unit then, where $\Pi(\mathbb{T}) = p^S$,*

$$\Sigma(\mathbb{T}_U) = \frac{p^{qdp^r}}{p^S}[p^S] \quad \textit{if} \quad I(p^S - 1) \geq p^r;$$

$$\Sigma(\mathbb{T}_U) = \frac{p^{qdp^r}}{p^{S+1}}[p^{S+1}] \quad \textit{if} \quad I(p^S - 1) < p^r.$$

Proof:

We prove this result by showing that for $\mathbb{T}$ a unit, $\mathbb{T} - 1$ nilpotent and $U$ a unit then $(\phi_a)_U = (\phi_0)_U$ for all $a \in \frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^r}\mathbb{F}_{p^q}[x]}$, the result then follows by lemma 3.3.17. For $\mathbb{T}$ with non-zero fixed points we have that, for any $a \in \frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^r}\mathbb{F}_{p^q}[x]}$, $(\phi_a)_0 = p^{e_a}$ where $S \geq e_a \geq 0$. Now, by lemma 2.3.6, $U \sim_1 U^*$ and as $\frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^r}\mathbb{F}_{p^q}[x]}$ is completely primary corollary 2.3.5 applies and $U^*$ is a unit with $(\phi_0)_{U^*}$ minimal but by lemma 3.3.17 we must have $(\phi_a)_0 | (\phi_0)_{U^*}$ for all $a \in \frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^r}\mathbb{F}_{p^q}[x]}$ and so by lemma 2.1.12, (i), $(\phi_a)_{U^*} | (\phi_0)_{U^*}$ for all $a \in \frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^r}\mathbb{F}_{p^q}[x]}$ and the result follows from the minimality of $(\phi_0)_{U^*}$. ■

We now consider nilpotent $U$ with $\mathcal{I}(U) < \mathcal{I}(\mathbb{T} - 1)$ so that $\Sigma(\mathbb{T}_U) \neq \Sigma(\mathbb{T})$. The remarks immediately preceding theorem 3.3.5 are valid in this case also, so we may exclude $\mathbb{T} = 1$ ($\mathcal{I}(\mathbb{T} - 1) = p^r$). The proof of the following lemma may be found in appendix B.

**Lemma 3.3.18** *Let $\mathbb{T}$ be a unit with $(\mathbb{T} - 1) \in \mathcal{D}_R(p^r d - 1, I)$, let $U \in \mathcal{D}_R(p^r d - 1, I_U)$ where $0 < I_U < I$ and $Ip^S = p^r + V$ then $(\phi_0)_U = p^S$ unless $(\phi_U)_0 = p^S$ and $I_U + V < I$ in which case $(\phi_0)_U = p^{S+1}$.* ■

**Theorem 3.3.6** *Let $\mathbb{T}$ be a unit with $(\mathbb{T}-1) \in \mathcal{D}_R(p^r d-1, I)$, let $U \in \mathcal{D}_R(p^r d-1, I_U)$ where $I_U < I$ and $Ip^S = p^r + k$ then*

(i) *If $(\phi_U)_0 = p^{S-1}$ or $(\phi_U)_0 = p^S$ and $I_U + k \geq I$ then*

$$\Sigma(\mathbb{T}_U) = p^{qp^r d-S}[p^S];$$

(ii) *If $(\phi_U)_0 = p^S$ and $I_U + k < I$ then*

$$\Sigma(\mathbb{T}_U) = p^{qp^r d-S-1}[p^{S+1}].$$

Proof:

In either case it suffices, by lemma 3.3.18, to show that, for all $a \in \frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$, $(\phi_a)_U = (\phi_0)_U$. Examining the proof of lemma 2.3.6 we see that in the present case $U \sim_1 U^*$ where $U^*$ is nilpotent with $I_{U^*} < I$ and $(\phi_0)_{U^*}$ the minimal orbit length under $\mathbb{T}_{U^*}$. By lemma 3.3.18 $(\phi_a)_0 | (\phi_0)_{U^*}$ hence by lemma 2.1.12, (i), $(\phi_a)_{U^*} | (\phi_0)_{U^*}$ for all $a \in \frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$ and hence $(\phi_a)_0 = (\phi_0)_{U^*}$ for all $a \in \frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]}$ by the minimality of $(\phi_0)_{U^*}$ and hence, as $\mathbb{T}_U$ and $\mathbb{T}_{U^*}$ are QDS, $(\phi_0)_U = (\phi_0)_{U^*}$ and the result follows. ■

In applying theorem 3.3.5 one needs to know when $I(p^S - 1) < p^r$, also, bearing lemma 3.3.10 in mind, it is instructive to see, if $I(p^S - 1) < p^r$ for some $r$ does this persist as $r$ is increased. These questions are answered in the following lemma, its proof can be found in appendix B, section B.2.

**Lemma 3.3.19** *For $\mathbb{T}$ a unit with $(\mathbb{T}-1) \in \mathcal{D}_R(p^r d-1, I)$, $r > 0$ and $I = p^n + J$. $n < r$ and $0 \leq J < p^n(p-1)$ then $I(p^S - 1) < p^r$ if $J = 0$ or if $n = r - n$ and $J = 1$ or if $n > r - n$ and $J < \left\lceil \frac{p^n}{p^{r-n}-1} \right\rceil$. Further for all $v \in \mathbb{N}$ let $\mathbb{T}_v \in \frac{\mathbb{F}_{pq}[x]}{R(x)^{p^{r+v}}\mathbb{F}_{pq}[x]}$ with $\pi_{r+v}(\mathbb{T}_v) = \mathbb{T}$, then $I(p^{S_{\mathbb{T}_V}} - 1) < p^{r+v}$ for all $v \in \mathbb{N}$ if and only if $J = 0$.* ■

Note that if $\mathbb{T}$ is such that $I(p^S - 1) \geq p^r$ and with $\mathbb{T}_v$, $v \in \mathbb{N}$ as described in the lemma, then $I(p^{S+v} - 1) \geq p^{r+v}$ for all $v \in \mathbb{N}$ for suppose that $I(p^S - 1) = p^r + k$ so $Ip^S = p^r + k + I$, then

$$I(p^{S+v} - 1) = I(p^S - 1) + Ip^S(p^v - 1) = p^{r+v} + kp^v + Ip^v - I \geq p^{r+v}$$

for any $v \in \mathbb{N}$.

In a similar vein to lemma 3.3.19 we have the following result, whose proof can also be found in appendix B.

**Lemma 3.3.20** *Let* $\mathbb{T} \in \frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^r}\mathbb{F}_{p^q}[x]}$, *a unit, with* $\mathbb{T}-1 \in \mathcal{D}_R(p^r d-1, I)$ *and let* $U \in \mathcal{D}_R(p^r d-1, I_U)$ *where* $0 < I_U < I < p^r$ *and suppose that under* $\mathbb{T}$ *one has* $(\phi_U)_0 = p^{S-1}$. *Let* $\{\mathbb{T}_v\}_{v\in\mathbb{N}}$ *be such that* $\mathbb{T}_v \in \frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^{r+v}}\mathbb{F}_{p^q}[x]}$ *with* $\pi_{r+v}(\mathbb{T}_v) = \mathbb{T}$, *then there is some* $v^* \in \mathbb{N}$ *such that if* $W \in \mathcal{D}_R(p^{r+v}d-1, I_U)$ *where* $v \geq v^*$ *then under* $\mathbb{T}_v$, $v \geq v^*$, $(\phi_W)_0 = p^{S+v}$. ■

Recall in theorem 3.3.6, (i), that if $(\phi_U)_0 = p^{S-1}$ or $(\phi_U)_0 = p^S$ and $I_U + k \geq I$ then $\Sigma(\mathbb{T}_U) = p^{p^r qd-S}[p^S]$, lemma 3.3.20 tells us that the first case ($(\phi_U)_0 = p^{S-1}$) cannot persist as $r$ is increased in the way described in the lemma. Finally we have

**Lemma 3.3.21** *Let* $\mathbb{T} \in \frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^r}\mathbb{F}_{p^q}[x]}$, *a unit, with* $\mathbb{T}-1 \in \mathcal{D}_R(p^r d-1, I)$ *and let* $\{\mathbb{T}_v\}_{v\in\mathbb{N}}$ *be such that* $\mathbb{T}_v \in \frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^{r+v}}\mathbb{F}_{p^q}[x]}$ *with* $\pi_{r+v}(\mathbb{T}_v) = \mathbb{T}$ *for all* $v \in \mathbb{N}$. *Then there is some* $v^* \in \mathbb{N}$ *such that if* $Ip^S = p^r + k$ *and* $k > 0$ *then for all integers* $v \geq v^*$ *one has* $I_U + k \geq I$ *for* $0 < I_U < I$.

Proof:

We have that $Ip^S = p^r + k$ if and only if $(p^n + J)p^{r-n} = p^r + k$ where $p^n \leq I < p^{n+1}$, $n < r$ and $0 \leq J \leq p^{n+1} - p^n$. Hence $k = Jp^{r-n}$ so if $J \neq 0$ then $k \neq 0$ and $k$ increases with $r$ if $I$ remains fixed, hence there will be some $v^* \in \mathbb{N}$ such that $k = Jp^{r+v^*-n} \geq I$ and hence for all integers $v \geq v^*$ one has $I_U + k \geq I$ for any $I_U \in \mathbb{N}$. ■

Under the conditions of lemma 3.3.21 we have $k = 0$ if and only if $J = 0$ so when $I$ is a power of $p$ ($< p^r$) we have that if $I_U < I$ then for all $v \in \mathbb{N}$

$$\Sigma((\mathbb{T}_v)_U) = p^{p^{r+v}qd-S-v-1}[p^{S+v+1}],$$

and the lemma tells us that $J = 0$ is the only case in which the above is true for all $v \in \mathbb{N}$. Summarising we have that if $\mathbb{T} \in \frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^r}\mathbb{F}_{p^q}[x]}$, a unit, with $\mathbb{T}-1 \in \mathcal{D}_R(p^r d-1, I)$ and $\{\mathbb{T}_v\}_{v\in\mathbb{N}}$ is such that $\mathbb{T}_v \in \frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^{r+v}}\mathbb{F}_{p^q}[x]}$ with $\pi_{r+v}(\mathbb{T}_v) = \mathbb{T}$ for all $v \in \mathbb{N}$ and any $U \in \mathcal{D}_R(p^{r+v}d-1, I_U)$, $0 < I_U < I$ and $(\phi_U)_0 = p^{S+v}$ one has

$$\Sigma((\mathbb{T}_v)_U) = p^{p^{r+v}qd-S-v-1}[p^{S+v+1}],$$

for all $v \in \mathbb{N}$ if and only if $I = p^n$, $n < r$.

# Chapter 4

# Additive cellular automata over finite fields II

In this chapter we describe the behaviour of systems of the form (1.5.20) completely when $R$ is a finite field $\mathbb{F}_{p^q}$ and hence of linear cellular automata with state alphabet a finite field and periodic boundary conditions, both with and without time independent inputs, using the results of chapter 3. We highlight the relationship between behaviour on $np^r$ cells and on $np^{r+j}$ cells where $n$ is coprime to $p$, $r \in \mathbb{N}$ and $j \in \mathbb{N} \setminus \{0\}$. In section 4.1 we briefly discuss the relationship between behaviour on $nm$ cells and on $n$ (or $m$) cells.

In section 4.2 we concentrate on $np^r$ cells, $n$ coprime to $p$ and $r \in \mathbb{N}$ and begin by describing the relationships between the behaviour for different values of $r$, to do so we introduce the idea of $(x^n - 1)$-sets and associated $R_i(x)$-sets where $x^n - 1 = \prod_{i=1}^{m} R_i(x)$. These sets and their properties facilitate the application of lemma 3.3.11 and we show that the representatives of a given linear cellular automata on $np^r$ cells, $r \in \mathbb{N}$, form an $(x^n - 1)$ set for each integer $n > 0$ coprime to $p$. We show that a linear cellular automata over $\mathbb{F}_{p^q}$ is reversible on $np^r$ cells if and only if it is reversible on $n$ cells. A simple formula for the number of fixed points of a linear cellular automata on $np^r$ cells is found and we show (in corollary 4.2.2) that for each positive integer coprime to $p$ there is an integer $J > 0$ such that for every $r > J$ the cellular automata has the same number of fixed points on $np^r$ cells as on $np^J$ cells and also that if a linear cellular automata has no non-zero fixed points on $n$ cells then it has no non-zero fixed points on $np^r$ cells for any $r \in \mathbb{N}$.

In lemma 4.2.8 we describe the invariant set under a linear cellular automata and give formulas for the maximal cycle length and the orbit length of any configuration under the cellular automata. In corollary 4.2.4 we show that for each positive integer $n$ coprime to $p$ there is an integer $J > 0$ such that for all $r \in \mathbb{N}$ the maximal cycle length on $np^{r+J}$ cells is $p^r$ times the maximal cycle length on $np^J$ cells. We also show that the fraction of configurations on cycles that are on cycles of maximal length on $np^r$ cells approaches 1 as $r$ increases. Efficient computation of the cycle set of a linear cellular automata over $\mathbb{F}_{p^q}$ is discussed.

In section 4.2.2 we discuss transient behaviour when the cellular automata is irreversible, by the results of chapter 2 it is sufficient to do this for the zero input case. The transient behaviour is completely described, in particular we show that the maximum possible number of time steps for a configuration to evolve to a cycle under any linear cellular automata rule over $\mathbb{F}_{p^q}$ on $np^r$ cells is $p^r$, giving conditions for this maximum transience time to be realised and we show that for each positive integer $n$ coprime to

$p$ there is an integer $J > 0$ such that the in-degree of any vertex in the state transition graph of the cellular automata on $np^{r+J}$ cells is fixed and equal to the in-degree of any vertex in the state transition graph of the cellular automata on $np^J$ cells.

In section 4.3 we consider periodic behaviour in the presence of non-zero inputs. We are able to count the number of inputs such that the system with inputs gives qualitatively similar behaviour to that without inputs in the sense described in chapter 2, section 2.3. We find a necessary and sufficient condition for the system with a particular input to have fixed points. In theorem 4.3.1 we show that on $np^r$ cells a given linear cellular automata rule with inputs has at most $r + 2$ qualitatively distinct behaviours (*i.e.* distinct cycle sets) and show that the condition of theorem 2.3.3 is satisfied so that a necessary and sufficient condition for inputs $U$ and $V$ to give qualitatively similar behaviour is that the minimum orbit length occurring for the system with input $U$ be equal to that occurring for the system with input $V$. A formula for the minimal orbit length is given. In theorem 4.3.2 we show that additive cellular automata over finite fields, with time independent inputs, cannot generate cycles of lengths $p^{qN} - 1$ or $p^{qN}$ on $N$ cells, $N > 1$.

In section 4.4 we introduce a notion of qualitative dynamical similarity for different cellular automata rules on $N$ cells. In theorems 4.4.2 and 4.4.3 we give some circumstances where this can occur and be extended from $np^r$ cells to $np^{r+s}$ cells for all $s \in \mathbb{N}$. The general question of exactly which linear rules give qualitatively similar behaviour on a given number of cells is discussed and we indicate how this problem is related to the problem of factorisation in the ring of cycle sets $C(\mathbb{Z})$ introduced in chapter 1.

Finally in section 4.5 we rewrite the direct product decomposition of $\frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]}$ in terms of idempotent elements in preparation for chapter 5, and show how the idempotents for the $np^r$ cell case may be calculated from those for the $n$ cell case.

## 4.1 The relationship between $\frac{\mathbb{F}_{pq}[x]}{(x^{nm}-1)\mathbb{F}_{pq}[x]}$ and $\frac{\mathbb{F}_{pq}[x]}{(x^{n}-1)\mathbb{F}_{pq}[x]}$

In section 4.2 we describe the relations between $\frac{\mathbb{F}_{pq}[x]}{(x^{n}-1)\mathbb{F}_{pq}[x]}$ and $\frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]}$ in detail.

In this section we briefly discuss the general case of composite $N$. Suppose that $N = nm$, then there is a ring epimorphism

$$\rho_n : \frac{\mathbb{F}_{pq}[x]}{(x^N - 1)\mathbb{F}_{pq}[x]} \longrightarrow \frac{\mathbb{F}_{pq}[x]}{(x^n - 1)\mathbb{F}_{pq}[x]}$$

$$a(x) + (x^N - 1)\mathbb{F}_{p^q}[x] \quad \mapsto \quad a(x) + (x^n - 1)\mathbb{F}_{p^q}[x],$$

this follows from the factor theorem as, by corollary A.2.1, $x^n - 1 | x^{nm} - 1$ and hence $(x^N - 1)\mathbb{F}_{p^q}[x] \subseteq (x^n - 1)\mathbb{F}_{p^q}[x]$. Let $f$ be the local rule of an additive cellular automata, given by (1.5.1), we recall from definition 1.5.1 that the representative of the global rule on $N$ cells is

$$\begin{aligned} \mathbb{T}_N &= \mathbb{T}_N(x) + (x^N - 1)\mathbb{F}_{p^q}[x] \\ &= \sum_{j=0}^{l} \alpha_{-j} x^j + \sum_{j=1}^{l} \alpha_j x^{N-j} + (x^N - 1)\mathbb{F}_{p^q}[x]. \end{aligned}$$

Strictly speaking, if $l > N$, as we noted in chapter 1 after definition 1.5.1, $\sum_{j=1}^{l} \alpha_j x^{N-j}$ may not be a polynomial, however, recalling the isomorphism

$$\frac{\mathbb{F}_{p^q}[x, x^{-1}]}{(x^N - 1)\mathbb{F}_{p^q}[x, x^{-1}]} \cong \frac{\mathbb{F}_{p^q}[x]}{(x^N - 1)\mathbb{F}_{p^q}[x]}$$

described in lemma A.2.4, as long as $\sum_{j=1}^{l} \alpha_j x^{N-j}$ appears in expressions of the form $a(x) + \sum_{j=1}^{l} \alpha_j x^{N-j} + (x^N - 1)\mathbb{F}_{p^q}[x]$ we shall sometimes abuse notation and write $\sum_{j=1}^{l} \alpha_j x^{N-j}$ as $A_N(x)$. Of course if $N \geq l$ then $A_N(x)$ is a polynomial.

**Lemma 4.1.1** *Let $f : a_i \mapsto \sum_{j=-l}^{l} \alpha_j a_{i+j}$ be the local rule of an additive cellular automata. Let $\mathbb{T}_{nm}$ be the representative of $f$ on $N = nm$ cells. Let $\mathbb{T}_n$ be the representative of $f$ on $n$ cells, then*

$$\mathbb{T}_n = \rho_n(\mathbb{T}_{nm}).$$

Proof:

Using definition 1.5.1 we have

$$\begin{aligned} \mathbb{T}_{nm} &= \sum_{j=0}^{l} \alpha_{-j} x^j + \sum_{j=1}^{l} \alpha_j x^{nm-j} + (x^{nm} - 1)\mathbb{F}_{p^q}[x] \\ \mathbb{T}_n &= \sum_{j=0}^{l} \alpha_{-j} x^j + \sum_{j=1}^{l} \alpha_j x^{n-j} + (x^n - 1)\mathbb{F}_{p^q}[x]. \end{aligned}$$

Now

$$\mathbb{T}_{nm} = \sum_{j=0}^{l} \alpha_{-j} x^j + x^{n(m-1)} \sum_{j=1}^{l} \alpha_j x^{n-j} + (x^{nm} - 1)\mathbb{F}_{p^q}[x]$$

$$= \sum_{j=0}^{l} \alpha_{-j} x^j + A_n(x) - A_n(x) + x^{n(m-1)} \sum_{j=1}^{l} \alpha_j x^{n-j} + (x^{nm} - 1)\mathbb{F}_{p^q}[x]$$

$$= \sum_{j=0}^{l} \alpha_{-j} x^j + A_n(x) + (x^{n(m-1)} - 1)A_n(x) + (x^{nm} - 1)\mathbb{F}_{p^q}[x],$$

and, by corollary A.2.1, $x^n - 1 | x^{n(m-1)} - 1$ hence

$$\begin{aligned} \rho_n(\mathbb{T}_{nm}) &= \sum_{j=0}^{l} \alpha_{-j} x^j + A_n(x) + (x^n - 1)\mathbb{F}_{p^q}[x] \\ &= \mathbb{T}_n. \quad \blacksquare \end{aligned}$$

If $N$ is coprime to $p$ then $x^N - 1$ is separable and if $n$ is any positive divisor of $N$ one has an isomorphism $\Theta_n$

$$\frac{\mathbb{F}_{p^q}[x]}{(x^N - 1)\mathbb{F}_{p^q}[x]} \cong \frac{\mathbb{F}_{p^q}[x]}{(x^n - 1)\mathbb{F}_{p^q}[x]} \times \frac{\mathbb{F}_{p^q}[x]}{g_n(x)\mathbb{F}_{p^q}[x]}$$

where $g_n(x) = \frac{x^N - 1}{x^n - 1}$ and

$$\begin{aligned} \Theta_n : a(x) + (x^N - 1)\mathbb{F}_{p^q}[x] &\mapsto (a(x) + (x^n - 1)\mathbb{F}_{p^q}[x], a(x) + g_n(x)\mathbb{F}_{p^q}[x]) \\ &= (\rho_n(a), a(x) + g_n(x)\mathbb{F}_{p^q}[x]). \end{aligned}$$

**Lemma 4.1.2** *Let $f : a_i \mapsto \sum_{i=-l}^{l} \alpha_l a_{i+l}$ be the local rule of an additive cellular automata, let $\mathbb{T}_N$ be the representative of $f$ on $N$ cells and let $\mathbb{T}_n$ be the representative of $f$ on $n$ cells, where $n|N$, then the image of $\mathbb{T}_N$ in $\frac{\mathbb{F}_{p^q}[x]}{(x^n-1)\mathbb{F}_{p^q}[x]}$ under $\Theta_n$ is $\mathbb{T}_n$.*

Proof:

Follows immediately from the definition of $\Theta_n$ and lemma 4.1.1. $\blacksquare$

Thus if we have already computed $\Sigma(\mathbb{T}_n)$ whilst considering $f$ on $n$ cells then when considering $f$ on $N$ cells we need merely compute $\Sigma(\mathbb{T}_{g_n})$ where $\mathbb{T}_{g_n}$ is the image of $\mathbb{T}_N$ under $\Theta_n$ in $\frac{\mathbb{F}_{p^q}[x]}{g_n(x)\mathbb{F}_{p^q}[x]}$ and then

$$\Sigma(\mathbb{T}_N) = \Sigma(\mathbb{T}_n)\Sigma(\mathbb{T}_{g_n}).$$

Note that there will be an element $\mathbb{T}'_N$ in $\frac{\mathbb{F}_{p^q}[x]}{(x^N-1)\mathbb{F}_{p^q}[x]}$ such that $\Theta_n(\mathbb{T}'_N) = (\mathbb{T}_n, 0)$ so any additive cellular automata represented by $\mathbb{T}'_N$ on $N$ cells emulates the behaviour of

$f$ on $n$ cells, i.e. $\Sigma(\mathbb{T}'_N) = \Sigma(\mathbb{T}_n)$. Further, let $g_n(x) = \prod_{i=1}^{s} g_{n,i}(x)$ where each $g_{n,i}(x)$ is irreducible, then any $\mathbb{T}'$ such that $\Theta_n(\mathbb{T}') = (\mathbb{T}_n, \overline{\mathbb{T}'})$ where $\overline{\mathbb{T}'} \bmod g_{n,i}(x) \in \{0,1\}$, not all zero, then with

$$I = \{i : 1 \leq i \leq s, \overline{\mathbb{T}'} \bmod g_{n,i}(x) = 1\}$$

one has

$$\Sigma(\mathbb{T}') = p^{q \sum_{j \in I} deg\, g_{n,j}(x)} \Sigma(\mathbb{T}_n).$$

Also there is an ideal $\mathfrak{A} \lhd \frac{\mathbb{F}_{pq}[x]}{(x^N-1)\mathbb{F}_{pq}[x]}$ consisting of those elements $a$ such that $\Theta_n(a) = (\rho_n(a), 0)$ and any $\mathbb{T} \in \frac{\mathbb{F}_{pq}[x]}{(x^N-1)\mathbb{F}_{pq}[x]}$ acts like $\rho_n(\mathbb{T})$ on $\mathfrak{A}$.

## 4.2 Dynamics in $\frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]}$ when $U = 0$

Throughout this section $n$ is a positive integer with $\gcd(p, n) = 1$. From theorem 3.1.1 one has that, for all $r \in \mathbb{N}$,

$$\frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]} \cong \prod_{i=1}^{m} \frac{\mathbb{F}_{pq}[x]}{R_i(x)^{p^r}\mathbb{F}_{pq}[x]}$$

where the $R_i(x)$ are distinct irreducible polynomials in $\mathbb{F}_{pq}[x]$ with $x^n - 1 = \prod_{i=1}^{m} R_i(x)$. The degree of $R_i(x)$ is $d_i$ and

$$\frac{\mathbb{F}_{pq}[x]}{R_i(x)\mathbb{F}_{pq}[x]} \cong \mathbb{F}_{p^{qd_i}}.$$

We apply results from chapter 3 to produce results for $\frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]}$.

Let $M = \{1, \ldots, m\}$, let $a \in \frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]}$, we shall write $\{a_i\}_{i \in M}$ for the image of $a$ in $\prod_{i=1}^{m} \frac{\mathbb{F}_{pq}[x]}{R_i(x)^{p^r}\mathbb{F}_{pq}[x]}$. We shall denote the units in $\prod_{i=1}^{m} \frac{\mathbb{F}_{pq}[x]}{R_i(x)^{p^r}\mathbb{F}_{pq}[x]}$ by $U_{pq}(np^r)$ and the zero divisors by $ZD_{pq}(np^r)$.

We shall frequently identify across the isomorphism

$$\frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]} \cong \prod_{i=1}^{m} \frac{\mathbb{F}_{pq}[x]}{R_i(x)^{p^r}\mathbb{F}_{pq}[x]}$$

throughout the rest of this chapter and thus will use $\frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]}$ and $\prod_{i=1}^{m} \frac{\mathbb{F}_{pq}[x]}{R_i(x)^{p^r}\mathbb{F}_{pq}[x]}$ interchangeably. We shall sometimes change the ordering of the $m$ rings $\frac{\mathbb{F}_{pq}[x]}{R_i(x)^{p^r}\mathbb{F}_{pq}[x]}$, $1 \leq i \leq m$, in the direct product and write subsets of $\frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]}$ as Cartesian products of subsets of the rings $\frac{\mathbb{F}_{pq}[x]}{R_i(x)^{p^r}\mathbb{F}_{pq}[x]}$, $1 \leq i \leq m$, in the new ordering, this reordering should be born in mind if one wants to actually construct elements of these sets.

One of our goals is to establish relationships between additive cellular automata behaviour on $np^i$ cells and $np^{i+j}$ cells for $i \geq 0$, $j > 0$, to this end we must accept an increase in the complexity of our notation.

Recall the ring epimorphisms

$$\pi_{r,r-j} : \frac{\mathbb{F}_{pq}[x]}{R(x)^{p^r}\mathbb{F}_{pq}[x]} \longrightarrow \frac{\mathbb{F}_{pq}[x]}{R(x)^{p^{r-j}}\mathbb{F}_{pq}[x]}, \quad 0 < j \leq r,$$

introduced in chapter 3. We shall denote the epimorphisms of this type between the $i-th$ factor of $\frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]}$ and the $i-th$ factor of $\frac{\mathbb{F}_{pq}[x]}{(x^{np^{r-j}}-1)\mathbb{F}_{pq}[x]}$ by $\pi^i_{r,r-j}$. Also recall the ring epimorphisms $\theta_i : \frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]} \longrightarrow \frac{\mathbb{F}_{pq}[x]}{R_i(x)^{p^r}\mathbb{F}_{pq}[x]}$, we now denote these maps by $\theta^i_r$. We introduce a ring epimorphism $\Gamma_{r,r-j}$ defined in the usual way via the factor theorem:

$$\begin{aligned} \Gamma_{r,r-j} : \frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]} &\longrightarrow \frac{\mathbb{F}_{pq}[x]}{(x^{np^{r-j}}-1)\mathbb{F}_{pq}[x]}, \quad 0 < j \leq r. \\ a(x) + (x^{np^r}-1)\mathbb{F}_{pq}[x] &\mapsto a(x) + (x^{np^{r-j}}-1)\mathbb{F}_{pq}[x]. \end{aligned}$$

We note that

$$\Gamma_{r-j,r-j-k} \circ \Gamma_{r,r-j} = \Gamma_{r,r-j-k}, \quad 0 < j \leq r, 0 < k \leq r-j.$$

We also note that, by reference to section 4.1, $\Gamma_{r,r-j} = \rho_{np^r-j}$. The situation is summed up in the following lemma, whose proof is a tedious but straight forward verification.

**Lemma 4.2.1** *Figure 4.1 commutes.* ■

We shall frequently be interested in sets $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$ with $\mathbb{T}_r \in \frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}}$ and $\Gamma_{r+1,r}(\mathbb{T}_{r+1}) = \mathbb{T}_r$ for all $r \in \mathbb{N}$. We make the following definition:

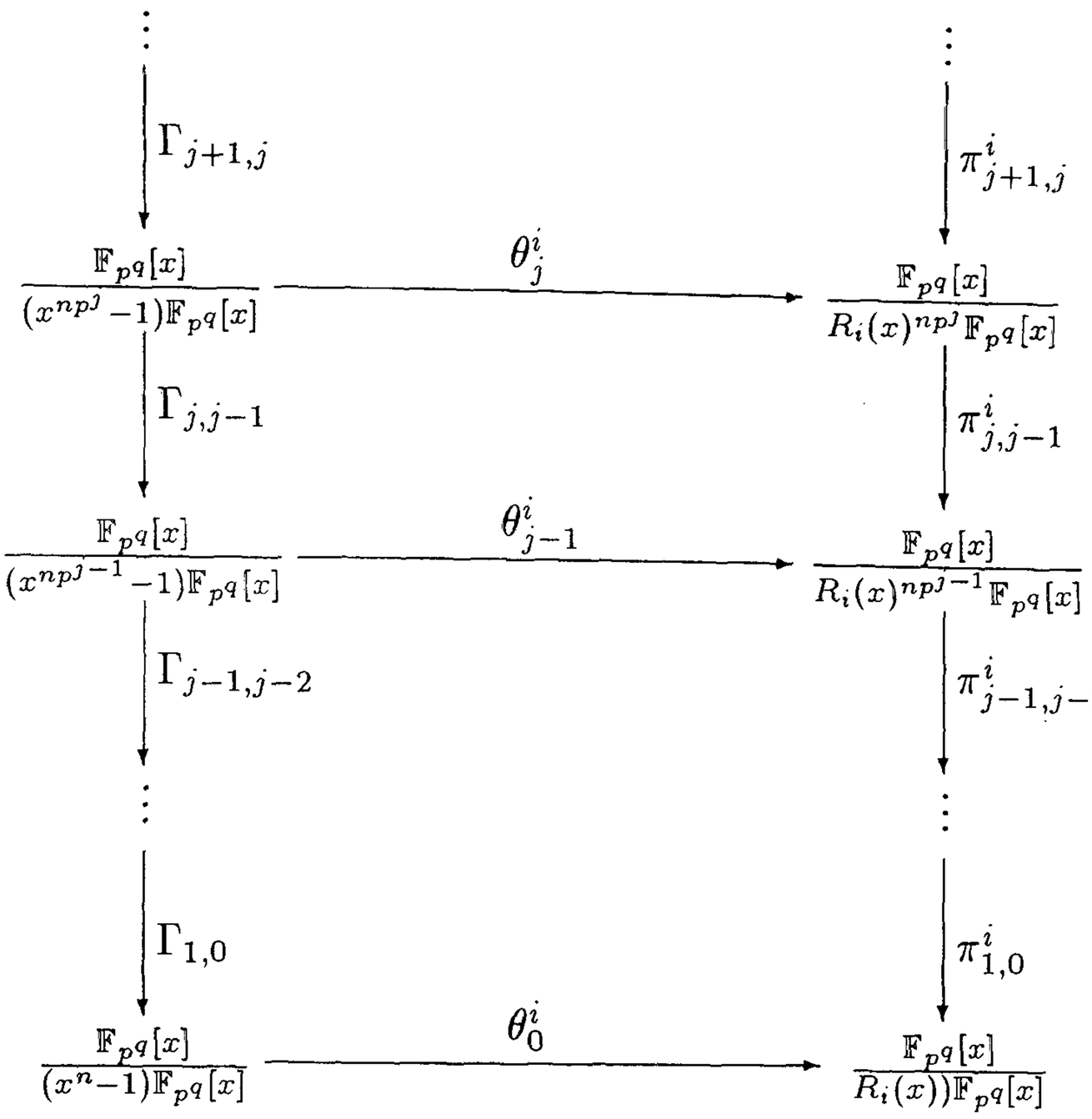


Figure 4.1: The homomorphisms $\Gamma_{j+1,j}, \theta^i_j, \pi^i_{j+1}$ *etc*, are all surjective and the diagram commutes.

**Definition 4.2.1** *A $g(x)$-set is a set $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$ such that $\mathbb{T}_r \in \frac{\mathbb{F}_{pq}[x]}{g(x)^{p^r}\mathbb{F}_{pq}}$ for all $r \in \mathbb{N}$ and $\gamma_{r+1,r}(\mathbb{T}_{r+1}) = \mathbb{T}_r$ where $\gamma_{r+1,r} : \frac{\mathbb{F}_{pq}[x]}{g(x)^{p^{r+1}}\mathbb{F}_{pq}} \longrightarrow \frac{\mathbb{F}_{pq}[x]}{g(x)^{p^r}\mathbb{F}_{pq}}$ is the canonical ring epimorphism defined via the factor theorem, for all $r \in \mathbb{N}$.*

If $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$ is a $g(x)$-set such that $\mathbb{T}_r = 0$ for all $r \in \mathbb{N}$ then we shall call $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$ the trivial $g(x)$-set. Given an $(x^n-1)$-set $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$ then for each of the irreducible factors $R_j(x)$ of $x^n-1$, $1 \leq j \leq m$, the set

$$\{\mathbb{T}_{r,j}\}_{r\in\mathbb{N}} = \{\theta^j_r(\mathbb{T}_r)\}_{r\in\mathbb{N}}$$

is an $R_j(x)$-set (this follows from the commutativity of figure 4.1). If $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$ is a $g(x)$ set it follows that so is $\{\mathbb{T}^l_r + \alpha\}_{r\in\mathbb{N}}$ for all $l \geq 1$ and any $\alpha \in \mathbb{F}_{p^q}$. Note that definition 4.2.1 was made with the exploitation of lemma 3.3.11 in mind. We show that the representatives of a given additive cellular automata on $np^r$ cells for all $r \in \mathbb{N}$ form an $(x^n-1)$-set.

**Lemma 4.2.2** *Let $f : a_i \mapsto \sum_{s=-l}^{l} \alpha_s a_{i+s}$ be the local rule of an additive cellular automata, let $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$ be the set where $\mathbb{T}_r$ is the representative of $f$ on $np^r$ cells, then $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$ is a $(x^n-1)$-set.*

Proof:

For all $r \in \mathbb{N} \setminus \{0\}$ this follows from lemma 4.1.1 as clearly $\Gamma_{r,r-1} = \rho_{np^{r-1}}$. ■

**Definition 4.2.2** *Let $f$ be the local rule of an additive cellular automata, let $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$ be the $(x^n-1)$-set of representatives of $f$ on $np^r$ cells, $r\in \mathbb{N}$. We call this $(x^n-1)$-set the $(x^n-1)$-set of $f$, and call the associated $R_j(x)$-sets $\{\mathbb{T}_{r,j}\}_{r\in\mathbb{N}}$ the $R_j(x)$-sets of $f$.*

Recall definition 3.3.1, we restate that definition here in notation compatible with that used in this chapter.

**Definition 4.2.3** *For any $r \in \mathbb{N}$ and each $i \in M$, let $\mathcal{I}_i : \frac{\mathbb{F}_{pq}[x]}{R_i(x)^{p^r}\mathbb{F}_{pq}[x]} \longrightarrow \{0,1,\ldots,p^r\}$ be the map given by*

$$\begin{aligned} a &\mapsto j \text{ if } R_i(x)^j | a(x) \text{ but } R_i(x)^{j+1} \nmid a(x),\ a \neq 0, \\ 0 &\mapsto p^r. \end{aligned}$$

Recall also the integer $S = S(\mathbb{T})$ defined in theorem 3.3.1 and $L = L(\mathbb{T})$, the minimal orbit length under $\mathbb{T}$. In the present context, for given $\mathbb{T} \in \frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}}$, the values of $S$ and $L$ in the $i-th$ factor ring will be denoted by $S(\mathbb{T}_i)$ and $L(\mathbb{T}_i)$ respectively, or just $S_i$ and $L_i$. We recall that $L(\mathbb{T}_i) = O(\pi^i_{r,o}(\mathbb{T}_i))$ and that, by lemma 3.3.11, for an $(x^n-1)$-set $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$, $L(\mathbb{T}_{r+1,j}) = L(\mathbb{T}_{r,j}) = L_j$ for all $r \in \mathbb{N}$ and $j \in M$.

**Definition 4.2.4** *For any $\mathbb{T} \in \frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]}$, with $\mathbb{T}_j = \theta^j_r(\mathbb{T})$,*

$$\begin{aligned} M^r_0(\mathbb{T}) &= \{j \in M : \mathbb{T}_j \text{ is nilpotent}\} \\ M^r_1(\mathbb{T}) &= \{j \in M \setminus M^r_0(\mathbb{T}) : \mathbb{T}_j - 1 \text{ is nilpotent}\} = \{j \in M \setminus M^r_0(\mathbb{T}) : L(\mathbb{T}_j) = 1\}. \end{aligned}$$

**Lemma 4.2.3** *For any $(x^n-1)$-set $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$ one has*

$$\begin{aligned} M^r_0(\mathbb{T}_r) &= M^0_0(\mathbb{T}_0) \text{ and} \\ M^r_1(\mathbb{T}_r) &= M^0_1(\mathbb{T}_0). \end{aligned}$$

*for all $r \in \mathbb{N}$.*

Proof:

For any $(x^n-1)$-set $\{\mathbb{T}_r\}_{r\in\mathbf{N}}$ one has the associated $R_j(x)$-sets $\{\mathbb{T}_{r,j}\}_{i\in\mathbf{N}}$, $1 \leq j \leq m$. From lemma 3.3.11 we have, where we denote Ker $\pi^j_{r,0}$ by $Nil_{p^q}(R_j, r)$,

$$\mathbb{T}_{r+s,j} \in U_{p^q}(R_j, r+s) \quad \Leftrightarrow \quad \mathbb{T}_{r,j} \in U_{p^q}(R_j, r) \text{ for all } r, s \in \mathbf{N}$$

$$\mathbb{T}_{r+s,j} \in Nil_{p^q}(R_j, r+s) \quad \Leftrightarrow \quad \mathbb{T}_{r,j} \in Nil_{p^q}(R_j, r) \text{ for all } r, s \in \mathbf{N}$$

and $L_j = L(\mathbb{T}_{r+s,j}) = L(\mathbb{T}_{r,j})$ for all $r, s \in \mathbf{N}$ if $\mathbb{T}_{r,j}$ is a unit. It follows that $M_0^r(\mathbb{T}_r) = M_0^0(\mathbb{T}_0)$ for all $r \in \mathbf{N}$. Now, $\{\mathbb{T}_{r,j}^{L_j} - 1\}_{r\in\mathbf{N}}$ is a $R_j(x)$-set and by the above comments $\mathbb{T}_{r,j} - 1$ is nilpotent if and only if $\mathbb{T}_{0,j} - 1$ is nilpotent (in fact zero). ■

Thus for a $(x^n - 1)$-set $\{\mathbb{T}_r\}_{r\in\mathbf{N}}$ we define $M_1(\mathbb{T}) = M_1^0(\mathbb{T}_0)$ and $M_0(\mathbb{T}) = M_0^0(\mathbb{T}_0)$. Clearly, for any $r \in \mathbf{N}$, $\mathbb{T}_r$ is a unit if and only if $M_0(\mathbb{T}) = \emptyset$.

**Corollary 4.2.1** *Let $f$ be the local rule of an additive cellular automata, let $\{\mathbb{T}_r\}_{r\in\mathbf{N}}$ be the $(x^n - 1)$-set of $f$. Then $f$ is reversible on $np^r$ cells if and only if $f$ is reversible on $n$ cells and $f$ is nilpotent on $np^r$ cells if and only if $f$ is the zero rule on $n$ cells.*

Proof:

This is immediate from lemma 4.2.3. ■

Thus it suffices, when testing for reversibility on $np^r$ cells, to do so only on $n$ cells. The next lemma is extremely useful, its proof can be found in appendix B, section B.3.

**Lemma 4.2.4** *Let $f$ be the local rule of an additive cellular automata over $\mathbb{F}_{p^q}$, not the trivial rule. Let $n$ be a non-zero positive integer such that $\gcd(n, p) = 1$. Let $\{\mathbb{T}_r\}_{r\in\mathbf{N}}$ be the $(x^n - 1)$-set of $f$. If $M_0(\mathbb{T}) \neq \emptyset$ then for any $i \in M_0(\mathbb{T})$ the associated $R_i(x)$-set $\{\mathbb{T}_{r,i}\}_{r\in\mathbf{N}}$ is non-trivial.* ■

If $\{\mathbb{T}_r\}_{r\in\mathbf{N}}$ is the $(x^n - 1)$-set of a local cellular automata rule $f$ we can apply lemma 4.2.4 to the $(x^n - 1)$-set $\{\mathbb{T}_r^L - a\}_{r\in\mathbf{N}}$ where $a \in \mathbb{F}_{p^q}$ and $L > 0$, and the associated $R_i(x)$-sets, $1 \leq i \leq m$, for $\mathbb{T}_r^L$ is the representative of the composition of $f$ with itself $L$ times and this is the local rule of an additive cellular automata and hence adding on an element of $\mathbb{F}_{p^q}$ one again has the local rule of an additive cellular automata.

### 4.2.1 Periodic behaviour when $U = 0$

We shall count the numbers of units and zero-divisors in $\frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$ and hence the numbers of distinct reversible and irreversible additive cellular automata rules on $np^r$ cells, the proof of the following result may be found in appendix B.

**Lemma 4.2.5** *For all* $r \in \mathbb{N}$

$$\begin{aligned} |U_{pq}(n)| &= \textstyle\prod_{i=1}^{m}(p^{qd_i}-1), \quad |U_{pq}(np^r)| &= p^{qn(p^r-1)}\,|U_{pq}(n)|\,, \\ |ZD_{pq}(n)| &= p^{qn}-|U_{pq}(n)|, \quad |ZD_{pq}(np^r)| &= p^{qn(p^r-1)}\,|ZD_{pq}(n)| \quad \blacksquare \end{aligned}$$

We can describe the set of fixed points for any $\mathbb{T}$ in $\frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]}$:

**Lemma 4.2.6** *For any* $\mathbb{T}$ *in* $\frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]}$, $Fix(\mathbb{T}) = \{0\}$ *if and only if* $M_1^r(\mathbb{T}) = \emptyset$.

*Further*

$$\begin{aligned} Fix(\mathbb{T}) &= \{a : a_i = 0 \ \forall\ i \in M \setminus M_1^r(\mathbb{T}), \\ & \qquad a_i \in \bigcup_{j=p^r-\mathcal{I}_i(\mathbb{T}_i-1)}^{p^r-1} \mathcal{D}_{R_i}(p^r d_i - 1, j) \cup \{0\} \ \forall\ i \in M_1^r(\mathbb{T})\} \end{aligned}$$

*and*

$$|Fix(\mathbb{T})| = p^{q\sum_{j\in M_1^r(\mathbb{T})}\mathcal{I}_j(\mathbb{T}_j-1)d_j}.$$

*where* $\mathbb{T}_j = \theta_r^j(\mathbb{T})$

Proof:

Suppose that $Fix(\mathbb{T}) = \{0\}$ but $\mathbb{T}_j - 1$ is nilpotent for some $j \in M$, then there is an element $a$ with $a_i = 0, i \neq j$ and $(\mathbb{T}_j - 1)a_j = 0$, then $\mathbb{T}a = a$ so $a \in Fix(\mathbb{T})$, a contradiction, hence $Fix(\mathbb{T}) = \{0\}$ implies $M_1^r(\mathbb{T}) = \emptyset$. Now suppose that $M_1^r(\mathbb{T}) = \emptyset$ and $a \in Fix(\mathbb{T})$, then $\mathbb{T}_i a_i = a_i$ for $1 \leq i \leq m$, and each $\mathbb{T}_i$ is either zero or $(\mathbb{T}_i - 1)a_i = 0$ so $\mathbb{T}_i - 1$ is nilpotent which contradicts $M_1^r(\mathbb{T}) = \emptyset$. The description of $Fix(\mathbb{T})$ follows from lemma 3.3.4 and lemma 3.3.8. Using lemma 3.3.9 one has

$$\left|\bigcup_{j=p^r-\mathcal{I}_i(\mathbb{T}_i-1)}^{p^r-1} \mathcal{D}_{R_i}(p^r d_i - 1, j)\right| = p^{\mathcal{I}_i(\mathbb{T}_i-1)qd_i} - 1.$$

Then

$$|Fix(\mathbb{T})| = \prod_{i\in M_1^r(\mathbb{T})}\left(p^{\mathcal{I}_i(\mathbb{T}_i-1)qd_i} - 1 + 1\right) = p^{q\sum_{i\in M_1^r(\mathbb{T})}\mathcal{I}_i(\mathbb{T}_i-1)d_i}. \quad \blacksquare$$

Note that for $r = 0$ lemma 4.2.6 reduces to

$$\begin{aligned} Fix(\mathbb{T}) &= \{a : a_i = 0 \ \forall\ i \in M \setminus M_1^0(\mathbb{T})\} \\ |Fix(\mathbb{T})| &= p^{q\sum_{i\in M_1^0(\mathbb{T})} d_i}, \end{aligned}$$

since in this case $\mathcal{I}_i(1-1) = p^0 = 1$.

In the following corollary we make our first use of lemma 4.2.4.

**Corollary 4.2.2** *Let $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$ be the $(x^n-1)$-set of an additive cellular automata. Then, for all $r \in \mathbb{N}$, $Fix(\mathbb{T}_r) = \{0\}$ if and only if $Fix(\mathbb{T}_0) = \{0\}$. Let $J > 0$ be the minimal integer such that $\mathbb{T}_{J,j} - 1 \neq 0$ for all $j \in M_1(\mathbb{T})$, then for all integers $I > 0$*

$$|Fix(\mathbb{T}_{J+I})| = |Fix(\mathbb{T}_J)|.$$

Proof:

That $Fix(\mathbb{T}_r) = \{0\}$ if and only if $Fix(\mathbb{T}_0) = \{0\}$ follows from lemma 4.2.3 and lemma 4.2.6. There is a integer $J$, minimal, such that $\mathbb{T}_{J,j} - 1 \neq 0$ by lemma 4.2.4 and the comments afterwards. For all $j \in M_1(\mathbb{T})$ , by lemma 3.3.11, $\mathcal{I}_j(\mathbb{T}_{J+s,j} - 1) = \mathcal{I}_j(\mathbb{T}_{J,j} - 1)$ for all $s \in \mathbb{N}$, it follows from lemma 4.2.6 that $|Fix(\mathbb{T}_{J+I})| = |Fix(\mathbb{T}_J)|$. ■

Note that if $J$ in corollary 4.2.2 is minimal for each associated $R_i(x)$-set, $i \in M_1(\mathbb{T})$, then for $r < J$ one has

$$|Fix(\mathbb{T}_r)| = |Fix(\mathbb{T}_0)|^{p^r}.$$

For each $N \in \mathbb{N} \setminus \{0\}$ one can define an equivalence relation on the set of all linear local rules by $f \sim_N g$ if $f$ and $g$ have the same representative on $N$ cells. We shall denote the $\sim_N$ equivalence class of $f$ by $[f]_N$ and say that $[f]_N$ has non-zero fixed points if the representative of $f$, $\mathbb{T}_f$, has non-zero fixed points and that $[f]_N$ is reversible if $\mathbb{T}_f$ is a unit *etc.*. One can use lemma 4.2.6 to count the number of distinct equivalence classes $[f]_{np^r}$ with no non-zero fixed points, any rule in such an equivalence class has qualitative behaviour on $np^r$ cells that cannot be altered by the presence of time independent inputs (by corollary 2.3.3).

**Lemma 4.2.7** *On $np^r$ cells, $r \in \mathbb{N}$, there are*

$$p^{qn(p^r-1)} \prod_{j\in M} (p^{qd_j} - 1)$$

*distinct $\sim_N$ equivalence classes $[f]_N$ with no non-zero fixed points, of which*

$$p^{qn(p^r-1)} \prod_{j\in M} (p^{qd_j} - 2)$$

*are reversible.*

Proof:

In the $j-th$ factor of $\frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$ there are $|Nil_{p^q}(R_j,r)|$ units $\mathbb{T}_j$ such that $\mathbb{T}_j-1$ is nilpotent for (remark A.1.1) if $P$ is nilpotent then $1-P$ is a unit, $U$ say, such that $U-1$ is nilpotent and conversely. By lemma 3.3.3, $|Nil_{p^q}(R_j,r)| = p^{qd_j(p^r-1)}$. By lemma 4.2.6 $Fix(\mathbb{T}) = \{0\}$ if and only if $M_1^r(\mathbb{T}) = \emptyset$. Thus there are

$$\prod_{j=1}^{m}\left(p^{qp^r d_j} - p^{qd_j(p^r-1)}\right) = p^{q(p^r-1)\sum_{j=1}^{m} d_j}\prod_{j=1}^{m}(p^{qd_j}-1) = p^{q(p^r-1)}\prod_{j=1}^{m}(p^{qd_j}-1)$$

$\mathbb{T}$ with $M_1^r(\mathbb{T}) = \emptyset$. If we only wish to count reversible rules with $M_1^r(\mathbb{T}) = \emptyset$ we have

$$\prod_{j=1}^{m}\left(p^{qp^r d_j} - 2\,|Nil_{p^q}(R_j,r)|\right) = p^{qn(p^r-1)}\prod_{j=1}^{m}(p^{qd_j}-2)$$

such rules. ■

**Corollary 4.2.3** *When the state alphabet is $\mathbb{F}_2$, if an additive cellular automata is reversible on $N$ cells then it has non-zero fixed points on $N$ cells.*

Proof:

This follows on putting $p=2$ and $q=1$ in lemma 4.2.7. ■

For any $a \in \frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$ define

$$\overline{M}_0^r(a) = \{j \in M : a_j = 0\},$$

and

$$\overline{M}_1^r(a) = \overline{M}_0^r(a-1).$$

Clearly $\overline{M}_0^0(a) = M_0^0(a)$ and $\overline{M}_1^0(a) = M_1^0(a)$.

We now give an explicit description of the maximal cycle length, the attracting set and the orbit length of any element under an additive cellular automata rule represented by $\mathbb{T}$ on $np^r$, $r \in \mathbb{N}$, the proof is in appendix B.

**Lemma 4.2.8** *On $np^r$ cells an additive cellular automata rule represented by $\mathbb{T} \in \frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$ has the following properties:*

(i) $\Pi_n(\mathbb{T}) = \mathrm{lcm}_{i\in M\setminus M_0^0(\mathbb{T})}(O(\mathbb{T}_i))$,

$$\Pi_{np^r}(\mathbb{T}) = p^S \Pi_n(\Gamma_{r,0}(\mathbb{T})), \quad S = \max_{i \in M \setminus M_0^r(\mathbb{T})}(S(\mathbb{T}_i));$$

(ii) $Att(\mathbb{T}) = \{a : a_i = 0 \ \forall \ i \in M_0^r(\mathbb{T})\}$,

$$|Att(\mathbb{T})| = |Att(\Gamma_{r,0}(\mathbb{T}))|^{p^r} = \left(p^{q \sum_{i \in M \setminus M_0^0(\Gamma_{r,o}(\mathbb{T}))} d_i}\right)^{p^r};$$

(iii) $(\phi_a)_0 = \mathrm{lcm}_{i \in M \setminus (M_0^0(a) \cup M_0^0(\mathbb{T}))}(O(\mathbb{T}_i))$,

*when* $r = 0$ *for any* $a$ *in* $\frac{\mathbb{F}_{p^q}[x]}{(x^n-1)\mathbb{F}_{p^q}[x]}$ *under* $\mathbb{T}$. *For* $r > 0$ *one has*

$$(\phi_a)_0 = p^J \mathrm{lcm}_{s \in M \setminus (\overline{M_0^r}(a) \cup M_0^r(\mathbb{T}))}(O(\pi_{r,0}^s(\mathbb{T}_s)))$$

*where* $(\phi_{\theta_r^s(a)})_0 = p^{j_s} O(\pi_{r,0}^s(\mathbb{T}_s))$ *and* $J = max(j_s)$. ■

From lemma 4.2.8 it is clear that $|Att(\mathbb{T})|$ depends only upon $r$ and $M_0^r(\mathbb{T})$.

**Corollary 4.2.4**

(i)*Let* $\{\mathbb{T}_r\}_{r \in \mathbb{N}}$ *be a* $(x^n - 1)$*-set such that there is a positive integer* $J$ *such that* $\mathbb{T}_{J,j}^{L(\mathbb{T}_j)} - 1 \neq 0$ *for all* $j \in M \setminus M_0(\mathbb{T})$. *Then*

$$\Pi_{np^{J+r}}(\mathbb{T}_{J+r}) = p^r \Pi_{np^J}(\mathbb{T}_J).$$

*If there is no such integer* $J$ *but there is an integer* $J'$ *such that* $\mathbb{T}_{J',j}^{L(\mathbb{T}_j)} - 1 \neq 0$ *for all* $j$ *in some non empty subset of* $M \setminus M_0(\mathbb{T})$ *then the above still holds with* $J$ *replaced by* $J'$, *otherwise*

$$\Pi_{np^r}(\mathbb{T}_r) = \Pi_n(\mathbb{T}_0) \quad \textit{for all } r \in \mathbb{N}.$$

(ii) *Let* $\{\mathbb{T}_r\}_{r \in \mathbb{N}}$ *be the* $(x^n - 1)$*-set of a non-trivial additive cellular automata then there is some positive integer* $J$ *such that*

$$\Pi_{np^{J+r}}(\mathbb{T}_{J+r}) = p^r \Pi_{np^J}(\mathbb{T}_J).$$

Proof:

(i) In the case where either $J$ or $J'$ exists the result follows from lemma 3.3.11 (iv) as $\max_{j \in M \setminus M_0(\mathbb{T})}(S_j + 1) = \max_{j \in M \setminus M_0(\mathbb{T})}(S_j) + 1$. When neither $J$ or $J'$ exist one has $S_j = S(\theta_r^j(\mathbb{T})) = 0$ for all $j \in M \setminus M_0(\mathbb{T})$ and $r \in \mathbb{N}$ and the result follows.

(ii) Follows from lemma 4.2.4 and part (i). ■

**Corollary 4.2.5** *Let $f$ be the local rule of an additive cellular automata which is not reversible on $n$ cells, then the fraction of configurations on cycles on $np^r$ cells*

$$\frac{|Att(\mathbb{T})|}{p^{qnp^r}} \longrightarrow 0 \quad as \quad r \longrightarrow \infty.$$

proof:

Consider the $(x^n - 1)$-set of $f$, $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$. By part (ii) of lemma 4.2.8 the fraction of configurations on cycles under $\mathbb{T}_r$ is

$$\frac{p^{qp^r \sum_{j\in M\setminus M_0(\mathbb{T})} d_j}}{p^{qnp^r}} = \frac{1}{(p^{q\sum_{j\in M_0(\mathbb{T})} d_j})^{p^r}} \longrightarrow 0 \quad \text{as} \quad r \longrightarrow \infty. \quad \blacksquare$$

We are now in a position to describe the cycle set of $\mathbb{T}$.

**Theorem 4.2.1** *For any $\mathbb{T} \in \frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$, $\Sigma(\mathbb{T})$ is given by the cycle product*

$$\Sigma(\mathbb{T}) = p^{p^r q\beta} \prod_{j\in M\setminus(M_0^r(\mathbb{T})\cup\overline{M_1^r}(\mathbb{T}))} \Sigma(\mathbb{T}_j),$$

*where*

$$\beta = \sum_{M_0^r(\mathbb{T})\cup\overline{M_1^r}(\mathbb{T})} d_i.$$

*In particular, when $r = 0$,*

$$\Sigma(\mathbb{T}) = p^{q\beta} \prod_{M\setminus(M_0^0(\mathbb{T})\cup M_1^0(\mathbb{T}))} \left(1[1] + \frac{p^{qd_i} - 1}{O(\mathbb{T}_i)}[O(\mathbb{T}_i)]\right)$$

*where*

$$\beta = \sum_{M_1^0(\mathbb{T})} d_i.$$

Proof:

Using theorem 1.5.1 the cycle set of $\mathbb{T}$ is the cycle product

$$\left(\prod_{M_0^r(\mathbb{T})} 1[1]\right)\left(\prod_{\overline{M_1^r}(\mathbb{T})} p^{p^r qd_i}[1]\right) \prod_{M\setminus(M_0^0(\mathbb{T})\cup\overline{M_1^r}(\mathbb{T}))} \Sigma(\mathbb{T}_j).$$

The result then follows by applying the definition of the cycle product and in the $r = 0$ case from lemma 3.2.1. ■

In theorem 4.2.1, the $\Sigma(\mathbb{T}_j)$ are in general given by theorem 3.3.2, examining that theorem one sees that $\Sigma(\mathbb{T}_j)$, $j \notin M_0^r(\mathbb{T})$, is determined completely by $L(\mathbb{T}_j)$ and $\mathcal{I}_j(\mathbb{T}_j^{L(\mathbb{T}_j)} - 1)$, thus we have the following remark:

**Remark 4.2.1** *On $np^r$ cells $\Sigma(\mathbb{T})$ is determined completely by $M_0^r(\mathbb{T})$ and the $|M \setminus M_0^r(\mathbb{T})|$ pairs of positive integers $(L(\mathbb{T}_j), \mathcal{I}_j(\mathbb{T}_j^{L(\mathbb{T}_j)} - 1))$, $j \in M \setminus M_0^r(\mathbb{T})$.* ■

For an $(x^n - 1)$-set $\{\mathbb{T}_r\}_{r \in \mathbb{N}}$ such that there is an integer $J > 0$ such that $\mathbb{T}_{J,i}^{L_i} - 1 \neq 0$ for all $i \in M \setminus M_0^r(\mathbb{T})$ (for instance the $(x^n - 1)$-set of an additive cellular automata) then for $r > J$, $\overline{M_1^r}(\mathbb{T}) = \emptyset$. It is particularly easy to use theorem 3.3.3 to construct the cycle set of $\mathbb{T}_{J+r}$ from the cycle sets of the $\mathbb{T}_{J+r,i}$ for all $r \in \mathbb{N}$, for by lemma 3.3.11 and the comments afterwards one has the same $L_i$, $i \in M \setminus M_0^r(\mathbb{T})$ for all $r \in \mathbb{N}$ and $\mathcal{I}_i(\mathbb{T}_{J+r,i}^{L_i} - 1) = \mathcal{I}_i(\mathbb{T}_{J,i}^{L_i} - 1)$, hence $\Sigma(\mathbb{T}_{J+r,i})$ is computed easily using theorem 3.3.3 and of course

$$\Sigma(\mathbb{T}_{J+r}) = p^{\beta r + J q \beta} \prod_{i \in M \setminus M_0^r(\mathbb{T})} \Sigma(\mathbb{T}_{J+r,i}), \quad \beta = \sum_{j \in M_0^r(\mathbb{T})} d_j.$$

We showed in corollary 4.2.5 that for cellular automata rule $f$ which is not reversible on $n$ cells the fraction of configurations on cycles on $np^r$ cells vanishes in the limit $r \longrightarrow \infty$. The situation, even for rules not reversible on $n$ cells, is somewhat different for the fraction $\Xi_N$ of configurations on cycles that are on cycles of the maximal length $\Pi_N(\mathbb{T})$ occurring under $\mathbb{T}$ on $N$ cells.

Martin *et. al.* [3] made the observation that for large $N$ it appears that nearly all configurations on cycles are on cycles of length $\Pi_N(\mathbb{T})$. We note that a lower bound on $n$ cells $(\gcd(p, n) = 1)$ for $\Xi_n$ is, using theorem 4.2.1

$$\Xi_{n,L} = p^{q\beta} \prod_{j \in M \setminus (M_0^0(\mathbb{T}) \cup M_1^0(\mathbb{T}))} \left( \frac{p^{qd_j} - 1}{p^{qd_j}} \right), \quad \beta = \sum_{i \in M_1^0(\mathbb{T})} d_j.$$

As the $r$ increases we can improve the lower bound $\Xi_{np^r,L}$ as we show in the next result.

**Theorem 4.2.2** *Let $\{\mathbb{T}_r\}_{r \in \mathbb{N}}$ be the $(x^n - 1)$-set of an additive cellular automata. Then*

$$\Xi_{np^r} \longrightarrow 1 \quad as \quad r \longrightarrow \infty.$$

Proof:

Clearly $\Xi_{np^r}$ is bounded above by 1. A lower bound $\Xi_{np^r,L}$ is given by the product of the fractions $\Xi_j^r$, $j \in M \setminus M_0(\mathbb{T})$, of configurations in $\frac{\mathbb{F}_{pq}[x]}{(R_j(x)^{p^r}\mathbb{F}_{pq}[x]}$ on cycles under $\mathbb{T}_{r,j}$ which are on cycles of the maximal length occurring under $\mathbb{T}_{r,j}$. A lower bound on $\Xi_j^r$ is, using theorem 3.3.2,

$$\frac{p^{p^r qd_j} - p^{\mathcal{I}_j(\mathbb{T}_{r,j}^{L_j}-1)p^{S_j-1}qd_j}}{p^{p^r qd_j}},$$

unless $L_j = 1$ and $\mathbb{T}_{r,j} = 1$ when $\Xi_j^r = 1$, however, by lemma 4.2.4 there is some $r' \in \mathbb{N}$ such that $\mathbb{T}_{r,j}^{L_j} - 1 \neq 0$ for all $j \in M \setminus M_0(\mathbb{T})$ and by lemmas 3.3.10 and 3.3.11 we see that $\mathcal{I}_j(\mathbb{T}_{r,j}^{L_j} - 1) = \mathcal{I}_j(\mathbb{T}_{r',j}^{L_j} - 1)$ for all $r \geq r'$ and, for $s \in \mathbb{N}$, $S(\mathbb{T}_{r'+s,j}) = r' + s - n_j$ when $p^{n_j} \leq \mathcal{I}_j(\mathbb{T}_{r',j}^{L_j} - 1) < p^{n_j+1}$. Hence for $r > r'$ the lower bound on $\Xi_j^r$ becomes

$$\frac{p^{p^r qd_j} - p^{(p^{n_j+1}-1)p^{r-n_j-1}qd_j}}{p^{p^r qd_j}} = 1 - \frac{1}{p^{p^{r-n_j-1}qd_j}} \longrightarrow 1 \quad \text{as} \quad r \longrightarrow \infty.$$

It now follows (by elementary analysis) that $\Xi_j^r \longrightarrow 1$ as $r \longrightarrow \infty$ and hence that the lower bound on $\Xi_{np^r}$ goes to 1 in the limit of $r \longrightarrow \infty$ and hence $\Xi_{np^r}$ goes to 1 in the limit of $r \longrightarrow \infty$. ■

### 4.2.2 Transient behaviour

When $M_0^r(\mathbb{T}) \neq \emptyset$ one has non-trivial transient behaviour, corresponding to non-trivial tree structure in the state transition graph. Of particular interest are the garden of Eden configurations, *i.e.* the elements without predecessors. We shall sometimes refer to such elements as leaves (in reference to the state transition graph). Given $a \in \frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]}$, $a$ is a leaf if and only if there is some $i \in M_0^r(\mathbb{T})$ such that $\theta_r^i(a) = a_i$ is a leaf under $\theta_r^i(\mathbb{T}) = \mathbb{T}_i$. We shall denote the set of leaves under $\mathbb{T}_i$ by $Lf^r(\mathbb{T}, i)$ and the set of leaves under $\mathbb{T}$ by $Lf^r(\mathbb{T})$. Similarly we shall denote the set of elements with predecessors under $\mathbb{T}_i$ by $NLf^r(\mathbb{T}, i)$ and the set of elements with predecessors under $\mathbb{T}$ by $NLf^r(\mathbb{T})$.

**Lemma 4.2.9** *The set of elements with predecessors under* $\mathbb{T}$ *is, where* $\prod$ *is the Cartesian product,*

$$NLf^r(\mathbb{T}) = \prod_{i \in M_0^r(\mathbb{T})} NLf^r(\mathbb{T}, i) \prod_{j \in M \setminus M_0^r(\mathbb{T})} \frac{\mathbb{F}_{p^q}[x]}{R_j^{p^r}(x)\mathbb{F}_{p^q}[x]},$$

*the set of garden of Eden states is*

$$Lf^r(\mathbb{T}) = \prod_{s \in M} \frac{\mathbb{F}_{p^q}[x]}{R_s^{p^r}(x)\mathbb{F}_{p^q}[x]} \setminus NLf^r(\mathbb{T})$$

*and*

$$|Lf^r(\mathbb{T})| = \frac{p^{qp^r n}}{p^{q\sum_{i \in m_0^r(\mathbb{T})} \mathcal{I}_i(\mathbb{T}_i)d_i}} \left( p^{q\sum_{i \in m_0^r(\mathbb{T})} \mathcal{I}_i(\mathbb{T}_i)d_i} - 1 \right).$$

Proof:

The first two statements are obvious. Let $I_i = \mathcal{I}_i(\mathbb{T}_i)$ for each $i \in M_0^r(\mathbb{T})$, then using lemma 3.3.12 one has

$$NLf^r(\mathbb{T}, i) = \frac{\mathbb{F}_{p^q}[x]}{R_i^{p^r}(x)\mathbb{F}_{p^q}[x]} \setminus \bigcup_{0 < I_a < I_i} \mathcal{D}_R(p^r d - 1, I_a),$$

using (3.3.3) now gives

$$|NLf^r(\mathbb{T}, i)| = p^{p^r q d_i} - p^{(p^r - I_i)qd_i}(p^{I_i q d_i} - 1) = p^{p^r q d_i - I_i q d_i} = p^{qd_i(p^r - I_i)}.$$

Using the above one sees that

$$|NLf^r(\mathbb{T})| = \prod_{i \in M_0^r(\mathbb{T})} p^{qd_i(p^r - I_i)} \prod_{j \in M \setminus M_0^r(\mathbb{T})} p^{p^r q d_j} = p^{q(p^r n - \sum_{i \in M_0^r(\mathbb{T})} I_i d_i)}$$

and hence

$$|Lf^r(\mathbb{T})| = p^{p^r qn} - p^{q(p^r n - \sum_{i \in M_0^r(\mathbb{T})} I_i d_i)} = \frac{p^{p^r qn}}{p^{q\sum_{i \in M_0^r(\mathbb{T})} I_i d_i}} \left( p^{q\sum_{i \in M_0^r(\mathbb{T})} I_i d_i} - 1 \right). \quad \blacksquare$$

**Corollary 4.2.6** *Let* $J$ *be the minimum integer such that* $\mathbb{T}_i \neq 0$ *for all* $i \in M_0^r(\mathbb{T})$. *Then for any* $s \in \mathbb{N}$

$$|Lf^{J+s}(\mathbb{T})| = p^{qnp^J(p^s-1)}|Lf^J(\mathbb{T})|$$

*and the fraction* $\frac{|Lf^{J+s}(\mathbb{T})|}{p^{qp^r n}}$ *of garden of Eden states is* $\frac{|Lf^J(\mathbb{T})|}{p^{qp^J n}}$.

Proof:

The minimal integer $J$ exists by lemma 4.2.4, the result then follows easily from lemma 4.2.9. ■

One could use a similar technique to that used to count the garden of Eden states in the proof of lemma 4.2.9 to count the numbers of elements at a particular height, however as we shall see in the next lemma, it is far easier to use a different technique. We shall continue to use the notation $I_i = \mathcal{I}_i(\mathbb{T}_i)$ for each $i \in M_0^r(\mathbb{T})$.

**Lemma 4.2.10** *The maximum tree height under* $\mathbb{T}$ *is* $T = \max_{i \in M_0^r(\mathbb{T})}(\lceil p^r / I_i \rceil)$, *every element not a garden of Eden state has exactly* $p^{q\sum_{i \in M_0^r(\mathbb{T})} I_i d_i}$ *predecessors and the number of elements at height* $t$ , $1 \leq t \leq T$, *is*

$$p^{qp^r \sum_{M \setminus M_0^r(\mathbb{T})} d_j} p^{(t-1)q\sum_{M_0^r(\mathbb{T})} I_i d_i} \left( p^{q\sum_{M_0^r(\mathbb{T})} I_i d_i} - 1 \right).$$

Proof:

That the maximum tree height is $max_{i \in M_0^r(\mathbb{T})}(\lceil p^r / I_i \rceil)$ follows from lemma 3.3.12. By theorem 2.2.1 the trees rooted at each element of $Att(\mathbb{T})$ are identical so to count numbers of predecessors it is sufficient to do so for $T_0(\mathbb{T}, 0)$. Clearly we can write $T_0(\mathbb{T}, 0)$ as the Cartesian product

$$T_0(\mathbb{T}, 0) = \prod_{i \in M_0^r(\mathbb{T})} \frac{\mathbb{F}_{p^q}[x]}{R_i^{p^r}(x)\mathbb{F}_{p^q}[x]} \times \{0\}^{|M \setminus M_0^r(\mathbb{T})|}.$$

Let $|M_0^r(\mathbb{T})| = k$, let $a \in T_0(\mathbb{T}, 0)$, not a leaf, then we can write $a = (a_1, \ldots, a_k, 0, \ldots, 0)$. Any $m$-tuple $(b_1, \ldots, b_k, 0, \ldots, 0)$ such that $\mathbb{T}_i b_i = a_i$, $1 \leq i \leq k$, is a predecessor of $a$. For non-zero $a_i$ there are, by theorem 3.3.4, $p^{I_i q d_i}$ such $b_i$ and for $a_i = 0$ there are, again by theorem 3.3.4, $p^{I_i q d_i} - 1$ such $b_i$ that are non-zero, but zero is a predecessor of zero and it follows that every $a \in T_0(\mathbb{T}, 0)$, $a$ not a leaf, has $\prod_{i \in M_0^r(\mathbb{T})} p^{I_i q d_i} = p^{q\sum_{i \in M_0^r(\mathbb{T})} I_i d_i}$ predecessors, hence by theorem 2.2.1 every element not a leaf has this number of predecessors. It follows from the above that the number of elements at height 1 in $T_0(\mathbb{T}, 0)$ is $p^{q\sum_{i \in M_0^r(\mathbb{T})} I_i d_i} - 1$, the number of elements at height 2 in $T_0(\mathbb{T}, 0)$ is $p^{q\sum_{i \in M_0^r(\mathbb{T})} I_i d_i}(p^{q\sum_{i \in M_0^r(\mathbb{T})} I_i d_i} - 1)$ and by induction that the number of elements at height $t$, $1 \leq t \leq T$, in $T_0(\mathbb{T}, 0)$ is

$$p^{(t-1)q\sum_{i \in M_0^r(\mathbb{T})} I_i d_i}(p^{q\sum_{i \in M_0^r(\mathbb{T})} I_i d_i} - 1).$$

Employing theorem 2.2.1 once again we see that the total number of elements at height $t$, $1 \leq t \leq T$, is

$$\begin{aligned} & |Att(\mathbb{T})|p^{(t-1)q\sum_{i\in M_0^r(\mathbb{T})} I_i d_i}(p^{q\sum_{i\in M_0^r(\mathbb{T})} I_i d_i} - 1) \\ = \quad & p^{qp^r \sum_{M\setminus M_0^r(\mathbb{T})} d_j} p^{(t-1)q\sum_{M_0^r(\mathbb{T})} I_i d_i}\left(p^{q\sum_{M_0^r(\mathbb{T})} I_i d_i} - 1\right) \end{aligned}$$

by lemma 4.2.8. ■

**Corollary 4.2.7** *The maximum possible tree height on $np^r$ cells is $p^r$, which occurs if $I_i = 1$ for some $i \in M_0^r(\mathbb{T})$.*

Proof:

Immediate from lemma 4.2.10. ■

**Corollary 4.2.8** *Let $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$ be the $(x^n - 1)$-set of an additive cellular automata, let $J$ be the least integer such that $T_{J,i} \neq 0$ for all $j \in M_0^r(\mathbb{T})$. Then the number of predecessors of any configuration which is not a garden of Eden configuration on $np^r$ cells, $r \geq J$, is fixed and equal the number for $r = J$.*

Proof:

We know from lemma 4.2.4 that $J$ exists, then by lemma 3.3.11, $\mathcal{I}_i(\mathbb{T}_{r,i}) = \mathcal{I}_i(\mathbb{T}_{J,i})$ for all $r \geq J$ and $i \in M_0^r(\mathbb{T})$ and the result follows from lemma 4.2.10. ■

On comparing the numbers of elements at height $T$ with the numbers of leaves one sees that all the leaves are at height $T$ if and only if

$$\begin{aligned} 0 \quad &= \quad p^r \sum_{M\setminus M_0^r(\mathbb{T})} d_i + T\sum_{M_0^r(\mathbb{T})} I_j d_j - p^r n \\ \Leftrightarrow \qquad T \quad &= \quad \frac{p^r(n - \sum_{M\setminus M_0^r(\mathbb{T})} d_i)}{\sum_{m_0^r(\mathbb{T})} I_j d_j} = p^r \frac{\sum_{M_0^r(\mathbb{T})} d_i}{\sum_{M_0^r(\mathbb{T})} I_j d_j}, \end{aligned}$$

where we have used lemmas 4.2.9 and 4.2.10. Thus the trees are balanced if and only if $\mathbb{T}$ takes this value, and in that case $T = p^r$ if and only if $I_j = 1$ for each $j \in M_0^r(\mathbb{T})$.

**Remark 4.2.2** *Examining the results in this section one sees that the qualitative tree structure, i.e. the numbers of elements in each tree, the height of the tree and the in-degrees of the vertices, is completely determined by $M_0^r(\mathbb{T})$ and the $|M_0^r(\mathbb{T})|$ positive integers $\mathcal{I}_i(\mathbb{T}_i)$, $i \in M_0^r(\mathbb{T})$.* ■

We have a special case when $r = 0$, we summarise the results for that case bellow.

**Theorem 4.2.3** *When* $\gcd(p, n) = 1$ *and* $\mathbb{T} \in \frac{\mathbb{F}_{p^q}[x]}{(x^n-1)\mathbb{F}_{p^q}[x]}$ *is not a unit the trees rooted at each element of* $Att(\mathbb{T})$ *have height* 1 *and consist of* $p^{q\sum_{M_0(\mathbb{T})} d_i} - 1$ *leaves. The leaves are the units and those non-units* $a$ *satisfying*

$$(M \setminus M_0(a)) \cap M_0(\mathbb{T}) \neq \emptyset.$$

Proof:

That the maximum tree height that can occur in this case is 1 follows from corollary 4.2.7. The number of leaves in each tree is $\frac{|Lf^0(\mathbb{T})|}{p^{q\sum_{M_1(\mathbb{T})} d_i}}$ and using lemma 4.2.9 gives the stated result. If $a$ is not a unit but is a leaf then we must have $a_i \neq 0$ for some $i \in M_0(\mathbb{T})$, thus any non-unit satisfying $(M \setminus M_0(a)) \cap M_0(\mathbb{T}) \neq \emptyset$ is a leaf. ■

In general for an element $a$, not a unit, to be a leaf one needs

$$(M \setminus \overline{M}_0^r(a)) \cap M_0^r(\mathbb{T}) \neq \emptyset.$$

## 4.3 Dynamics in $\frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$ when $U \neq 0$

We recall from chapter 2 (theorem 2.3.1) that $\mathbb{T}$ and $\mathbb{T}_U$ are QDS if and only if $Fix(\mathbb{T}_U) \neq \emptyset$. When $\mathbb{T}$ and $\mathbb{T}_U$ are QDS and we know the behaviour of $\mathbb{T}$ then to find the behaviour of $\mathbb{T}_U$ it is sufficient, by the proof of theorem 2.3.1, to know a single fixed point of $\mathbb{T}_U$. for if $a$ is such a fixed point then the map $\phi_a : Att(\mathbb{T}) \longrightarrow Att(\mathbb{T}_U), b \mapsto a+b$ maps distinct cycles to distinct cycles and further, extending $\phi_a$ to $\frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$ in the obvious way, it is clear that $\phi_a$ preserves tree structure (as it is a bijection and satisfies $\mathbb{T}_U \circ \phi_a = \phi_a \circ \mathbb{T}$). If we do not want such detailed information but wish to know what the elements of $Att(\mathbb{T}_U)$ are, or the set of elements on orbits of a particular period we apply theorem 2.2.2 or lemma 2.2.1.

We can describe and count the inputs $U$ such that $\mathbb{T}$ and $\mathbb{T}_U$ are QDS.

**Lemma 4.3.1** *For any* $\mathbb{T} \in \frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$, $\mathbb{T}$ *and* $\mathbb{T}_U$ *are* QDS *for all* $U \in \frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$ *if and only if* $M_1^r(\mathbb{T}) = \emptyset$. *If* $M_1^r(\mathbb{T}) \neq \emptyset$ *then the inputs* $U$ *such that* $\mathbb{T}$ *and* $\mathbb{T}_U$ *are* QDS *are the elements of the Cartesian product*

$$\prod_{i \in M_1^r(\mathbb{T})} \left( \{0\} \cup \bigcup_{I_i = \mathcal{I}_i(\mathbb{T}_i - 1)}^{p^r-1} \mathcal{D}_{R_i}(p^r d_i - 1, I_i) \right) \prod_{j \in M \setminus M_1^r(\mathbb{T})} \frac{\mathbb{F}_{p^q}[x]}{R_j(x)^{p^r}\mathbb{F}_{p^q}[x]}$$

*and the inputs $U$ such that $\mathbb{T}$ and $\mathbb{T}_U$ are not* QDS *are the elements of the Cartesian product*

$$\prod_{i\in M_1^r(\mathbb{T})}\left(\bigcup_{I_i=0}^{\mathcal{I}_i(\mathbb{T}_i-1)-1}\mathcal{D}_{R_i}(p^r d_i-1,I_i)\right)\prod_{j\in M\setminus M_1^r(\mathbb{T})}\frac{\mathbb{F}_{p^q}[x]}{R_j(x)^{p^r}\mathbb{F}_{p^q}[x]}.$$

*There are* $p^{q(p^r n-\sum_{i\in M_1^r(\mathbb{T})}\mathcal{I}_i(\mathbb{T}_i-1)d_i)}$ *inputs $U$ such that $\mathbb{T}$ and $\mathbb{T}_U$ are QDS.*

Proof:

By lemma 4.2.6 $M_1^r(\mathbb{T})=\emptyset$ if and only if $Fix(\mathbb{T})=\{0\}$. By corollary 2.3.3 $\mathbb{T}$ and $\mathbb{T}_U$ are QDS for all inputs $U$ if and only if $Fix(\mathbb{T})=\{0\}$ and so the first statement is true. When $M_1^r(\mathbb{T})\neq\emptyset$, then for $i\in M_1^r(\mathbb{T})$, we know from lemma 3.3.14 that $(\mathbb{T}_i)_{U_i}$ has a fixed point if and only if $U_i$ is nilpotent and $\mathcal{I}_i(\mathbb{T}_i-1)\leq\mathcal{I}_i(U_i)$, thus for such $i$ the $U_i$ with $\mathbb{T}_i$ and $(\mathbb{T}_i)_{U_i}$ QDS are the elements of

$$\bigcup_{I_i=\mathcal{I}_i(\mathbb{T}_i-1)}^{p^r-1}\mathcal{D}_{R_i}(p^r d_i-1,I_i)\cup\{0\}$$

and the $U_i$ with $\mathbb{T}_i$ and $(\mathbb{T}_i)_{U_i}$ not QDS are the elements of

$$\bigcup_{I_i=0}^{\mathcal{I}_i(\mathbb{T}_i-1)-1}\mathcal{D}_{R_i}(p^r d_i-1,I_i).$$

The description of the sets of inputs $U$ such that $\mathbb{T}$ and $\mathbb{T}_U$ are QDS (not QDS) follows.

By corollary 2.3.3 there are

$$\frac{\left|\frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}\right|}{|Fix(\mathbb{T})|}=\frac{p^{p^r qn}}{p^{q\sum_{i\in M_1^r(\mathbb{T})}\mathcal{I}_i(\mathbb{T}_i-1)d_i}}$$

$U$ such that $\mathbb{T}$ and $\mathbb{T}_U$ are QDS, where we have used lemma 4.2.6. ■

**Corollary 4.3.1** *The fraction of inputs $U$ such that $\mathbb{T}$ and $\mathbb{T}_U$ are* QDS *is*

$$\frac{1}{p^{q\sum_{i\in M_1^r(\mathbb{T})}\mathcal{I}_i(\mathbb{T}_i-1)d_i}}.$$

*If $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$ is the $(x^n-1)$-set of an additive cellular automata and $J$ is the minimal integer such ihat $\mathbb{T}_{J,i}-1\neq 0$ for all $i\in M_1(\mathbb{T})$, then the fraction of inputs $U$ such that $\mathbb{T}_r$ and $(\mathbb{T}_r)_U$ are* QDS *is constant and equal to the fraction for $\mathbb{T}_J$ for all integers $r\geq J$.*

Proof:

The first part is immediate from the lemma. For the second part, $J$ exists by lemma 4.2.4 and for all $r \geq J$ and all $i \in M_1(\mathbb{T})$, by lemma 3.3.11, $\mathcal{I}_i(\mathbb{T}_{r,i} - 1) = \mathcal{I}_i(\mathbb{T}_{J,i} - 1)$ hence the result follows from the first part. ■

**Definition 4.3.1** *For any* $\mathbb{T}$ *and* $U$ *in* $\frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$*:*

$$M_1^r(\mathbb{T}, U) = \{i \in M_1^r(\mathbb{T}) \setminus \overline{M}_1^r(\mathbb{T}) : \mathcal{I}_i(\mathbb{T}_i - 1) > \mathcal{I}_i(U_i)\}.$$

Note that $\mathcal{I}_i(\mathbb{T}_i - 1) > \mathcal{I}_i(U_i)$ includes the case $U_i$ a unit for then $\mathcal{I}_i(U_i) = 0$.

**Lemma 4.3.2** *For any* $\mathbb{T}$ *and* $U$ *in* $\frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$, $\mathbb{T}_U$ *has a fixed point if and only if* $M_1^r(\mathbb{T}, U) = \emptyset$ *and* $\overline{M}_1^r(\mathbb{T}) \subseteq M_0^r(U)$.

Proof:

Suppose $\mathbb{T}_U$ has a fixed point, $a$ say. Then $a_i \in Fix((\mathbb{T}_i)_{U_i})$ for all $i \in M$ but if $i \in M_1^r(\mathbb{T}, U)$ then, by lemma 3.3.14, $(\mathbb{T}_i)_{U_i}$ has no fixed points and thus $M_1^r(\mathbb{T}, U)$ must be empty. For $i \in \overline{M}_1^r(\mathbb{T})$ we have $a_i + U_i = a_i$ hence $U_i = 0$ hence $\overline{M}_1^r(\mathbb{T}) \subseteq M_0^r(U)$.

Now suppose that $M_1^r(\mathbb{T}, U) = \emptyset$ and $\overline{M}_1^r(\mathbb{T}) \subseteq M_0^r(U)$, we construct fixed points for $\mathbb{T}_U$. We can partition $M$ into the disjoint union

$$M = \bigcup_{i=1}^{6} \mathcal{M}_i, \tag{4.3.1}$$

where

$$\begin{aligned}
\mathcal{M}_1 &= M_0^r(U) \setminus (M_1^r(\mathbb{T}) \cup M_0^r(U)); \\
\mathcal{M}_2 &= \overline{M}_1^r(\mathbb{T}); \\
\mathcal{M}_3 &= (M_1^r(\mathbb{T}) \cap M_0^r(U)) \setminus \overline{M}_1^r(\mathbb{T}); \\
\mathcal{M}_4 &= M_1^r(\mathbb{T}) \setminus (M_1^r(\mathbb{T}) \cap M_0^r(U)); \\
\mathcal{M}_5 &= M \setminus (M_1^r(\mathbb{T}) \cup M_0^r(U) \cup M_0^r(\mathbb{T})); \\
\mathcal{M}_6 &= M_0^r(\mathbb{T}) \setminus (M_0^r(\mathbb{T}) \cap M_0^r(U)).
\end{aligned}$$

The fixed points of $\mathbb{T}_U$ are the elements $a$ of the form:

$$\begin{aligned}
a_i &= 0, && i \in \mathcal{M}_1;\\
a_i &= a_i^*, && i \in \mathcal{M}_2, \text{ where } a_i^* \text{ is any element of } \tfrac{F_{p^q}[x]}{R_i(x)^{p^r}\mathbb{F}_{p^q}[x]};\\
a_i &= a_i^*, && i \in \mathcal{M}_3, \text{ where } a_i^* \text{ is any fixed point of } \mathbb{T}_i;\\
a_i &= a_i^*, && i \in \mathcal{M}_4, \text{ where } a_i^* \text{ is any fixed point of } (\mathbb{T}_i)_{U_i};\\
a_i &= -(\mathbb{T}_i - 1)^{-1}U_i, && i \in \mathcal{M}_5;\\
a_i &= (\mathbb{T}_i^{T_i-1} + \ldots + \mathbb{T}_i + 1)U_i, && i \in \mathcal{M}_6,
\end{aligned}$$

where for $i \in \mathcal{M}_3$, $\mathbb{T}_i$ has non-zero fixed points by lemma 4.2.6 and for $i \in \mathcal{M}_4$, $(\mathbb{T}_i)_{U_i}$ has non-zero fixed points by lemma 3.3.14 and for $i \in \mathcal{M}_6$, $T_i$ is the maximum tree height under $\mathbb{T}_i$ and the stated expression gives the unique fixed point in this case by lemma 3.3.14. ■

Of course, if $\mathbb{T}_U$ has fixed points then, as $\mathbb{T}$ and $\mathbb{T}_U$ are QDS, one has

$$|Fix(\mathbb{T}_U)| = |Fix(\mathbb{T})|.$$

**Remark 4.3.1** *Examining the results of chapter 3 it is clear that any difference in the qualitative behaviour of $\mathbb{T}_U$ from that of $\mathbb{T}$ is determined by $M_1^r(\mathbb{T})$ and the $|M_1^r(\mathbb{T})|$ pairs of positive integers $(\mathcal{I}_i(\mathbb{T}_i - 1).\mathcal{I}_i(U_i))$.* ■

When $\mathbb{T}$ has non-zero fixed points and $\Sigma(\mathbb{T}) \neq \Sigma(\mathbb{T}_U)$ then either $M_1^r(\mathbb{T}, U) \neq \emptyset$ or $\overline{M_1^r}(\mathbb{T}) \subsetneq M_0^r(U)$ or both. If $i \in \overline{M_1^r}(\mathbb{T}) \setminus (\overline{M_1^r}(\mathbb{T}) \cap M_0^r(U))$ then clearly

$$\Sigma((\mathbb{T}_i)_{U_i}) = p^{p^r q d_i - 1}[p]. \tag{4.3.2}$$

One can write $M_1^r(\mathbb{T}, U) = \bigcup_{i=1}^5 \mathcal{M}_{1,i}^r(\mathbb{T}, U)$, a disjoint union, where, with $\mathcal{I}_i(\mathbb{T}_i^{L(\mathbb{T}_i)} - 1) = I_i$ and $I_i p^{S_i} = p^r + k_i$, $k_i \geq 0$.

$$\begin{aligned}
\mathcal{M}_{1,1}^r(\mathbb{T}, U) &= \{i : U_i \text{ a } \textit{unit} \text{ and } I_i(p^{S_i} - 1) \geq p^r\};\\
\mathcal{M}_{1,2}^r(\mathbb{T}, U) &= \{i : U_i \text{ a } \textit{unit} \text{ and } I_i(p^{S_i} - 1) < p^r\};\\
\mathcal{M}_{1,3}^r(\mathbb{T}, U) &= \{i : 0 < \mathcal{I}_i(U_i) < I_i \text{ and } (\phi_{U_i})_0 = p^{S_i - 1}\};\\
\mathcal{M}_{1,4}^r(\mathbb{T}, U) &= \{i : 0 < \mathcal{I}_i(U_i) < I_i \text{ and } (\phi_{U_i})_0 = p^{S_i} \text{ and } \mathcal{I}_i(U_i) + k_i \geq I_i\};\\
\mathcal{M}_{1,5}^r(\mathbb{T}, U) &= \{i : 0 < \mathcal{I}_i(U_i) < I_i \text{ and } (\phi_{U_i})_0 = p^{S_i} \text{ and } \mathcal{I}_i(U_i) + k_i < I_i\}.
\end{aligned}$$

Recalling theorems 3.3.5 and 3.3.6 we see that

$$\begin{aligned}
i \in \mathcal{M}^r_{1,1}(\mathbb{T}, U) &\Rightarrow \Sigma((\mathbb{T}_i)_{U_i}) = p^{p^r q d_i - S_i}[p^{S_i}];\\
i \in \mathcal{M}^r_{1,2}(\mathbb{T}, U) &\Rightarrow \Sigma((\mathbb{T}_i)_{U_i}) = p^{p^r q d_i - S_i - 1}[p^{S_i+1}];\\
i \in \mathcal{M}^r_{1,3}(\mathbb{T}, U) &\Rightarrow \Sigma((\mathbb{T}_i)_{U_i}) = p^{p^r q d_i - S_i}[p^{S_i}];\\
i \in \mathcal{M}^r_{1,4}(\mathbb{T}, U) &\Rightarrow \Sigma((\mathbb{T}_i)_{U_i}) = p^{p^r q d_i - S_i}[p^{S_i}];\\
i \in \mathcal{M}^r_{1,5}(\mathbb{T}, U) &\Rightarrow \Sigma((\mathbb{T}_i)_{U_i}) = p^{p^r q d_i - S_i - 1}[p^{S_i+1}].
\end{aligned}$$

We note that, by lemmas 3.3.19, 3.3.20 and 3.3.21, that if $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$ is the $(x^n-1)$-set of an additive cellular automata that there is some $r'$ such that $\mathcal{M}^r_{1,3}(\mathbb{T}_r, U) = \emptyset$ for all integers $r \geq r'$ and that $\mathcal{M}^r_{1,2}(\mathbb{T}_r, U) = \emptyset$ and $\mathcal{M}^r_{1,5}(\mathbb{T}_r, U) = \emptyset$ for all $r \geq r'$ unless there is some $i \in \mathcal{M}^r_{1,2}(\mathbb{T}_r, U)$ $(i \in \mathcal{M}^r_{1,5}(\mathbb{T}_r, U))$ such that $\mathcal{I}_i(\mathbb{T}_{r',i} - 1) = p^l$, $0 < l < r'$.

**Theorem 4.3.1** *For* $\mathbb{T} \in \frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$ *with non-zero fixed points there are at most* $r+2$ *distinct* $\Sigma(\mathbb{T}_U)$ *as* $U$ *runs through* $\frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$ *and the cycle set that occurs is completely determined by the integer* $\eta(U)$, $0 \leq \eta(U) \leq r+1$, *where* $\eta(U) = 0$ *if* $\mathbb{T}_U$ *has a fixed point and*

$$\eta(U) = \max(1, \max_{i\in\mathcal{M}^r_{1,1}(\mathbb{T},U)\cup\mathcal{M}^r_{1,3}(\mathbb{T},U)\cup\mathcal{M}^r_{1,4}(\mathbb{T},U)}(S_i), \max_{i\in\mathcal{M}^r_{1,2}(\mathbb{T},U)\cup\mathcal{M}^r_{1,5}(\mathbb{T},U)}(S_i+1))$$

*otherwise, in the sense that* $\mathbb{T}_U$ *and* $\mathbb{T}_V$ *are* QDS *if and only if* $\eta(U) = \eta(V)$.

Proof:

We claim that $p^{\eta(U)}$ is the minimal orbit length occurring under $\mathbb{T}_U$ and that $p^{\eta(U)}|(\phi_a)_U$ for all $a \in \frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$, this is clear when $\mathbb{T}_U$ has a fixed point. For $\eta(U) > 0$ we note that, with

$$\overline{M}(U) = (\overline{M}^r_1(\mathbb{T}) \setminus (\overline{M}^r_1(\mathbb{T}) \cap M^r_0(U))) \cup M^r_1(\mathbb{T}, U),$$

one has

$$\Sigma(\mathbb{T}_U) = (p^{p^r q(\sum_{\overline{M}(U)} d_i) - \eta(U)}[p^{\eta(U)}]) \prod_{M\setminus\overline{M}(U)} \Sigma((\mathbb{T}_i)_{U_i}). \tag{4.3.3}$$

Using the definition of the cycle product it is clear that $p^{\eta(U)}$ will divide each of the orbit lengths that occur in $\Sigma(\mathbb{T}_U)$ and is the minimum orbit length occurring under

$\mathbb{T}_U$, hence by theorem 2.3.3 we have that $\mathbb{T}_U$ and $\mathbb{T}_V$ are QDS if and only if $\eta(U) = \eta(V)$ (irrespective of whether or not $\overline{M}(U) = \overline{M}(V)$ !). As $\eta(U)$ takes values in $\{0, 1, \ldots, r+1\}$ we see that there are at most $r+2$ qualitatively distinct behaviours available to $\mathbb{T}_U$. ■

The proof of theorem 4.3.1 gives an expression for $\Sigma(\mathbb{T}_U)$, for using (4.3.3) one has

$$\Sigma(\mathbb{T}_U) = (p^{p^r q(\sum_{\overline{M}(U)} d_i) - \eta(U)}[p^{\eta(U)}]) \prod_{M \setminus \overline{M}(U)} \Sigma((\mathbb{T}_i)), \tag{4.3.4}$$

for $\Sigma((\mathbb{T}_i)_{U_i}) = \Sigma(\mathbb{T}_i)$ when $i \in M \setminus \overline{M}(U)$. One can prove theorem 4.3.1 without using theorem 2.3.3, by examining the cycle product as $\overline{M}(U)$ changes with $U$, however it is far easier to use theorem 2.3.3. Theorem 4.3.1 gives a necessary and sufficient condition for QDS via theorem 2.3.3 by showing that cellular automata over finite fields satisfy the conditions of theorem 2.3.3 and giving an explicit formula for the minimum orbit length under $\mathbb{T}_U$ for any $U \in \frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$.

One should note that every orbit length occurring under $\mathbb{T}_U$ divides the maximum orbit length occurring under $\mathbb{T}_U$.

**Lemma 4.3.3** *For any* $U \in \frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$ *one has*

$$\Pi_{np^r}(\mathbb{T}_U) = \Pi_{np^r}(\mathbb{T}) \quad or \quad p\Pi_{np^r}(\mathbb{T}).$$

Proof:

By lemma 4.2.8 and its proof we have, with $\theta_r^i(\mathbb{T}) = \mathbb{T}_i$,

$$\Pi_{np^r}(\mathbb{T}) = p^S \mathrm{lcm}_{i \in M \setminus M_0^r(\mathbb{T})}(L(\mathbb{T}_i)),$$

where $S = \max_{i \in M \setminus M_0^r(\mathbb{T})}(S_i)$. Now

$$\Pi_{np^r}(\mathbb{T}_U) = \mathrm{lcm}(\Pi_{np^r}((\mathbb{T}_i)_{U_i}))$$

and $\Pi_{np^r}((\mathbb{T}_i)_{U_i}) = \Pi_{np^r}(\mathbb{T}_i)$ unless $L_i = 1$ and $i \in \overline{M}_1^r(\mathbb{T}) \cup \mathcal{M}_{1,2}^r(\mathbb{T}, U) \cup \mathcal{M}_{1,5}^r(\mathbb{T}, U)$, in which case

$$\Pi_{np^r}((\mathbb{T}_i)_{U_i}) = p^{S_i+1} = p\Pi_{np^r}(\mathbb{T}_i).$$

Now either $S_i + 1 \leq S$ for all such $i$ or $S_i + 1 = S + 1$ for one or more such $i$, in the first case clearly $\Pi_{np^r}(\mathbb{T}_U) = \Pi_{np^r}(\mathbb{T})$ and in the second case $\Pi_{np^r}(\mathbb{T}_U) = p\Pi_{np^r}(\mathbb{T})$. ■

By theorem 2.1.1, when $U = 0$ and $N > 1$ a cycle of length $p^{qN} - 1$ cannot occur under any additive cellular automata rule over $\mathbb{F}_{p^q}$. For non-zero input $U$, if $\mathbb{T}$ and $\mathbb{T}_U$ are not QDS then by theorem 4.3.1 $p$ divides all orbit lengths occurring under $\mathbb{T}_U$, hence orbits of length $p^{qN} - 1$ cannot occur, however one might suppose that there could be an orbit of length $p^{qN}$ in this case, we show that this cannot happen for $N > 1$.

**Theorem 4.3.2** *Additive cellular automata with state alphabet $\mathbb{F}_{p^q}$ and periodic boundary conditions on $N$ cells, $N > 1$, and with time independent inputs cannot generate orbits of lengths $p^{qN} - 1$ or $p^{qN}$.*

Proof:

By the remarks preceding the theorem $\mathbb{T}_U$, $U \neq 0$, cannot have a cycle of length $p^{qN} - 1$ if $\mathbb{T}$ does not hence additive cellular automata with state alphabet $\mathbb{F}_{p^q}$ and periodic boundary conditions on $N$ cells and with time independent inputs cannot generate orbits of lengths $p^{qN} - 1$. For an orbit of length $p^{qN}$ consider $(\phi_0)_U$ when $\mathbb{T}_U$ is not QDS to $\mathbb{T}$,

$$(\phi_0)_U | p\Pi_{np^r}(\mathbb{T}) = p \operatorname{lcm}_{i \in M}(p^{S_i} L_i)$$

by lemma 2.1.13, where $0 \leq S_i \leq r$ and $L_i | p^{qd_i} - 1$ for each $i \in M$. If $L_i = 1$ for all $i \in M$ then $\phi | p^{r+1} < p^{qnp^r}$ for $N > 1$ (and for $N = 1$ when $p > 2$). If $L_j > 1$ for some $j \in M$ then $p \nmid L_j$ and $L_j \nmid p^I$ for any $I \in \mathbb{N}$, hence $p \nmid \operatorname{lcm}_{i \in M}(L_i)$ and $\operatorname{lcm}_{i \in M}(L_i) \nmid p^I$ for any $I \in \mathbb{N}$ and so $(\phi_0)_U$ cannot equal $p^{qp^r n}$. ■

Note that when $q = 1$ cycles of length $p^n - p$ are possible for $n > 1$ with $n$ and $p$ coprime if $m = 2$ for then

$$\frac{\mathbb{F}_p[x]}{(x^n - 1)\mathbb{F}_p[x]} \cong \frac{\mathbb{F}_p[x]}{(x - 1)\mathbb{F}_p[x]} \times \frac{\mathbb{F}_p[x]}{R(x)\mathbb{F}_p[x]} \cong \mathbb{F}_p \times \frac{\mathbb{F}_p[x]}{R(x)\mathbb{F}_p[x]}$$

where $\deg R(x) = d = n - 1$ and so if $\mathbb{T}$ is a unit with $\mathbb{T}_1 = 1$ and $U_1 \neq 0$ and if $L(\mathbb{T}_2) = p^d - 1$ and any $U_2$ then

$$\Pi_n(\mathbb{T}_U) = \operatorname{lcm}(p, p^d - 1) = p(p^d - 1) = p^{d+1} - p = p^n - p.$$

## 4.4 Conditions For qualitatively similar dynamics for additive cellular automata over a finite field

In this section we begin to answer the question : under what conditions do two distinct additive cellular automata give qualitatively similar behaviour on $N$ cells? We must

first define what we mean by qualitatively similar behaviour.

**Definition 4.4.1** *Let* $\mathbb{T}$ *and* $\mathbb{T}'$ *be in* $\frac{\mathbb{F}_{pq}[x]}{(x^N-1)\mathbb{F}_{pq}[x]}$, $N > 0$, *then*

(i) $\mathbb{T}$ *and* $\mathbb{T}'$ *are eventually qualitatively dynamically similar* (*eventually* QDS) *if* $\Sigma(\mathbb{T}) = \Sigma(\mathbb{T}')$;

(ii) $\mathbb{T}$ *and* $\mathbb{T}'$ *are transiently qualitatively dynamically similar* (*transiently* QDS) *if the tree rooted at zero in the state transition graph of* $\mathbb{T}$ *is identical* (*as a graph*) *to the tree rooted at zero in the state transition graph of* $\mathbb{T}'$;

(iii) $\mathbb{T}$ *and* $\mathbb{T}'$ *are qualitatively dynamically similar* (QDS) *if* $\mathbb{T}$ *and* $\mathbb{T}'$ *are eventually* QDS *and transiently* QDS.

With the above definition we can define qualitative dynamical similarity on $N$ cells for cellular automata rules.

**Definition 4.4.2** *If* $f$ *and* $g$ *are the local rules of additive cellular automata over* $\mathbb{F}_{pq}$ *with representatives* $\mathbb{T}$ *and* $\mathbb{T}'$ *respectively on* $N$ *cells then we shall say that* $f$ *and* $g$ *are qualitatively dynamically similar* (QDS) (*eventually* QDS, *transiently* QDS) *on* $N$ *cells if* $\mathbb{T}$ *and* $\mathbb{T}'$ *are* QDS (*eventually* QDS, *transiently* QDS).

**Definition 4.4.3** *Let* $\mathbb{T}$ *and* $\mathbb{T}'$ *be in* $\frac{\mathbb{F}_{pq}[x]}{(x^N-1)\mathbb{F}_{pq}[x]}$, $N > 0$, *then* $\mathbb{T}$ *and* $\mathbb{T}'$ *are strongly* QDS (*strongly eventually* QDS, *strongly transiently* QDS) *if* $\mathbb{T}$ *and* $\mathbb{T}'$ *are* QDS (*eventually* QDS, *transiently* QDS) *and* $Att(\mathbb{T}) = Att(\mathbb{T}')$. *We say that cellular automata rules represented by* $\mathbb{T}$ *and* $\mathbb{T}'$ *are strongly* QDS (*strongly eventually* QDS, *strongly transiently* QDS) *if* $\mathbb{T}$ *and* $\mathbb{T}'$ *are strongly* QDS (*strongly eventually* QDS, *strongly transiently* QDS).

It is clear from lemma 4.2.8, (ii) that $\mathbb{T}$ and $\mathbb{T}'$ are strongly eventually QDS (Strongly transiently QDS) if and only if $\mathbb{T}$ and $\mathbb{T}'$ are eventually QDS (transiently QDS) and $M_0^r(\mathbb{T}) = M_0^r(\mathbb{T}')$.

The above definitions can be extented to include time independent inputs:

**Definition 4.4.4** *Let* $\mathbb{T}$ *and* $\mathbb{T}'$ *be in* $\frac{\mathbb{F}_{pq}[x]}{(x^N-1)\mathbb{F}_{pq}[x]}$, $N > 0$, *then* $\mathbb{T}$ *and* $\mathbb{T}'$ *are affinely eventually* QDS (*affinely strongly eventually* QDS) *if* $\mathbb{T}$ *and* $\mathbb{T}'$ *are affinely eventually* QDS (*affinely strongly eventually* QDS) *and there is a bijection* $\omega : \frac{\mathbb{F}_{pq}[x]}{(x^N-1)\mathbb{F}_{pq}[x]} \longrightarrow$

$\frac{\mathbb{F}_{pq}[x]}{(x^N-1)\mathbb{F}_{pq}[x]}$ *such that for all* $U \in \frac{\mathbb{F}_{pq}[x]}{(x^N-1)\mathbb{F}_{pq}[x]}$,

$$\Sigma(\mathbb{T}_U) = \Sigma(\mathbb{T}'_{\omega(U)}).$$

*We say that cellular automata rules represented by* $\mathbb{T}$ *and* $\mathbb{T}'$ *are affinely eventually* QDS (*affinely strongly eventually* QDS) *if* $\mathbb{T}$ *and* $\mathbb{T}'$ *are.*

**Lemma 4.4.1** *Let* $\mathbb{T}$ *and* $\mathbb{T}'$ *be in* $\frac{\mathbb{F}_{pq}[x]}{(x^N-1)\mathbb{F}_{pq}[x]}$, $N > 0$, *then if* $\mathbb{T}$ *and* $\mathbb{T}'$ *are not eventually* QDS *then* $\mathbb{T}$ *and* $\mathbb{T}'$ *are not affinely eventually* QDS.

Proof:

We show that there is no bijection $\omega$ such that $\Sigma(\mathbb{T}) = \Sigma(\mathbb{T}'_{\omega(0)})$, for let $\omega : \frac{\mathbb{F}_{pq}[x]}{(x^N-1)\mathbb{F}_{pq}[x]} \longrightarrow \frac{\mathbb{F}_{pq}[x]}{(x^N-1)\mathbb{F}_{pq}[x]}$, then one either has

$$\Sigma(\mathbb{T}'_{\omega(0)}) = \Sigma(\mathbb{T}') \neq \Sigma(\mathbb{T})$$

or $\mathbb{T}'_{\omega(0)}$ has no fixed points and so $\Sigma(\mathbb{T}'_{\omega(0)}) \neq \Sigma(\mathbb{T})$. ■

In definition 4.4.4 we have ignored transient structure, this is because, by theorem 2.2.1 the tree structures under $\mathbb{T}$ and $\mathbb{T}_U$ are always identical as graphs and hence the tree structures of $\mathbb{T}_U$ and $\mathbb{T}'_W$, any $U, W$, are the same if and only if $\mathbb{T}$ and $\mathbb{T}'$ are transiently QDS. Thus we make the following definition:

**Definition 4.4.5** *Let* $\mathbb{T}$ *and* $\mathbb{T}'$ *be in* $\frac{\mathbb{F}_{pq}[x]}{(x^N-1)\mathbb{F}_{pq}[x]}$, $N > 0$, *then* $\mathbb{T}$ *and* $\mathbb{T}'$ *are affinely* QDS(*affinely strongly* QDS) *if* $\mathbb{T}$ *and* $\mathbb{T}'$ *are affinely eventually* QDS (*affinely strongly eventually* QDS) *and* $\mathbb{T}$ *and* $\mathbb{T}'$ *are transiently* QDS. *We say that cellular automata rules represented by* $\mathbb{T}$ *and* $\mathbb{T}'$ *are affinely* QDS (*affinely strongly* QDS) *if* $\mathbb{T}$ *and* $\mathbb{T}'$ *are.*

We can characterise the qualitative behaviour of any additive cellular automata on $np^r$ cells in the way described in the following theorem, which is a summary of remarks made earlier in this chapter.

**Theorem 4.4.1** *Let* $\mathbb{T} \in \frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]}$, *then it's qualitative transient behaviour depends only on* $M_0^r(\mathbb{T})$ *and the* $|M_0^r(\mathbb{T})|$ *positive integers* $\mathcal{I}_i(\mathbb{T}_i)$, $i \in M_0^r(\mathbb{T})$ *and it's qualitative periodic behaviour depends only upon the* $|M \setminus M_0^r(\mathbb{T})|$ *pairs of positive integers* $(L_i(\mathbb{T}_i), \mathcal{I}_i(\mathbb{T}_i^{L(\mathbb{T}_i)} - 1))$, $i \in M \setminus M_0^r(\mathbb{T})$. *For non-zero* $U \in \frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]}$ *the difference in the qualitative periodic behaviour of* $\mathbb{T}_U$ *from that of* $\mathbb{T}$ *depends only on the* $|M_1^r(\mathbb{T})|$ *pairs of positive integers* $(\mathcal{I}_i(\mathbb{T}_i - 1), \mathcal{I}_i(U_i))$, $i \in M_1^r(\mathbb{T})$.

Proof:

This follows directly from remarks 4.2.1, 4.2.2 and 4.3.1. ■

**Corollary 4.4.1** *If* $\mathbb{T}, \mathbb{T}' \in \frac{\mathbb{F}_{p^q}[x]}{(x^N-1)\mathbb{F}_{p^q}[x]}$ *are such that* $M_0^r(\mathbb{T}) = M_0^r(\mathbb{T}')$ *and* $\mathcal{I}_i(\mathbb{T}_i)$ $= \mathcal{I}_i(\mathbb{T}_i')$ *for* $i \in M_0^r(\mathbb{T})$ *and* $(L(\mathbb{T}_i), \mathcal{I}_i(\mathbb{T}_i^{L(\mathbb{T}_i)} - 1)) = (L(\mathbb{T}_i'), \mathcal{I}_i(\mathbb{T}_i'^{L(\mathbb{T}_i')} - 1))$ *for* $i \in M \setminus M_0^r(\mathbb{T})$ *then* $\mathbb{T}$ *and* $\mathbb{T}'$ *are affinely strongly* QDS.

Proof:

That $\mathbb{T}$ and $\mathbb{T}'$ are strongly QDS follows from theorem 4.4.1. That $\mathbb{T}$ and $\mathbb{T}'$ are affinely strongly QDS then follows with $\omega = Id$. ■

**Theorem 4.4.2** *Suppose that* $f$ *and* $g$ *are the local rules of additive cellular automata, both non-trivial and that on* $np^r$ *cells for some integer* $r > 0$ *and where* $n$ *and* $p$ *are coprime,* $f$ *and* $g$ *have the same representative* $\mathbb{T} \in \frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$, *then*

(i) *If* $\mathbb{T}_i^{L(\mathbb{T}_i)} - 1 \neq 0$ *for all* $i \in M \setminus M_0^r(\mathbb{T})$ *then* $f$ *and* $g$ *are affinely strongly eventually* QDS *on* $np^s$ *cells for all* $s \in \mathbb{N}$.

(ii) *If* $\mathbb{T}_j \neq 0$ *for all* $i \in M_0^r(\mathbb{T})$ *then* $f$ *and* $g$ *are strongly transiently* QDS *on* $np^s$ *cells for all* $s \in \mathbb{N}$.

(iii) *If the conditions of* (i) *and* (ii) *hold then* $f$ *and* $g$ *are affinely strongly* QDS *on* $np^s$ *cells for all* $s \in \mathbb{N}$.

Proof:

As $f$ and $g$ are both represented by $\mathbb{T}$ on $np^r$ cells it follows from lemma 4.2.2 that $f$ and $g$ have the same representative on $np^s$ cells, $0 \leq s \leq r$ and so (i),(ii) and (iii) hold trivially for $0 \leq s \leq r$. We prove (i), (ii) is very similar and (iii) follows from (i) and (ii). Let $\{\mathbb{T}_s\}_{s\in\mathbb{N}}$ be the $(x^n-1)$-set of $f$ and let $\{\hat{\mathbb{T}}_s\}_{s\in\mathbb{N}}$ be the $(x^n-1)$-set of $g$, so $\mathbb{T} = \mathbb{T}_r = \hat{\mathbb{T}}_r$. As $\mathbb{T}_{r,i}^{L(\mathbb{T}_{r,i})} - 1 \neq 0$ for any $i \in M \setminus M_0^r(\mathbb{T})$ we have, by lemma 3.3.11, that $L(\mathbb{T}_{s,i}) = L(\hat{\mathbb{T}}_{s,i}) = L_i$ for all integers $s \geq r$ and $\mathcal{I}_i(\mathbb{T}_{s,i}^{L_i} - 1) = \mathcal{I}_i(\hat{\mathbb{T}}_{s,i}^{L_i} - 1)$ for all integers $s \geq r$. It follows from corollary 4.4.1 that $\mathbb{T}_s$ and $\hat{\mathbb{T}}_s$ are affinely strongly eventually QDS for all $s \geq r$ and hence for all $s \in \mathbb{N}$. ■

Results in the vein of theorem 4.4.2 are interesting as they raise the possibility of replacing rules with large radius $l$ and most of the rule coefficients non-zero with rules of small radius $k$ and/or most of the rule coefficients zero.

**Example 4.4.1**

With $p = 2, q = 1$ the local rules

$$\begin{aligned} f_1 : a_i &\mapsto a_{i-1} + a_{i+1} \\ f_2 : a_i &\mapsto a_{i-1} + a_{i-5} \\ f_3 : a_i &\mapsto a_{i-5} + a_{i+5} \\ f_4 : a_i &\mapsto a_{i-9} + a_{i-6} + a_{i-5} + a_{i-1} + a_i + a_{i+3} + a_{i+7} + a_{i+13} \end{aligned}$$

(and infinitely many more) all have the same representative

$$\mathbb{T} = x + x^5 + (x^6 - 1)\mathbb{F}_2[x]$$

on 6 cells. One finds

$$\Theta(\mathbb{T}) = (0 + (x^2 + 1)\mathbb{F}_2[x], x^3 + (x^4 + x^2 + 1)\mathbb{F}_2[x]) = (0, \mathbb{T}_2)$$

and that $L(\mathbb{T}_2) = 1, \mathcal{I}_2(\mathbb{T}_2 - 1) = 1$. Thus by theorem 4.4.2 the local rules $f_1, f_2, f_3, f_4$ *etc.* are all affinely strongly eventually QDS on $3.2^s$ cells, $s \in \mathbb{N}$. ♦

**Theorem 4.4.3** *Let $f$ and $g$ be the local rules of non-trivial additive cellular automata such that on $np^r$ cells, some $r \in \mathbb{N}$, $f$ is represented by $\mathbb{T}_f \in \frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$ and $g$ is represented by $\mathbb{T}_g \in \frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$ where $M_0^r(\mathbb{T}_f) = M_0^r(\mathbb{T}_g) = M_0^r$ then :*

(i) *If for each $i \in M \setminus M_0^r$ one has $L((\mathbb{T}_f)_i) = L((\mathbb{T}_g)_i) = L_i$ and $p^r > \mathcal{I}_i((\mathbb{T}_f)_i^{L_i} - 1)$ $= \mathcal{I}_i((\mathbb{T}_g)_i^{L_i} - 1) > 0$ then $f$ and $g$ are affinely strongly eventually* QDS *on $np^{r+s}$ cells for all $s \in \mathbb{N}$.*

(ii) *If for each $i \in M_0^r$ one has $\mathcal{I}_i((\mathbb{T}_f)_i) = \mathcal{I}_i((\mathbb{T}_g)_i)$ then $f$ and $g$ are strongly transiently* QDS *on $np^{r+s}$ cells for all $s \in \mathbb{N}$.*

(iii) *If the conditions of* (i) *and* (ii) *hold then $f$ and $g$ are affinely strongly* QDS *on $np^{r+s}$ cells for all $s \in \mathbb{N}$.*

Proof:

This is very similar to the proof of theorem 4.4.2, it follows from lemma 3.3.11 and theorem 4.4.1, with the affine part following with $\omega = Id$. ■

**Example 4.4.2**

With $p = 2, q = 1$ and $N = 6$ the local rules

$$\begin{aligned} f : a_i &\mapsto a_{i-1} + a_{i+4} \\ g : a_i &\mapsto a_{i-3} + a_{i+1} \end{aligned}$$

have representatives

$$\begin{aligned}\mathbb{T}_f &= x + x^2 + (x^6 - 1)\mathbb{F}_2[x] \\ \mathbb{T}_g &= x^4 + x^5 + (x^6 - 1)\mathbb{F}_2[x]\end{aligned}$$

with

$$\begin{aligned}\Theta(\mathbb{T}_f) &= ((\mathbb{T}_f)_1, (\mathbb{T}_f)_2) \\ &= (1 + x + (1 + x^2)\mathbb{F}_2[x], x + x^2 + (1 + x^2 + x^4)\mathbb{F}_2[x]) \\ \Theta(\mathbb{T}_g) &= ((\mathbb{T}_g)_1, (\mathbb{T}_g)_2) \\ &= (1 + x + x^2 + x^3 + (1 + x^2)\mathbb{F}_2[x], x + x^2 + (1 + x^2 + x^4)\mathbb{F}_2[x]).\end{aligned}$$

One finds that $\mathcal{I}_1((\mathbb{T}_f)_1) = \mathcal{I}_1((\mathbb{T}_g)_1) = 1$ and $L((\mathbb{T}_f)_2) = L((\mathbb{T}_g)_2) = 1$ and $\mathcal{I}_2((\mathbb{T}_f)_2 - 1) = \mathcal{I}_2((\mathbb{T}_g)_2 - 1) = 1$, hence $f$ and $g$ are affinely strongly QDS on $3.2^i$ cells for all integers $i \geq 1$. ♦

In light of theorem 4.4.3 it is natural to ask how many elements $\mathbb{T}$ of $\frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$ share the same values of $L(\mathbb{T}_i)$ and $\mathcal{I}_i(\mathbb{T}_i^{L(\mathbb{T}_i)} - 1)$ for $i \in M \setminus M_0^r(\mathbb{T})$. The proof of the following result can be found in appendix B.

**Lemma 4.4.2** *For any subset $M_0^r \subseteq M$ there are*

$$\prod_{i \in M \setminus M_0^r} \phi(L_i)|\mathcal{D}_R(p^r d_i - 1, I_i)| \prod_{j \in M_0^r} |\mathcal{D}_R(p^r d_i - 1, I_j)|$$

*elements $\mathbb{T}$ of $\frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$ sharing the same values $L_i = L(\mathbb{T}_i)$ and $I_i = \mathcal{I}_i(\mathbb{T}_i^{L_i} - 1)$ for each $i \in M \setminus M_0^r$ and $I_j = \mathcal{I}_j(\mathbb{T}_j)$ for each $j \in M_0^r$, where $\phi$ is Eulers function and $L_i | p^{qd_i} - 1$, each $i \in M \setminus M_0^r$.* ■

Let the distinct degrees of the irreducible factors $R_i(x)$, $1 \leq i \leq m$, of $x^n - 1$ over $\mathbb{F}_{p^q}$ be $d_1, \ldots, d_s$ where $s \leq m$ and $d_i < d_j$ if $i < j$. Let $M_i$, $1 \leq i \leq s$, be the set $\{j \in M : deg R_j(x) = d_i\}$, so $j_i, j_2 \in M_i$ implies that

$$\frac{\mathbb{F}_{p^q}[x]}{R_{j_1}(x)\mathbb{F}_{p^q}[x]} \cong \frac{\mathbb{F}_{p^q}[x]}{R_{j_2}(x)\mathbb{F}_{p^q}[x]}.$$

We can partition $M$ as $M = \bigcup_{i=1}^{s} M_i$ and write the direct product decomposition of $\frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]}$ accordingly,

$$\frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]} \cong \prod_{i=1}^{s} \prod_{j \in M_i} \frac{\mathbb{F}_{pq}[x]}{R_j(x)^{p^r}\mathbb{F}_{pq}[x]}.$$

For any $\mathbb{T} \in \frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]}$ we can partition $M_0^r(\mathbb{T})$ and $M \setminus M_0^r(\mathbb{T})$ in the same manner, so

$$M = \bigcup_{i=1}^{s} (M_i \setminus M_{0,i}^r(\mathbb{T}) \cup M_{0,i}^r(\mathbb{T})).$$

Formally define $L(\mathbb{T}_j) = 0$ if $\mathbb{T}_j$ is nilpotent, then define

$$\varphi(\mathbb{T}_j) = \begin{cases} \mathcal{I}_j(\mathbb{T}_j) & \text{if} \quad L(\mathbb{T}_j) = 0; \\ \mathcal{I}_j(\mathbb{T}_j^{L(\mathbb{T}_j)} - 1) & \text{if} \quad L(\mathbb{T}_j) \neq 0. \end{cases}$$

Now define

$$\Upsilon_{\mathbb{T},i}(\mathbb{T}) = \times_{j \in M_i \setminus M_{0,i}^r(\mathbb{T})}(L(\mathbb{T}_j), \varphi(\mathbb{T}_j)) \times_{j \in M_{0,i}^r(\mathbb{T})} (L(\mathbb{T}_j), \varphi(\mathbb{T}_j))$$

for $1 \leq i \leq s$ and define

$$\Upsilon_{\mathbb{T}}(\mathbb{T}) = \times_{i=1}^{s} \Upsilon_{\mathbb{T},i}(\mathbb{T}).$$

Let $\hat{\mathbb{T}}$ be another element of $\frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]}$ and let

$$\Upsilon_{\mathbb{T},i}(\hat{\mathbb{T}}) = \times_{j \in M_i \setminus M_{0,i}^r(\mathbb{T})}(L(\hat{\mathbb{T}}_j), \varphi(\hat{\mathbb{T}}_j)) \times_{j \in M_{0,i}^r(\mathbb{T})} (L(\hat{\mathbb{T}}_j), \varphi(\hat{\mathbb{T}}_j))$$

for $1 \leq i \leq s$ and

$$\Upsilon_{\mathbb{T}}(\hat{\mathbb{T}}) = \times_{i=1}^{s} \Upsilon_{\mathbb{T},i}(\hat{\mathbb{T}}).$$

By theorem 4.4.1, $\Upsilon_{\mathbb{T}}(\mathbb{T})$ determines the qualitative behaviour of $\mathbb{T}$ and it follows that if $\Upsilon_{\mathbb{T},i}(\hat{\mathbb{T}})$ is a permutation of $\Upsilon_{\mathbb{T},i}(\mathbb{T})$ for each $i$, $1 \leq i \leq s$, then $\Sigma(\mathbb{T}) = \Sigma(\hat{\mathbb{T}})$ and $\mathbb{T}$ and $\hat{\mathbb{T}}$ are affinely QDS. At this stage the question of whether $\mathbb{T}$ and $\hat{\mathbb{T}}$ can be eventually QDS when $\Upsilon_{\mathbb{T},i}(\hat{\mathbb{T}})$ is not a permutation of $\Upsilon_{\mathbb{T},i}(\mathbb{T})$ for some $i$ arises. We noted in chapter 1 that the set of cycle sets forms a ring $C(\mathbb{Z})$, thus the question asked above can be viewed as a question about factorisation in $C(\mathbb{Z})$. However, the factorisation properties of $C(\mathbb{Z})$ are not obvious and we feel that an investigation of these properties is beyond the scope of this thesis.

## 4.5 Description in terms of idempotent elements

In this section we rewrite the direct product decomposition of $\frac{\mathbb{F}_{p^q}[x]}{(x^N-1)\mathbb{F}_{p^q}[x]}$ in terms of idempotents. This will be used for $q = 1$ in chapter 5, it also provides an alternative approach to reconstruction. Recall that, for $\gcd(p, n) = 1$,

$$\frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]} \cong \prod_{i=1}^{m} \frac{\mathbb{F}_{p^q}[x]}{R_i(x)^{p^r}\mathbb{F}_{p^q}[x]}.$$

From theorem A.5.3 we know that

$$\frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]} \cong \prod_{i=1}^{m} e_i \frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$$

for some pairwise orthogonal idempotents $e_i$, our task is to determine the $e_i$.

**Lemma 4.5.1** *For $1 \leq i \leq m$ let $S_i = R_i(x)^{p^r} + (x^{np^r}-1)\mathbb{F}_{p^q}[x]$ and let $\hat{S}_i = \prod_{j\neq i} R_j(x)^{p^r} + (x^{np^r}-1)\mathbb{F}_{p^q}[x]$, then $e_i = \hat{S}_i^{(\phi_{\hat{S}_i})_0}$ is idempotent and the $e_i$ are pairwise orthogonal,* where $(\phi_{\hat{S}_i})_0 = \prod_{np^r}(\hat{S}_i)$.

Proof:

With $\hat{S}_i$ as defined and with $k = (\phi_{\hat{S}_i})_0$ there is some $T_i > 0$ such that $\hat{S}_i^{k+T_i} = \hat{S}_i^{T_i}$ ($T_i > 0$ as $\hat{S}_i S_i = 0$ so $\hat{S}_i$ is not a unit). Then

$$e_i^2 = \hat{S}_i^{2k} = \hat{S}_i^{k+T_i+k-T_i} = \hat{S}_i^{k+T_i-T_i} = \hat{S}_i^k = e_i,$$

hence $e_i$ is idempotent. For $j \neq i$, with $k_i = (\phi_{\hat{S}_i})_0$ and $k_j = (\phi_{\hat{S}_j})_0$ we have

$$e_i e_j = \hat{S}_i^{k_i}\hat{S}_j^{k_j} = \hat{S}_i\hat{S}_j\hat{S}_i^{k_i-1}\hat{S}_j^{k_j-1} = \hat{S}_i S_i(\prod_{l\neq i,j} R_l^{p^r})\hat{S}_i^{k_i-1}\hat{S}_j^{k_j-1} = 0$$

and hence the $e_i$, $1 \leq i \leq m$, are pairwise orthogonal. ■

**Lemma 4.5.2** *With $e_i$ as described in lemma 4.5.1, $1 \leq i \leq m$,*

$$e_i \frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]} \cong \frac{\mathbb{F}_{p^q}[x]}{R_i(x)^{p^r}\mathbb{F}_{p^q}[x]}.$$

Proof:

Define a map $E_i : \frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]} \longrightarrow e_i\frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]}$ by

$$a(x) + (x^{np^r} - 1)\mathbb{F}_{pq}[x] \mapsto (a(x) + (x^{np^r} - 1)\mathbb{F}_{pq}[x])e_i.$$

Clearly $E_i$ is well defined and $E_i(0) = 0$ and $E_i(1) = e_i$ and

$$\begin{aligned}
E_i(a+b) &= (a(x) + b(x) + (x^{np^r} - 1)\mathbb{F}_{pq}[x])e_i \\
&= (a(x) + (x^{np^r} - 1)\mathbb{F}_{pq}[x])e_i + (b(x) + (x^{np^r} - 1)\mathbb{F}_{pq}[x])e_i \\
&= E_i(a) + E_i(b); \\
E_i(ab) &= (a(x)b(x) + (x^{np^r} - 1)\mathbb{F}_{pq}[x])e_i \\
&= (a(x) + (x^{np^r} - 1)\mathbb{F}_{pq}[x])(b(x) + (x^{np^r} - 1)\mathbb{F}_{pq}[x])e_i \\
&= (a(x) + (x^{np^r} - 1)\mathbb{F}_{pq}[x])e_i(b(x) + (x^{np^r} - 1)\mathbb{F}_{pq}[x])e_i \\
&= E_i(a)E_i(b),
\end{aligned}$$

hence $E_i$ is a homomorphism. Hence we have a homomorphism $E_i \circ \pi_{np^r} : \mathbb{F}_{pq}[x] \longrightarrow e_i\frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]}$, $a(x) \mapsto e_i(x)a(x) + (x^{np^r} - 1)\mathbb{F}_{pq}[x]$. Examining the kernel of this homomorphism we see that, for $a \neq 0$, $e_i a = 0$ if and only $R_i(x)^{p^r} | a(x)$ so

$$\text{Ker } E_i \circ \pi_{np^r} = R_i(x)^{p^r}\mathbb{F}_{pq}[x]$$

then with $\pi_{R_i,r}$ denoting the natural projection $\pi_{R_i,r} : \mathbb{F}_{pq}[x] \longrightarrow \frac{\mathbb{F}_{pq}[x]}{R_i(x)^{p^r}\mathbb{F}_{pq}[x]}$ we employ the factor theorem to see that there is a ring monomorphism

$$\epsilon_i : \frac{\mathbb{F}_{pq}[x]}{R_i(x)^{p^r}\mathbb{F}_{pq}[x]} \longrightarrow e_i\frac{\mathbb{F}_{pq}[x]}{(x^{np^r} - 1)\mathbb{F}_{pq}[x]},$$

$\epsilon_i \circ \pi_{R_i,r} = E_i \circ \pi_{np^r}$, see figure 4.2. Further for any $a \in e_i\frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]}$, $a = e_i a$ so $a(x) + R_i(x)^{p^r}\mathbb{F}_{pq}[x]$ is a preimage of $a$ hence $\epsilon_i$ is surjective and hence a isomorphism, with $\epsilon_i^{-1}$ given by $a \mapsto a(x) + R_i(x)^{p^r}\mathbb{F}_{pq}[x]$. ■

It follows from lemma 4.5.2 that

$$\frac{\mathbb{F}_{pq}[x]}{(x^{np^r} - 1)\mathbb{F}_{pq}[x]} \cong \prod_{i=1}^{m} e_i\frac{\mathbb{F}_{pq}[x]}{(x^{np^r} - 1)\mathbb{F}_{pq}[x]} \tag{4.5.1}$$

where the $e_i$ are as described in lemma 4.5.1. Let $a = (a_1, \ldots, a_m)$ be an element of the right hand side of (4.5.1), then it corresponds to the element

$$\overline{a} = a_1e_1 + \ldots + a_me_m$$

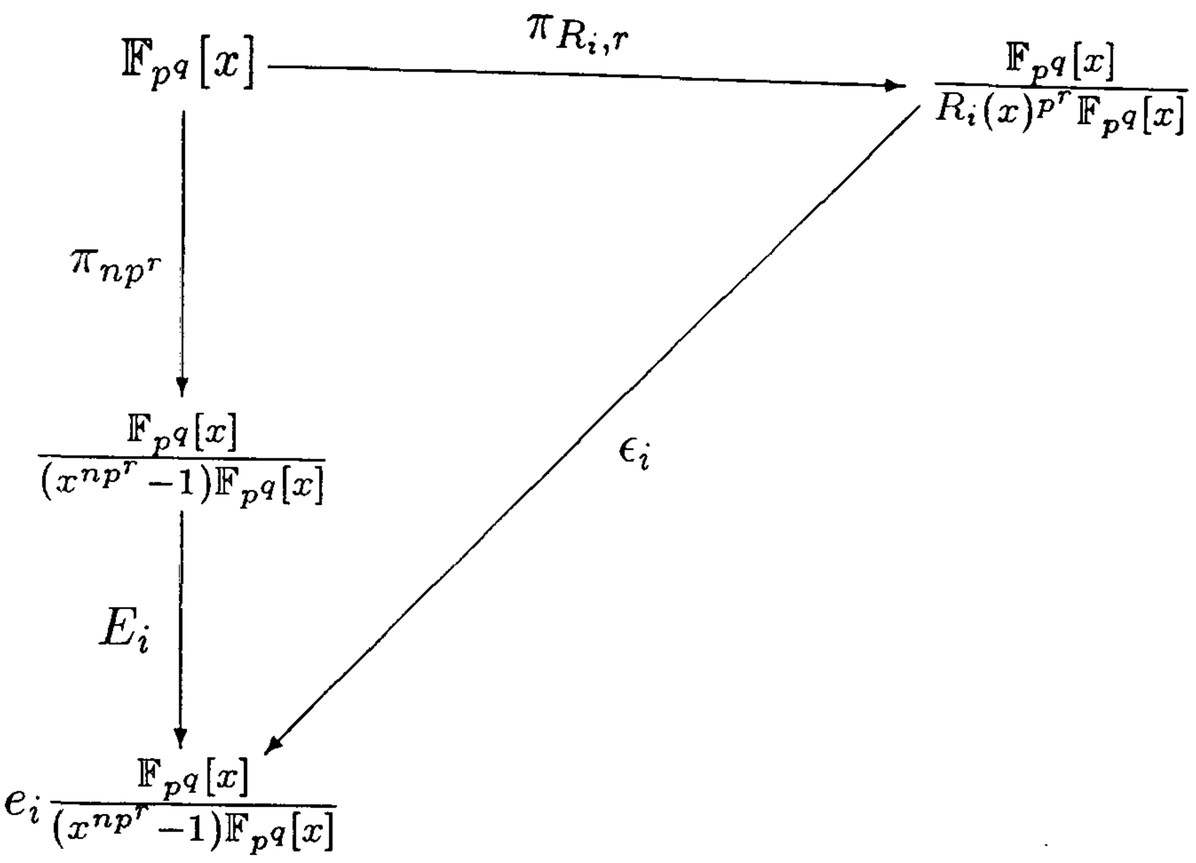


Figure 4.2: $\epsilon_i$ is an isomorphism.

of $\frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]}$, in particular

$$1 = e_1 + \ldots e_m.$$

Hence if we have been working with $\prod_{i=1}^{m} \frac{\mathbb{F}_{pq}[x]}{R_i(x)^{p^r}\mathbb{F}_{pq}[x]}$ and know the $e_i$, then if $b = (b_1, \ldots, b_m)$ is in $\prod_{i=1}^{m} \frac{\mathbb{F}_{pq}[x]}{R_i(x)^{p^r}\mathbb{F}_{pq}[x]}$ then we can find its unique preimage in $\frac{\mathbb{F}_{pq}[x]}{(x^{np^r}-1)\mathbb{F}_{pq}[x]}$ by

$$(b_1, \ldots, b_m) \mapsto \epsilon_1(b_1) + \ldots + \epsilon_m(b_m).$$

Note that it is easy to calculate the $e_i$, for clearly $\theta_r^j(\hat{S}_i) = 0$ if $j \neq i$, hence to find $(\phi_{\hat{S}_i})_0$ one just finds that value for $\theta_r^i(\hat{S}_i)$. When $r = 0$ this is just $O(\theta_0^i(\hat{S}_i))$. Recall from chapter 3, section 3.3, that for each $r > 1$ we have an isomorphism

$$\Phi : \frac{\mathbb{F}_{pq}[x]}{R_i(x)\mathbb{F}_{pq}[x]} \longrightarrow < 1, x^{p^r}, \ldots, x^{(d_i-1)p^r} >.$$

Where $< 1, x^{p^r}, \ldots, x^{(d_i-1)p^r} >$ is the subring of $\frac{\mathbb{F}_{pq}[x]}{R_i^{p^r}(x)\mathbb{F}_{pq}[x]}$ generated as a $\mathbb{F}_{pq}-$algebra by the elements

$$1 + R_i^{p^r}(x)\mathbb{F}_{pq}[x], \ \ldots, \ x^{p^r(d_i-1)} + R_i^{p^r}(x)\mathbb{F}_{pq}[x].$$

In exactly the same way we have an isomorphism

$$\Phi_n^r \ : \ \frac{\mathbb{F}_{pq}[x]}{(x^n-1)\mathbb{F}_{pq}[x]} \longrightarrow < 1, x^{p^r}, \ldots, x^{(n-1)p^r} >$$

$$a \mapsto a(x)^{p^r} + (x^{np^r} - 1)\mathbb{F}_{pq}[x],$$

for each $r > 0$, where $< 1, x^{p^r}, \ldots, x^{(n-1)p^r} >$ is the subring of $\frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$ generated as an $\mathbb{F}_{p^q}-$algebra by $1+(x^{np^r}-1)\mathbb{F}_{p^q}[x], \ldots, x^{p^r(n-1)}+(x^{np^r}-1)\mathbb{F}_{p^q}[x]$. On $np^r$ cells, any $r \in \mathbb{N}$, put $\hat{S}_i = \hat{S}_i^r$ and $e_i = e_i^r$, we can calculate $\hat{S}_i^r$ from $\hat{S}_i^0$ easily, for

$$\hat{S}_i^r = \prod_{j \neq i} R_j(x)^{p^r} + (x^{np^r}-1)\mathbb{F}_{p^q}[x] = \Phi_n^r(\hat{S}_i^0)$$

and hence, as $\Phi_n^r$ is an isomorphism, we have

**Lemma 4.5.3** *For $1 \leq 1 \leq m$ and all $r \in \mathbb{N}$ we have*

$$e_i^r = \Phi_n^r(e_i^0) = e_i^0(x)^{p^r} + (x^{np^r}-1)\mathbb{F}_{p^q}[x]. \quad \blacksquare$$

# Chapter 5

# Additive cellular automata over the integers modulo $m$ for any positive integer $m > 1$

Despite the title in this chapter we are mainly concerned with the case of state alphabet $R = \mathbb{Z}_{/p^k}$, as (see for instance theorem 1.5.1 and theorem 1.5.3) results from this case together with the finite field case suffice to prove results easily in the general $m$ composite case. As was mentioned in chapter 1 results for the case of state $\mathbb{Z}_{/p^k}$ and periodic boundary conditions were not hitherto available. We consider only periodic behaviour for reasons of space.

We begin in section 5.1 by obtaining a direct product decomposition for $R_N$ when $R = \mathbb{Z}_{/p^k}$ by using the technique of idempotent lifting from the $R = \mathbb{F}_p$ case on $N$ cells. A set of non-trivial pairwise orthogonal idempotent elements for the $\mathbb{Z}_{/p^k}$ case is calculated easily from the non-trivial pairwise orthogonal idempotent elements in the $\mathbb{F}_p$ case, lemma 5.1.2 and theorem 5.1.1 give the details. We show that the factors in the direct product decomposition of $R_N$ in this case are completely primary rings.

In 5.1.1 we establish some relationships between the rings occurring for $N = np^r$, $n$ coprime to $p$, for different values of $r$. In particular we show how the relevant idempotent elements for $r > 0$ can be calculated easily from those for the $r = 0$ case. In 5.1.1 the relationships between the cases for different values of $k$ are considered, this leads to useful techniques for obtaining results for the $\mathbb{Z}_{/p^k}$ case from the $\mathbb{Z}_{/p^{k-1}}$ case.

A canonical representation of the elements of the rings occurring in the direct product decomposition is found, this relates the elements in the $\mathbb{Z}_{/p^k}$ case to elements in the $\mathbb{Z}_{/p^{k-s}}$ cases, $0 < s < k$. An important distinction between the present case and the finite field case is that when the number of cells $N$ is not coprime to $p$ then in each of the rings occurring in the direct product decomposition the maximal ideal consisting of all the nilpotent elements is not principal.

In section 5.2 we examine the relevant dynamics in the individual rings occurring in the direct product decomposition, beginning by relating the maximum orbit length occurring under a unit in one of these rings to the maximum orbit length occurring under the image of the unit in the corresponding ring in the $\mathbb{F}_p$ case. In theorem 5.2.2 we give an explicit formula for the cycle set of a unit in such a ring when the number of cells $N$ is coprime to $p$. In theorem 5.2.3 we describe the orbit lengths that can occur when $N$ is not coprime to $p$, these are strongly related to those occurring in the finite field case. However we are not able to write down a general formula for the cycle set in this case, this is because of the non-principality of the ideal of nilpotent elements. A simple example is given that illustrates some of the difficulties.

In section 5.3 we turn to the case of non-zero inputs, again the results are stronger

when $N$ is coprime to $p$ and for general $N$ we content ourselves with showing that the condition of theorem 2.3.3 is satisfied (in theorem 5.3.2).

In section 5.4 we use the results from earlier in the chapter to obtain results for $R_N$, $R = \mathbb{Z}_{/p^k}$ and hence for linear cellular automata with time independent inputs and state alphabet $\mathbb{Z}_{/p^k}$. The results in this section follow similar lines to those in chapter 4 but are not in general as strong. In particular we show that a linear cellular automata with state alphabet $\mathbb{Z}_{/p^k}$ is reversible on $np^r$ cells, $n$ coprime to $p$ and any $r \in \mathbb{N}$ if and only if it is reversible on $n$ cells and give a formula for the maximal cycle length. The invariant set is described and we show that the condition of theorem 2.3.3 is satisfied.

In section 5.5 we return to the case of state alphabet $\mathbb{Z}_{/m}$, any integer $m > 1$ and prove two important results to illustrate the ease with which results in this case can be obtained from the special cases considered previously. Specifically we show that additive cellular automata with state alphabet $\mathbb{Z}_{/m}$ and periodic boundary conditions on $N$ cells with time independent inputs cannot have cycles of length $m^N$ for $N > 1$ and that for such cellular automata in the presence of time independent inputs the condition of theorem 2.3.3 is satisfied. We briefly discuss a straightforward generalisation and indicate how one might begin the process of obtaining the direct product decomposition of $R_N$, where $R$ is any finite ring, by using results from chapters 3 and 5.

## 5.1 The direct product decomposition

We know from theorem 1.5.3 that for $m$ a positive integer with factorisation into powers of primes $m = \prod_{i=1}^{I} p_i^{k_i}$, that

$$\frac{\mathbb{Z}_{/m}[x]}{(x^N-1)\mathbb{Z}_{/m}[x]} \cong \prod_{i=1}^{I} \frac{\mathbb{Z}_{/p_i^{k_i}}[x]}{(x^N-1)\mathbb{Z}_{/p_i^{k_i}}[x]}.$$

When $k_i = 1$, $\mathbb{Z}_{/p_i} \cong \mathbb{F}_{p_i}$ and thus if $m$ is square free the results of chapters 3 and 4 can be applied to obtain cycle sets *etc.*, for additive cellular automata over $\mathbb{Z}_{/m}$. However if $m$ is not square free, *i.e.* $k_i > 1$ for some $i$, one is confronted with rings of the form $\frac{\mathbb{Z}_{/p_i^{k_i}}[x]}{(x^N-1)\mathbb{Z}_{/p_i^{k_i}}[x]}$, $k_i > 1$, which we do not yet know how to deal with. Thus our major task in this chapter is to develop methods for handling additive cellular automata with state alphabet $\mathbb{Z}_{/p^k}$, $p$ prime and $k > 1$. Unlike $\mathbb{F}_p$, $\mathbb{Z}_{/p^k}$ contains non-zero nilpotent elements, as does $\mathbb{Z}_{/p^k}[x]$, which is neither a unique factorisation domain or a principal

ideal ring. A consequence of this is that in general, if $x^N - 1 = \prod_{i=1}^{m} R_i(x)^{s_i}$ is a factorisation into powers of irreducibles, one has

$$\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]} \ncong \prod_{i=1}^{m} \frac{\mathbb{Z}_{/p^k}[x]}{R_i(x)^{s_i}\mathbb{Z}_{/p^k}[x]}.$$

For instance in $\mathbb{Z}_{/4}[x]$,

$$x^4 - 1 = (x+1)(x+3)(x^2+1) = (x+3)^2(x^2+2x+3)$$

but one finds that $\frac{\mathbb{Z}_{/4}[x]}{(x^4-1)\mathbb{Z}_{/4}[x]}$ is completely primary and hence irreducible.

We make two observations which motivate our approach.

(1) There is a surjective ring homomorphism $\lambda_{k,1} : \mathbb{Z}_{/p^k} \longrightarrow \mathbb{Z}_{/p}$ for each $k \geq 1$, this implies (lemma A.2.3) that there is a ring epimorphism $\Lambda_{k,1} : \frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]} \longrightarrow \frac{\mathbb{F}_p[x]}{(x^N-1)\mathbb{F}_p[x]}$ and hence

$$\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]} \Big/ \text{Ker } \Lambda_{k,1} \cong \frac{\mathbb{F}_p[x]}{(x^N-1)\mathbb{F}_p[x]}.$$

The existence of $\Lambda_{k,1}$ leads one to suppose that one might be able to 'lift' results obtained in the $\mathbb{F}_p$ case to the present case.

(2) We refer to the discussion in appendix A of idempotents, the Pierce decomposition and idempotent lifting. We have obtained the direct product decomposition of $\frac{\mathbb{F}_p[x]}{(x^N-1)\mathbb{F}_p[x]}$ in terms of idempotents in section 4.5, if we can lift the pairwise orthogonal idempotents in $\frac{\mathbb{F}_p[x]}{(x^N-1)\mathbb{F}_p[x]}$ to pairwise orthogonal idempotents in $\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$ we can decompose that ring into a direct product of completely primary rings.

Firstly we look more closely at observation (1), throughout this chapter we shall identify across the isomorphism $\mathbb{Z}_{/p^k} \cong \mathbb{Z}/p^k\mathbb{Z}$. We shall frequently take a polynomial $a(x)$ in $\mathbb{Z}_{/p^{k-s}}[x]$, $k > 1, 0 < s < k$, and then refer to $a(x)$ in $\mathbb{Z}_{/p^k}[x]$, by which we shall mean $a(x)$ embedded in $\mathbb{Z}_{/p^k}[x]$ using the obvious injection $\mathbb{Z}_{/p^{k-s}}[x] \longrightarrow \mathbb{Z}_{/p^k}[x]$.

$$\sum (a_i + p^{k-s}\mathbb{Z})x^i \mapsto \sum (a_i + p^k\mathbb{Z})x^i. \tag{5.1.1}$$

Note that the map given by (5.1.1) is not a ring homomorphism.

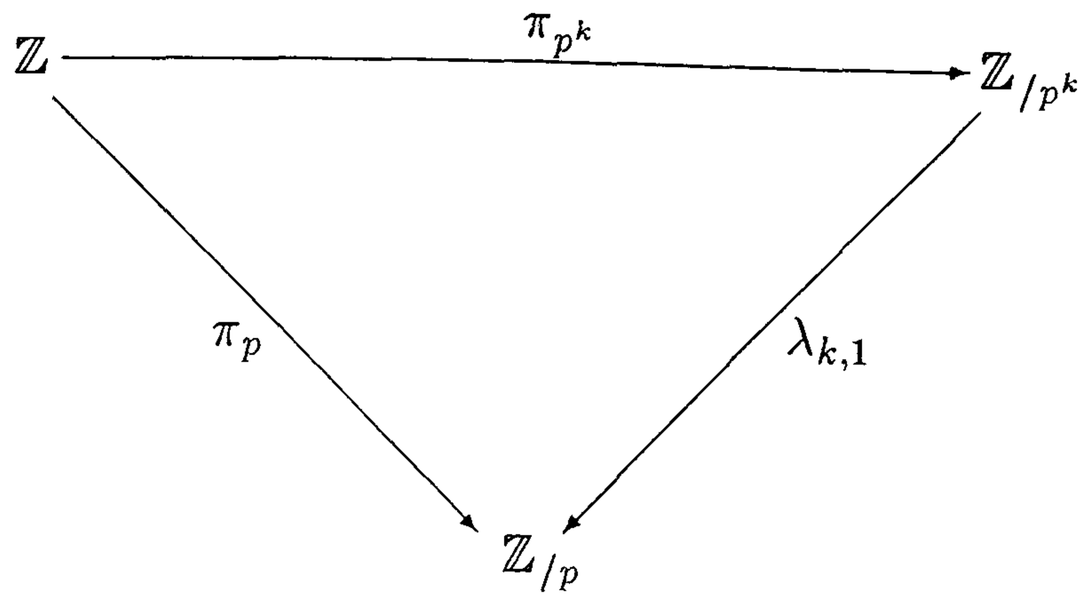


Figure 5.1: $\lambda_{k,1}$ is a ring epimorphism, $\lambda_{k,1} \circ \pi_{p^k} = \pi_p$.

We note that there is a unique ring epimorphism $\lambda_{k,1} : \mathbb{Z}_{/p^k} \longrightarrow \mathbb{Z}_{/p} \cong \mathbb{F}_p$, this follows from the factor theorem A.1.1, $\lambda_{k,1}$ is the unique homomorphism making figure 5.1 commute, where $\pi_p$ and $\pi_{p^k}$ are the natural projections and clearly Ker $\pi_{p^k} = p^k\mathbb{Z} \subset p\mathbb{Z} =$ Ker $\pi_p$. Explicitly $\lambda_{k,1}$ is given by $m + p^k\mathbb{Z} \mapsto m + p\mathbb{Z}$. It follows from lemma A.2.3 that there are ring epimorphisms

$$\lambda'_{k,1} : \mathbb{Z}_{/p^k}[x] \longrightarrow \mathbb{F}_p[x]$$

$$\Lambda_{k,1} : \frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]} \longrightarrow \frac{\mathbb{F}_p[x]}{(x^N-1)\mathbb{F}_p[x]}.$$

Explicitly, if $a(x) = \sum_{i=0}^{n} a_i x^i$, $\lambda'_{k,1}$ and $\Lambda_{k,1}$ are given by

$$\sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} \lambda_{k,1}(a_i)x^i,$$

$$a(x) + (x^N-1)\mathbb{Z}_{/p^k}[x] \mapsto \lambda'_{k,1}(a(x)) + (x^N-1)\mathbb{F}_p[x].$$

Note that Ker $\lambda_{k,1}$ is the maximal ideal of nilpotent elements in $\mathbb{Z}_{/p^k}$, its elements are the elements of the form $mp^s + p^k\mathbb{Z}$, $0 < s < k$ and $\mathbb{Z}_{/p^k}\Big/$ Ker $\lambda_{k,1} \cong \mathbb{F}_p$. For $\lambda'_{k,1}$,

$$\begin{aligned} \text{Ker } \lambda'_{k,1} &= \{a(x) : \lambda_{k,1}(a_i) = 0, 0 \le i \le \deg a\} \\ &= \{a(x) : p | a_i, 0 \le i \le \deg a\}, \end{aligned}$$

and again this is the ideal consisting of all the nilpotent elements of $\mathbb{Z}_{/p^k}[x]$. But for $\Lambda_{k,1}$

$$\begin{aligned} \text{Ker } \Lambda_{k,1} &= \{a(x) + (x^N-1)\mathbb{Z}_{/p^k}[x] : a(x) \in \text{Ker } \lambda'_{k,1}\} \\ &= (p + (x^N-1)\mathbb{Z}_{/p^k}[x])\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]} \end{aligned}$$

which, in general, does not contain every nilpotent element of $\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$.

We will find the following remark useful, its proof is in appendix B.

**Remark 5.1.1** *Let $R$ be a commutative ring with characteristic $p^k$, $k > 1$, and $p$ prime. Let $a$ be any element of $R$ and let $p|n \in R$. Then*

$$(a+n)^{p^{k-1}} = a^{p^{k-1}}. \quad \blacksquare$$

As an example of the usefulness of remark 5.1.1 and the epimorphisms $\lambda_{k,1}, \lambda'_{k,1}$ and $\Lambda_{k,1}$ consider the following lemma, the proof of which is also in appendix B.

**Lemma 5.1.1** *An element $a(x) \in \mathbb{Z}_{/p^k}[x]$ is a unit/nilpotent if and only if $\lambda'_{k,1}(a(x))$ is a unit/nilpotent. An element $a \in \frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$ is a unit/nilpotent if and only if $\Lambda_{k,1}(a)$ is a unit/nilpotent.* $\blacksquare$

The following remark is also useful:

**Remark 5.1.2** *Let $\Theta : R \longrightarrow S$ be a ring homomorphism, where $R$ and $S$ are commutative rings. Let $a, b \in R \setminus Ker\ \Theta$ then if $\Theta(b) \nmid \Theta(a)$ then $b \nmid a$.*

Proof:

Suppose $\Theta(b) \nmid \Theta(a)$ but $b|a$ then $a = bc$ some $c \notin$ Ker $\Theta$ so $\Theta(a) = \Theta(b)\Theta(c)$ which is a contradiction. $\blacksquare$

We now examine observation (2), as Ker $\Lambda_{k,1}$ is a nil ideal it is idempotent lifting (by lemma A.5.3).

**Lemma 5.1.2** *Let $e$ be a non-trivial idempotent element in $\frac{\mathbb{F}_p[x]}{(x^N-1)\mathbb{F}_p[x]}$, $e = e(x) + (x^N-1)\mathbb{F}_p[x]$, then*

$$e_{,k} = e(x)^{p^{k-1}} + (x^N-1)\mathbb{Z}_{/p^k}[x]$$

*is a non-trivial idempotent element in $\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$.*

Proof:

In $\mathbb{F}_p[x]$ one has $e(x)^2 = e(x) + g(x)(x^N - 1)$ for some $g(x) \in \mathbb{F}_p[x]$, thus in $\mathbb{Z}_{/p^k}[x]$ one has $e(x)^2 = e(x) + n(x) + g(x)(x^N - 1)$ where $n(x) \in \text{Ker } \lambda'_{k,1}$ and so

$$\begin{aligned} e(x)^{2p^{k-1}} &= (e(x) + n(x) + g(x)(x^N - 1))^{p^{k-1}} \\ &= (e(x) + n(x))^{p^{k-1}} + \text{ terms in } (x^N - 1) \\ &= e(x)^{p^{k-1}} + \text{ terms in } (x^N - 1) \end{aligned}$$

by remark 5.1.1 and hence in $\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$ one has $e_{,k}^2 = e_{,k}$. Now $\Lambda_{k,1}(e_{,k}) = e^{p^{k-1}} =$ $e$ as $e$ is idempotent in $\frac{\mathbb{F}_p[x]}{(x^N-1)\mathbb{F}_p[x]}$ and as $e$ is non-trivial so is $e_{,k}$. ■

We saw in chapter 4, section 4.5, how to calculate a set of non-trivial pairwise orthogonal idempotents $\{e_i, 1 \leq i \leq m\}$ in $\frac{\mathbb{F}_p[x]}{(x^N-1)\mathbb{F}_p[x]}$, we can now apply lemma 5.1.2 to lift these elements to a set of non-trivial pairwise orthogonal idempotents $\{e_{i,k}, 1 \leq i \leq m\}$ in $\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$. For consistency with the notation of this chapter we shall denote the idempotents in $\frac{\mathbb{F}_p[x]}{(x^N-1)\mathbb{F}_p[x]}$ by $e_{i,1}$ rather than $e_i$ from now on.

**Theorem 5.1.1** *Let $e_{i,1}$, $1 \leq i \leq m$, be the pairwise orthogonal idempotent elements satisfying $\sum_{i=1}^m e_{i,1} = 1$ such that*

$$\frac{\mathbb{F}_p[x]}{(x^N - 1)\mathbb{F}_p[x]} \cong \prod_{i=1}^{m} e_{i,1} \frac{\mathbb{F}_p[x]}{(x^N - 1)\mathbb{F}_p[x]}$$

*then the lifted idempotent elements $e_{i,k}$ described in lemma 5.1.2 are such that*

$$\frac{\mathbb{Z}_{/p^k}[x]}{(x^N - 1)\mathbb{Z}_{/p^k}[x]} \cong \prod_{i=1}^{m} e_{i,k} \frac{\mathbb{Z}_{/p^k}[x]}{(x^N - 1)\mathbb{Z}_{/p^k}[x]}.$$

Proof:

We have already shown that the $e_{i,k}$, $1 \leq i \leq m$, are non-trivial. For pairwise orthogonality we know that $e_{i,1}e_{j,1} = 0$, $i \neq j$, in $\frac{\mathbb{F}_p[x]}{(x^N-1)\mathbb{F}_p[x]}$, hence in $\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$ one has $e_{i,k}e_{j,k} = n_{i,j}$ where $n_{i,j} \in \text{Ker } \Lambda_{k,1}$ so $p|n_{i,j}$ and hence $(e_{i,k}e_{j,k})^k = 0$ hence as the $e_{i,k}$ are idempotent one has $e_{i,k}e_{j,k} = 0$ if $i \neq j$. We wish to apply theorem A.5.3 so we must show that $\sum_{i=1}^m e_{i,k} = 1$, as $\sum_{i=1}^m e_{i,1} = 1$ in $\frac{\mathbb{F}_p[x]}{(x^N-1)\mathbb{F}_p[x]}$ we have that

$\sum_{i=1}^{m} e_{i,k} = 1 + n$ in $\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$ where $n \in \text{Ker } \Lambda_{k,1}$ and hence $p|n$ so

$$(\sum_{i=1}^{m} e_{i,k})^{p^{k-1}} = 1$$

by remark 5.1.1 and from the pairwise orthogonality of the $e_{i,k}$, $1 \leq i \leq m$, we have that

$$1 = (\sum_{i=1}^{m} e_{i,k})^{p^{k-1}} = \sum_{i=1}^{m} e_{i,k}^{p^{k-1}} = \sum_{i=1}^{m} e_{i,k}.$$

Thus the $e_{i,k}$, $1 \leq i \leq m$, satisfy the conditions of theorem A.5.3 and so

$$\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]} \cong \prod_{i=1}^{m} e_{i,k} \frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}. \quad \blacksquare$$

The restriction of $\Lambda_{k,1}$ to $e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$ is a ring epimorphism which we shall denote by $\Lambda_{k,1}^i$,

$$\Lambda_{k,1}^i : e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]} \longrightarrow e_{i,1}\frac{\mathbb{F}_p[x]}{(x^N-1)\mathbb{F}_p[x]}.$$

By lemma 5.1.1 we know that an element $a \in e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$ is a unit (or is a nilpotent element) if and only if $\Lambda_{k,1}^i(a)$ is a unit (or is a nilpotent element) but $e_{i,1}\frac{\mathbb{F}_p[x]}{(x^N-1)\mathbb{F}_p[x]}$ is completely primary and thus we have proved:

**Lemma 5.1.3** *The rings* $e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$, $1 \leq i \leq m$, *are completely primary.* $\blacksquare$

**Example 5.1.1**

One has that

$$\frac{\mathbb{F}_2[x]}{(x^3-1)\mathbb{F}_2[x]} \cong e_1\frac{\mathbb{F}_2[x]}{(x^3-1)\mathbb{F}_2[x]} \times e_2\frac{\mathbb{F}_2[x]}{(x^3-1)\mathbb{F}_2[x]},$$

where

$$\begin{aligned} e_1 &= 1 + x + x^2 + (x^3-1)\mathbb{F}_2[x], \\ e_2 &= x + x^2 + (x^3-1)\mathbb{F}_2[x]. \end{aligned}$$

Using lemma 5.1.2 and theorem 5.1.1 we see that

$$\frac{\mathbb{Z}_{/4}[x]}{(x^3-1)\mathbb{Z}_{/4}[x]} \cong e_{1,2}\frac{\mathbb{Z}_{/4}[x]}{(x^3-1)\mathbb{Z}_{/4}[x]} \times e_{2,2}\frac{\mathbb{Z}_{/4}[x]}{(x^3-1)\mathbb{Z}_{/4}[x]},$$

where

$$\begin{aligned} e_{1,2} &= (1+x+x^2)^2 + (x^3-1)\mathbb{Z}_{/4}[x] \\ &= 3(1+x+x^2) + (x^3-1)\mathbb{Z}_{/4}[x], \\ e_{2,2} &= (x+x^2)^2 + (x^3-1)\mathbb{Z}_{/4}[x] \\ &= 2+x+x^2 + (x^3-1)\mathbb{Z}_{/4}[x]. \quad \blacklozenge \end{aligned}$$

Note that when $N = np^r$, $\gcd(p,n) = 1$ and integer $r > 0$, then $e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$ contains nilpotent elements that are not in Ker $\Lambda_{k,1}$, for instance $e_{i,k}R_i$.

At this stage one might ask: is $e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$ isomorphic to $\frac{\mathbb{Z}_{/p^k}[x]}{R_i(x)^{p^r}\mathbb{Z}_{/p^k}[x]}$, where $N = np^r$, $\gcd(p,n) = 1$ ? As we saw in chapter 4 this is true when $k = 1$, where we defined an isomorphism $\epsilon_i : \frac{\mathbb{F}_p[x]}{R_i^{p^r}\mathbb{F}_p[x]} \longrightarrow e_{i,1}\frac{\mathbb{F}_p[x]}{(x^{np^r}-1)\mathbb{F}_p[x]}$, $a \mapsto e_{i,1}a$, however, in general, over $\mathbb{Z}_{/p^k}$ one no longer has $R_i(x)^{p^r} | x^{np^r} - 1$ and one can no longer employ the factor theorem and, in general, the equivalent map in this situation is not well defined, hence we shall always work with the idempotent representation.

With regards to notation we shall sometimes say, for instance, $p|g$ for some $g \in e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$, by which we mean that $g$ is of the form $pg'$ where $g' \in e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$ (and of course $pg'$ means $(p + p^k\mathbb{Z})g'$), however in doing this we are abusing notation for, in general, $p \notin e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$ (of course $pe_{i,k}$ is in $e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$). Suppose $\alpha e_{i,1} \in e_{i,1}\frac{\mathbb{F}_p[x]}{(x^N-1)\mathbb{F}_p[x]}$, where $N = np^r$, $r \in \mathbb{N}$ and $\gcd(p,n) = 1$, $\alpha e_{i,1} = \alpha(x)e_{i,1}(x) + (x^N-1)\mathbb{F}_p[x]$, the image of the element $\alpha \in \frac{\mathbb{F}_p[x]}{R_i(x)^{p^r}\mathbb{F}_p[x]}$ under the isomorphism $\epsilon_i$ described in chapter 4, lemma 4.5.2, we shall frequently make use of the element $\alpha e_{i,k} \in e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$ defined by

$$\alpha e_{i,k} = \alpha(x)e_{i,k}(x) + (x^N-1)\mathbb{Z}_{/p^k}[x], \tag{5.1.2}$$

where $\alpha(x)$ in (5.1.2) is the embedded element described by (5.1.1). The element $\alpha e_{i,k}$ can be thought of as a canonical pre-image of $\alpha e_{i,1}$ under $\Lambda^i_{k,1}$, for clearly $\Lambda^i_{k,1}(\alpha e_{i,k}) =$

$\alpha e_{i,1}$, and we shall refer to $\alpha e_{i,k}$ as *the canonical pre-image* of $\alpha e_{i,1}$ in $e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$. In particular the canonical pre-image of $e_{i,1}$ is $e_{i,k}$. Because the canonical pre-images are in one-one correspondence with the elements of $e_{i,1}\frac{\mathbb{F}_p[x]}{(x^N-1)\mathbb{F}_p[x]}$ those canonical pre-images with a particular property can be easily counted using results from chapter 3. These properties are utilised in section 5.1.2 and onwards and are particularly useful when one sets about attempting to find cycle sets in the $\gcd(p,N) > 1$ case (see example 5.2.1).

We shall find the following result useful, its proof is in appendix B.

**Lemma 5.1.4** *Let $R$ be a commutative ring and $a \in R$, where char $R = p^k$, $k > 1$ and $p$ is prime. Let the identity element in $R$ be $e$, then*

$$a^p - e = (a-e)^p + p\eta_p(a)(a-e)$$

*and for all integers $j > 0$*

$$a^{p^j} - e = (a^{p^{j-1}} - e)^p + p\eta_p(a^{p^{j-1}})(a^{p^{j-1}} - e),$$

*where*

$$\eta_p(a) = \begin{cases} e & p = 2; \\ -\sum_{i=1}^{\frac{p-1}{2}} 1/p \begin{pmatrix} p \\ i \end{pmatrix} a^i(-e)^i(a^{p-2i-1} + a^{p-2i-2} + \ldots + e) & p > 2. \end{cases}$$

*Further, if non-unit $b \in R$ is such that $b|a-e$ then $b \nmid \eta_p(a)$.* ■

The proof of the following result utilises lemma 5.1.4 and is also in appendix B.

**Lemma 5.1.5** *If in $\mathbb{F}_p[x]$, $x^n - 1 = \prod_{i=1}^m R_i(x)$ then in $\mathbb{Z}_{/p^k}[x]$, where integer $k > 1$, one finds that for $1 \le i \le m$*

$$R_i(x)^{p^{r-k+1}} | x^{np^r} - 1 \quad but \quad R_i(x)^{p^{r-k+1}+1} \nmid x^{np^r} - 1,$$

*for all integers $r \ge k-1$.* ■

### 5.1.1 The relationship between $\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{p^k}[x]}$ and $\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^{r-j}}-1)\mathbb{Z}_{p^k}[x]}$ where

$$r \ge j > 0$$

Where necessary we shall denote $e_{i,k}$ in $\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{p^k}[x]}$ by $e^r_{i,k}$, $1 \le i \le m$. We have

$$x^{np^r} - 1 = (x^{np^{r-j}} - 1)(x^{np^{r-j}(p^j-1)} + x^{np^{r-j}(p^j-2)} + \ldots + x^{np^{r-j}} + 1)$$

for all $0 < j \leq r$, hence $(x^{np^r} - 1)\mathbb{Z}_{/p^k}[x] \subset (x^{np^{r-j}} - 1)\mathbb{Z}_{/p^k}[x]$. Applying the factor theorem we see that there is a ring homomorphism $\Gamma^k_{r,r-j}$:

$$\begin{aligned} \Gamma^k_{r,r-j} : \frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r} - 1)\mathbb{Z}_{p^k}[x]} &\longrightarrow \frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^{r-j}} - 1)\mathbb{Z}_{p^k}[x]} \\ a(x) + (x^{np^r} - 1)\mathbb{Z}_{p^k}[x] &\mapsto a(x) + (x^{np^{r-j}} - 1)\mathbb{Z}_{p^k}[x]. \end{aligned}$$

There is also a ring homomorphism

$$\begin{aligned} F^k_{r-j,r} : \frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^{r-j}} - 1)\mathbb{Z}_{p^k}[x]} &\longrightarrow \frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r} - 1)\mathbb{Z}_{p^k}[x]} \\ a(x) + (x^{np^{r-j}} - 1)\mathbb{Z}_{p^k}[x] &\mapsto a(x^{p^j}) + (x^{np^r} - 1)\mathbb{Z}_{p^k}[x] \end{aligned}$$

induced by the monomorphism $a(x) \mapsto a(x^{p^j})$ on $\mathbb{Z}_{/p^k}[x]$. In fact $F^k_{r-j,r}$ is a monomorphism for suppose that

$$F^k_{r-j,r}(a) = F^k_{r-j}(b),$$

then $a(x^{p^j}) - b(x^{p^j}) = c(x)(x^{np^r} - 1)$ for some $c(x) \in \mathbb{Z}_{/p^k}[x]$ when $a(x)$ and $b(x)$ are the canonical representatives of $a$ and $b$ and hence deg $a(x) < np^{r-j}$ and deg $b(x) < np^{r-j}$ thus deg $a(x^{p^j}) < np^r$ and deg $b(x^{p^j}) < np^r$ so must have $a(x^{p^j}) = b(x^{p^j})$ and hence $a(x) = b(x)$ as $a(x) \mapsto a(x^{p^j})$ is a monomorphism.

**Lemma 5.1.6** *Suppose that* $\{e^{r-j}_{i,k} : 1 \leq i \leq m\}$ *are the pairwise orthogonal idempotents such that*

$$\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^{r-j}} - 1)\mathbb{Z}_{/p^k}[x]} \cong \prod_{i=1}^{m} e^{r-j}_{i,k} \frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^{r-j}} - 1)\mathbb{Z}_{/p^k}[x]},$$

*let* $\hat{e}^r_{i,k} = F^k_{r-j,r}(e^{r-j}_{i,k})$, $1 \leq i \leq m$, *then*

$$\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r} - 1)\mathbb{Z}_{/p^k}[x]} \cong \prod_{i=1}^{m} \hat{e}^r_{i,k} \frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r} - 1)\mathbb{Z}_{/p^k}[x]}.$$

Proof:

It suffices to show that the $\hat{e}^r_{i,k}$, $1 \leq i \leq m$, are non-trivial pairwise orthogonal idempotents satisfying $\sum_{i=1}^{m} \hat{e}^r_{i,k} = 1$. The $\hat{e}^r_{i,k}$ are idempotent as homomorphisms map

idempotents to idempotents, similarly pairwise orthogonality is preserved and, as $F^k_{r-j,r}$ is a monomorphism, non-triviality is preserved. Now,

$$\sum_{i=1}^{m} \hat{e}^r_{i,k} = \sum_{i=1}^{m} F^k_{r-j,r}(e^{r-j}_{i,k}) = F^k_{r-j,r}(\sum_{i=1}^{m} e^{r-j}_{i,k}) = F^k_{r-j,r}(1) = 1. \quad \blacksquare$$

Note that it is easily verified that

$$F^k_{r-s+j,r} \circ F^k_{r-s,r-s+j} = F^k_{r-s,r},$$

for $0 < s \leq r$, $0 < j < s$.

At this stage an immediate question is whether or not the idempotents $\hat{e}^r_{i,k}$ calculated using lemma 5.1.6 are the same as those lifted from $\frac{\mathbb{F}_p[x]}{(x^{np^r}-1)\mathbb{F}_p[x]}$ as described in lemma 5.1.2, *i.e.* the $e^r_{i,k}$. The $e^r_{i,k}$, $1 \leq i \leq m$, satisfy $\Lambda_{k,1}(e^r_{i,k}) = e^r_{i,1}$. We have the following remark, its proof is in appendix B as is that of the lemma that follows it.

**Remark 5.1.3** *For* $1 \leq i \leq m$

$$\Lambda_{k,1}(\hat{e}^r_{i,k}) = e^r_{i,1}. \quad \blacksquare$$

**Lemma 5.1.7** *Suppose that* $e$ *and* $f$ *are idempotent in* $\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$ *and are such that* $\Lambda_{k,1}(e) = \Lambda_{k,1}(f)$, *then* $e = f$. $\blacksquare$

**Corollary 5.1.1** *For* $1 \leq i \leq m$

$$\hat{e}^r_{i,k} = e^r_{i,k}.$$

Proof:

Immediate from lemma 5.1.7 and remark 5.1.3. $\blacksquare$

Thus lemma 5.1.6 provides an easier method of computing the $e^r_{i,k}$.

**Example 5.1.2**

Recall from example 5.1.1 that

$$\frac{\mathbb{Z}_{/4}[x]}{(x^3-1)\mathbb{Z}_{/4}[x]} \cong e_{1,2}\frac{\mathbb{Z}_{/4}[x]}{(x^3-1)\mathbb{Z}_{/4}[x]} \times e_{2,2}\frac{\mathbb{Z}_{/4}[x]}{(x^3-1)\mathbb{Z}_{/4}[x]},$$

where

$$\begin{aligned} e_{1,2} &= 3(1+x+x^2) + (x^3-1)\mathbb{Z}_{/4}[x], \\ e_{2,2} &= 2+x+x^2 + (x^3-1)\mathbb{Z}_{/4}[x]. \end{aligned}$$

Then using lemma 5.1.6 and corollary 5.1.1 we have that

$$\frac{\mathbb{Z}_{/4}[x]}{(x^{2^r 3}-1)\mathbb{Z}_{/4}[x]} \cong e^r_{1,2}\frac{\mathbb{Z}_{/4}[x]}{(x^{2^r 3}-1)\mathbb{Z}_{/4}[x]} \times e^r_{2,2}\frac{\mathbb{Z}_{/4}[x]}{(x^{2^r 3}-1)\mathbb{Z}_{/4}[x]},$$

for all $r \in \mathbb{N}$ where for $r > 0$

$$\begin{aligned} e^r_{1,2} &= 3(1 + x^{2^r} + x^{2^{r+1}}) + (x^{2^r 3}-1)\mathbb{Z}_{/4}[x], \\ e^r_{2,2} &= 2 + x^{2^r} + x^{2^{r+1}} + (x^{2^r 3}-1)\mathbb{Z}_{/4}[x]. \quad \blacklozenge \end{aligned}$$

It is clear that Im $F^k_{r-j,r}$ is a subring of $\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$, isomorphic to $\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^{r-j}}-1)\mathbb{Z}_{/p^k}[x]}$, also it is clear that there is a corresponding subring of $e^r_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$ isomorphic to $e^{r-j}_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^{r-j}}-1)\mathbb{Z}_{/p^k}[x]}$ for $1 \le i \le m$. The proof of the next lemma is in appendix B.

**Lemma 5.1.8** *For* $1 \le i \le m$

$$\Gamma^k_{r,r-1}(e^r_{i,k}) = e^{r-1}_{i,k}. \quad \blacksquare$$

Note that

$$\Gamma^k_{r,r-s} = \Gamma^k_{r-j,r-s} \circ \Gamma^k_{r,r-j},$$

for $0 \le s \le r$ and $0 \le j \le s$.

Using lemma 5.1.8 it is clear that the restriction of $\Gamma^k_{r,r-1}$ to $e^r_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$ is a homomorphism onto $e^{r-j}_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^{r-j}}-1)\mathbb{Z}_{/p^k}[x]}$, $1 \le i \le m$, which, where necessary, we shall denote by $\Gamma^{i,k}_{r,r-1}$.

### 5.1.2 The relationship between $\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{p^k}[x]}$ and $\frac{\mathbb{Z}_{/p^{k-s}}[x]}{(x^N-1)\mathbb{Z}_{p^{k-s}}[x]}$ where $k > s > 0$

We note first that (as usual using the factor theorem) for all $k \in \mathbb{N}\setminus\{0\}$ and $k > s > 0$ there are ring epimorphisms

$$\begin{aligned} \lambda_{k,k-s} : \mathbb{Z}_{/p^k} &\longrightarrow \mathbb{Z}_{p^{k-s}} \\ m + p^k\mathbb{Z} &\mapsto m + p^{k-s}\mathbb{Z}, \end{aligned}$$

it follows that one has induced homomorphisms, all surjective,

$$\lambda'_{k,k-s} : \mathbb{Z}_{/p^k}[x] \longrightarrow \mathbb{Z}_{/p^{k-s}}[x],$$

$$\Lambda_{k,k-s} : \frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{p^k}[x]} \longrightarrow \frac{\mathbb{Z}_{/p^{k-s}}[x]}{(x^N-1)\mathbb{Z}_{p^{k-s}}[x]}.$$

It is easy to verify that $\lambda_{k,k-s} = \lambda_{k-j,k-s} \circ \lambda_{k,k-j}$ for $0 < j < s$ and it follows that

$$\lambda'_{k,k-s} = \lambda'_{k-j,k-s} \circ \lambda'_{k,k-j},$$

$$\Lambda_{k,k-s} = \Lambda_{k-j,k-s} \circ \Lambda_{k,k-j}.$$

We shall denote the restriction of $\Lambda_{k,k-s}$ to $e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{p^k}[x]}$ by $\Lambda^i_{k,k-s}$.

**Lemma 5.1.9** *Let $e_{i,1}$, $1 \leq i \leq m$, be a set of non-trivial idempotents in $\frac{\mathbb{F}_p[x]}{(x^N-1)\mathbb{F}_p[x]}$, let $e_{i,k}$ and $e_{i,k-s}$ be the lifted idempotents in $\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{p^k}[x]}$ and $\frac{\mathbb{Z}_{/p^{k-s}}[x]}{(x^N-1)\mathbb{Z}_{p^{k-s}}[x]}$ respectively. Then $\Lambda_{k,k-s}(e_{i,k}) = e_{i,k-s}$.*

Proof:

We have

$$e_{i,k} = e_{i,1}(x)^{p^{k-1}} + (x^N-1)\mathbb{Z}_{/p^k}[x]$$

$$e_{i,k-s} = e_{i,1}(x)^{p^{k-s-1}} + (x^N-1)\mathbb{Z}_{/p^{k-s}}[x],$$

thus

$$\begin{aligned}\Lambda_{k,k-s}(e_{i,k}) &= e_{i,1}(x)^{p^{k-1}} + (x^N-1)\mathbb{Z}_{/p^{k-s}}[x] \\ &= (e_{i,1}(x)^{p^{k-s-1}})^{p^s} + (x^N-1)\mathbb{Z}_{/p^{k-s}}[x] \\ &= e_{i,k-s}^{p^s} \\ &= e_{i,k-s}. \quad \blacksquare\end{aligned}$$

It follows that $\Lambda^i_{k,k-s}$ is a surjective homomorphism,

$$\Lambda^i_{k,k-s} : e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{p^k}[x]} \longrightarrow e_{i,k-s}\frac{\mathbb{Z}_{/p^{k-s}}[x]}{(x^N-1)\mathbb{Z}_{p^{k-s}}[x]}.$$

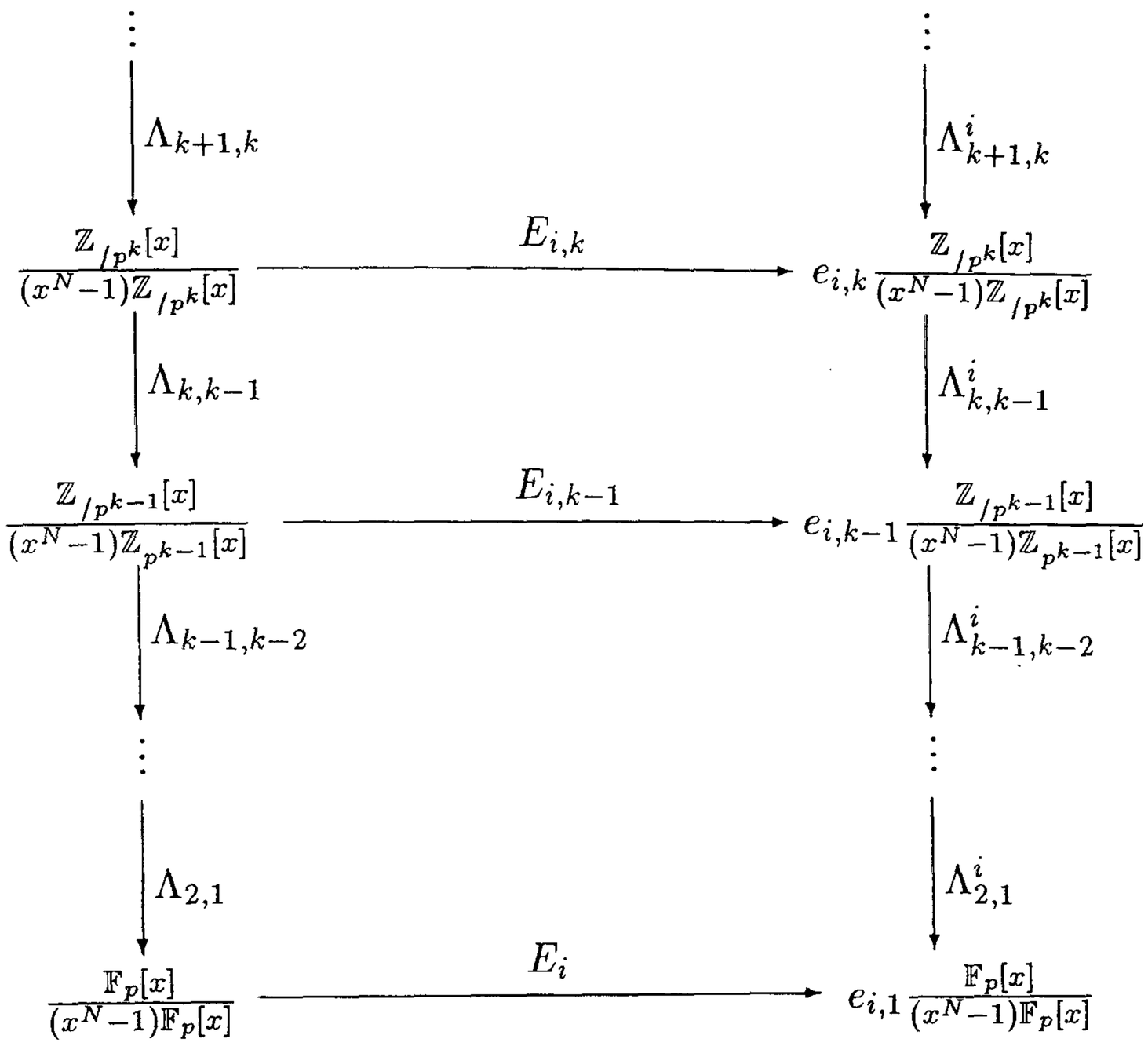


Figure 5.2: The homomorphisms $\Lambda_{k,k-1}, \Lambda^i_{k,k-1}$ and $E_{i,k}$ are all surjective and the diagram commutes.

We have "projection" homomorphisms $E_{i,k}$, $1 \leq i \leq m$,

$$E_{i,k} : \frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{p^k}[x]} \longrightarrow e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{p^k}[x]}$$

$$a(x) + (x^N-1)\mathbb{Z}_{/p^k}[x] \mapsto e_{i,k}(x)a(x) + (x^N-1)\mathbb{Z}_{/p^k}[x],$$

the situation is summed up in figure 5.2, where $E_{i,1}$ is denoted by $E_i$ for consistency with chapter 4.

**Lemma 5.1.10** *There is a bijection between* Ker $\Lambda^i_{k,n}$ *and* Im $\Lambda^i_{k,k-n}$ *for each integer* $n$, $0 < n < k$. ■

The proof of lemma 5.1.10 can be found in appendix B. We can use lemma 5.1.10 to count the elements of $e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{p^k}[x]}$.

**Lemma 5.1.11** *For* $1 \leq i \leq m$ *and each integer* $k \geq 1$

$$\left| e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{p^k}[x]} \right| = p^{kd_ip^r},$$

*where*

$$e_{i,1}\frac{\mathbb{F}_p[x]}{(x^{np^r}-1)\mathbb{F}_p[x]} \cong \frac{\mathbb{F}_p[x]}{R_i(x)^{p^r}\mathbb{F}_p[x]}$$

*and* $\deg\ R_i(x) = d_i$ *and* $\gcd(p,n) = 1$.

Proof:

By the first (ring) isomorphism theorem

$$e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{p^k}[x]} \Big/ \mathrm{Ker}\ \Lambda^i_{k,k-1} \cong e_{i,k-1}\frac{\mathbb{Z}_{/p^{k-1}}[x]}{(x^{np^r}-1)\mathbb{Z}_{p^{k-1}}[x]}$$

hence by Lagrange's theorem

$$\left|e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{p^k}[x]}\right| = \left|e_{i,k-1}\frac{\mathbb{Z}_{/p^{k-1}}[x]}{(x^{np^r}-1)\mathbb{Z}_{p^{k-1}}[x]}\right| \ \left|\mathrm{Ker}\ \Lambda^i_{k,k-1}\right|$$

and by lemma 5.1.10

$$\left|\mathrm{Ker}\ \Lambda^i_{k,k-1}\right| = \left|\mathrm{Im}\ \Lambda^i_{k,1}\right| = \left|e_{i,1}\frac{\mathbb{F}_p[x]}{(x^N-1)\mathbb{F}_p[x]}\right| = p^{p^r d_i}$$

hence

$$\left|e_{i,2}\frac{\mathbb{Z}_{/p^2}[x]}{(x^N-1)\mathbb{Z}_{p^2}[x]}\right| = \left|e_{i,1}\frac{\mathbb{F}_p[x]}{(x^N-1)\mathbb{F}_p[x]}\right| p^{p^r d_i} = p^{2d_i p^r},$$

the result now follows by induction on $k$. ■

**Corollary 5.1.2** *For all integers* $k > 1$ *and any integer* $s$ *such that* $0 < s < k$ *one has*

$$\left|Ker\ \Lambda^i_{k,s}\right| = p^{(k-s)d_i p^r}.$$

Proof:

By lemma 5.1.10 and lemma 5.1.11

$$\left|\mathrm{Ker}\ \Lambda^i_{k,s}\right| = \left|\mathrm{Im}\ \Lambda^i_{k,k-s}\right| = \left|e_{i,k-s}\frac{\mathbb{Z}_{/p^{k-s}}[x]}{(x^{np^r}-1)\mathbb{Z}_{p^{k-s}}[x]}\right| = p^{(k-s)d_i p^r} \quad \blacksquare$$

For each integer $i$, $1 \le i \le m$, and any integer $k > 1$ one has that

$$\mathrm{Ker}\ \Lambda^i_{k,k-1} \le \mathrm{Ker}\ \Lambda^i_{k,k-2} \le \ldots \le \mathrm{Ker}\ \Lambda^i_{k,2} \le \mathrm{Ker}\ \Lambda^i_{k,1},$$

thus one can write

$$\begin{aligned}\text{Ker } \Lambda^i_{k,1} &= \text{Ker } \Lambda^i_{k,1} \setminus \text{Ker } \Lambda^i_{k,2} \cup \text{Ker } \Lambda^i_{k,2} \setminus \text{Ker } \Lambda^i_{k,3} \cup \ldots \\ &\quad \ldots \cup \text{Ker } \Lambda^i_{k,k-2} \setminus \text{Ker } \Lambda^i_{k,k-1} \cup \text{Ker } \Lambda^i_{k,k-1} \setminus \{0\} \cup \{0\},\end{aligned}$$

a disjoint union. Putting $C^i_{k,j} = \text{Ker } \Lambda^i_{k,j} \setminus \text{Ker } \Lambda^i_{k,j+1}$, anything in $\text{Ker } \Lambda^i_{k,j}$ is annihilated by $p^{k-j}$ and hence anything in $C^i_{k,j}$ is annihilated by $p^{k-j}$ but not by $p^{k-j-1}$ and we have:

**Lemma 5.1.12** *For each integer $i$, $1 \leq i \leq m$, and any integer $k > 1$ one has that*

$$Ker\ \Lambda^i_{k,1} = C^i_{k,1} \cup C^i_{k,2} \cup \ldots \cup C^i_{k,k-2} \cup C^i_{k,k-1} \cup \{0\},$$

*a disjoint union and $a \in C^i_{k,j}$, $1 \leq j \leq k-1$, if and only if $p^{k-j}a = 0$ but $p^{k-j-1}a \neq 0$.*

■

The proof of the next lemma can be found in appendix B.

**Lemma 5.1.13** *For any integer $k > 1$ and all integers $j$, $1 \leq j \leq k-1$, one has*

$$\left|C^i_{k,j}\right| = p^{(k-j-1)d_i p^r}(p^{d_i p^r} - 1)$$

*and*

$$\left|C^i_{k,k-J} \cup \ldots \cup C^i_{k,k-1}\right| = p^{(J-1)d_i p^r} - 1,$$

*for any integer $J$, $2 < J \leq k$.* ■

When $\gcd(p, N) > 1$ it is instructive to look more closely at $C^i_{k,j}$. Suppose $N = np^r$, integer $r > 0$ and $\gcd(p, n) = 1$, repeated use of lemma 5.1.10 shows that one can write $C^i_{k,j}$ as the disjoint union

$$\begin{aligned}C^i_{k,j} = \{&p^j e^r_{i,k}\beta R^I_i + \sum_{s=1}^{k-1-j} p^{j+s} e^r_{i,k}\gamma_s R_i^{I_s} : p^r > I > 0, p^r > I_s \geq 0, 1 \leq s \leq k-1-j, \\ &e^r_{i,k}\beta \text{ a unit}, e^r_{i,k}\gamma_s \text{ either a unit or } 0, 1 \leq s \leq k-1-j\} \cup \\ &\{p^j e^r_{i,k}\beta + \sum_{s=1}^{k-1-j} p^{j+s} e^r_{i,k}\gamma_s R_i^{I_s} : p^r > I_s \geq 0, 1 \leq s \leq k-1-j, \\ &e^r_{i,k}\beta \text{ a unit}, e^r_{i,k}\gamma_s \text{ either a unit or } 0, 1 \leq s \leq k-1-j\},\end{aligned} \tag{5.1.3}$$

where $e^r_{i,k}\beta R^I_i$, $e^r_{i,k}\beta$ and the $e^r_{i,k}\gamma_s R^{I_s}_i$, $1 \leq s \leq k-1-j$, are the canonical pre-images of elements $e^r_{i,1}\beta R^I_i$, $e^r_{i,1}\beta$ and the $e^r_{i,1}\gamma_s R^{I_s}_i$, $1 \leq s \leq k-1-j$, in $e^r_{i,1}\frac{\mathbb{F}_p[x]}{(x^{np^r}-1)\mathbb{F}_p[x]}$ described by (5.1.2). Thus there are $|U_p(R_i,r)|$ choices for $e^r_{i,k}\beta$, $|Nil_p(R_i,r)|-1$ choices for $e^r_{i,k}\beta R^I_i$ and $p^{p^r d_i}$ choices for each $e^r_{i,k}\gamma_s R^{I_s}_i$, $1 \leq s \leq k-1-j$, where $d_i = \deg R_i(x)$. Using the previous comments we see that

$$\begin{aligned} |C^i_{k,j}| &= (|Nil_p(R_i,r)|-1)(p^{p^r d_i})^{k-j-1} + |U_p(R_i,r)|(p^{p^r d_i})^{k-j-1} \\ &= (p^{p^r d_i}-1)(p^{p^r d_i})^{k-j-1}, \end{aligned}$$

in agreement with lemma 5.1.13. Of course when $r > 0$ there are nilpotent elements, for instance $e^r_{i,k}R_i$, which are not in Ker $\Lambda^i_{k,1}$. We can easily count such elements, they are the pre-images of the non-zero nilpotent elements in $e^r_{i,1}\frac{\mathbb{F}_p[x]}{(x^{np^r}-1)\mathbb{F}_p[x]}$ and there are $(|Nil_p(R_i,r)|-1)|\text{Ker }\Lambda^i_{k,1}|$ of them, *i.e.* there are

$$(p^{d_i(p^r-1)}-1)p^{(k-1)d_i p^r} \tag{5.1.4}$$

nilpotent elements in $e^r_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$ which are not in Ker $\Lambda^i_{k,1}$, where we have used lemma 3.3.3 and corollary 5.1.2, consequently there are

$$p^{d_i(kp^r-1)} \tag{5.1.5}$$

nilpotent elements in total. It is clear that the maximal ideal of nilpotent elements is generated by $e^r_{i,k}R_i$ and $e^r_{i,k}p$. We shall denote the units in $e^r_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$ by $U(p^k,i,r)$.

**Lemma 5.1.14** *In* $e^r_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$, $r \in \mathbb{N}$, *the number of units is*

$$|U(p^k,i,r)| = p^{(kp^r-1)d_i}(p^{d_i}-1).$$

Proof:

When $r = 0$ one has

$$\begin{aligned} |U_{p^k}(i,0)| &= \left|e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^n-1)\mathbb{Z}_{/p^k}[x]}\right| - |\text{Ker }\Lambda^i_{k,1}| \\ &= p^{(k-1)d_i}(p^{d_i}-1), \end{aligned}$$

where we have used lemma 5.1.11 and corollary 5.1.2. For $r > 0$, again using lemma 5.1.11 and also (5.1.5) one gets

$$|U(p^k, i, r)| = p^{(kp^r-1)d_i}(p^{d_i} - 1). \quad \blacksquare$$

We can write any element $a \in e^r_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$ uniquely as

$$a = a_0 e^r_{i,k} + \sum_{j=1}^{k-1} p^j a_j e^r_{i,k} \tag{5.1.6}$$

a sum of canonical pre-images multiplied by distinct powers of $p$, for if

$$a = b_0 e^r_{i,k} + \sum_{j=1}^{k-1} p^j b_j e^r_{i,k}$$

is another such expression for $a$ one has

$$(a_0 - b_0)e^r_{i,k} + \sum_{j=1}^{k-1} p^j (a_j - b_j) e^r_{i,k} = 0$$

hence applying $\Lambda^i_{k,1}$ gives $a_0 e^r_{i,1} = b_0 e^r_{i,1}$ hence $a_0 e^r_{i,k} = b_0 e^r_{i,k}$, then applying $\Lambda^i_{k,2}$ shows that $a_1 e^r_{i,k} = b_1 e^r_{i,k}$ and so on. Every element has such a representation for the number of sums of the form (5.1.6) is $(p^{p^r d_i})^k = \left| e^r_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]} \right|$ by lemma 5.1.11.

We now turn our attention to the canonical pre-image of $e^r_{i,1}R_i$, $e^r_{i,k}R_i$, the proofs of the results in the remainder of this section can be found in appendix B. Let $N = np^r$, integer $r \geq 1$ and $\gcd(p, n) = 1$. When $k = 1$, $e^r_{i,1}R_i^{p^r} = 0$, this is no longer true for $k > 1$:

**Lemma 5.1.15** *For integer $k > 1$, $r \in \mathbb{N}\setminus\{0\}$ and $\gcd(p, n) = 1$, in $e^r_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$, $e^r_{i,k}R_i^{p^r} \neq 0$ for $1 \leq i \leq m$.* $\blacksquare$

We must now ask: what power of $e^r_{i,k}R_i$ is zero? It is instructive to start by considering the $k = 2$ case, where we have the following:

**Remark 5.1.4** *For $1 \leq i \leq m$ and integer $r > 0$*

$$e^r_{i,2}R_i^{p^r} = p\alpha_r R_i^{p^{r-1}},$$

*where $\alpha_r$ is a unit.* $\blacksquare$

We can now write down a useful expression for $e_{i,k}^r R_i^{p^r}$, $1 \leq i \leq m$, for $k \geq 2$ and $r \geq k-1$.

**Lemma 5.1.16** *For each integer $k > 1$ and all integers $r \geq k-1$ and $1 \leq i \leq m$*

$$e_{i,k}^r R_i^{p^r} = p\alpha_r e_{i,k}^r R_i^{p^{r-1}} + \sum_{j=2}^{k-1} p^j \beta_j e_{i,k}^r R_i^{p^{r-j}},$$

*where $\alpha_r e_{i,k}^r$ and the $\beta_j e_{i,k}^r$, $2 \leq j \leq k-1$, are units.* ■

Note that $\alpha_r e_{i,k}^r R_i^{p^{r-1}}$ and the $\beta_j e_{i,k}^r R_i^{p^{r-j}}$, $2 \leq j \leq k-1$, in lemma 5.1.16 are canonical pre-images. Of course when $r < k-1$ we can still write $e_{i,k}^r R_i^{p^r}$ as a sum

$$e_{i,k}^r = p\alpha_r e_{i,k}^r R_i^{p^{r-1}} + \sum_{j=2}^{k-1} p^j \gamma_j e_{i,k}^r,$$

but, in general, the canonical pre-image $\gamma_j e_{i,k}^r$, $2 \leq j \leq k-1$, is not equal to $\hat{\gamma}_j e_{i,k}^r R_i^{p^{r-j}}$ with $\hat{\gamma}_j e_{i,k}^r$ a unit.

**Lemma 5.1.17** *For $k = 3$ and all integers $r \geq 2$*

$$e_{i,3}^r R_i^{p^r + p^{r-1}(p-1)} = p^2 \alpha_r^2 e_{i,3}^r R_i^{p^{r-1}} + p^2 \beta_2 e_{i,3}^r R_i^{p^r + p^{r-2} - p^{r-1}}.$$

*For $k > 3$ and any integer $r \geq k-1$*

$$\begin{aligned} e_{i,k}^r R_i^{p^r + (k-2)p^{r-1}(p-1)} &= p^{k-1}\alpha_r^{k-1} e_{i,k}^r R_i^{p^{r-1}} + p^{k-1}\beta_2 e_{i,k}^r \alpha_r^{k-3} R_i^{p^r + p^{r-2} - p^{r-1}} \\ &\quad + \sum_{j=4}^{k} p^{k-1}\gamma_j e_{i,k}^r \alpha_r^{k-j} R_i^{p^r + p^{r-j+1} - p^{r-1}}. \end{aligned}$$ ■

Examination of lemma 5.1.17 reveals that

$$e_{i,k}^r R_i^{p^r + j} \in C_{k,k-s}^i, \quad \text{for } (s-1)p^{r-1}(p-1) \leq j \leq sp^{r-1}(p-1) - 1, \tag{5.1.7}$$

where $1 \leq s \leq k-2$. The next result shows that (5.1.7) extends to $s = k-1$.

**Corollary 5.1.3** *For $r \geq k-1$*

$$e_{i,k}^r R_i^{p^r + (k-1)p^{r-1}(p-1)} = 0$$

*and $p^r + (k-1)p^{r-1}(p-1)$ is the least power of $e_{i,k}^r R_i$ such that this is true.* ■

For any $R(x) \in \mathbb{Z}_{/p^k}[x]$ one has that, for each integer $s > 0$,

$$R(x^{p^s}) = R(x)^{p^s} + pV(x)$$

for some $V(x) \in \mathbb{Z}_{/p^k}[x]$. Let $r < k-1$, we can apply $F^k_{r,r+J}$ to $e^r_{i,k}R^I_i$, $I \in \mathbb{N} \setminus \{0\}$, for integer $J$, $r + J \geq k - 1$, then as $F^k_{r,r+J}$ is a monomorphism, we have

$$e^r_{i,k}R^I_i = 0 \text{ if and only if } F^k_{r,r+J}(e^r_{i,k}R^I_i) = 0.$$

The comments above are used in the proof of the following theorem.

**Theorem 5.1.2** *In* $e^r_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$ *for any* $k > 1$ *and* $r > 0$

$$e^r_{i,k}R_i^{p^r+(k-1)p^{r-1}(p-1)} = 0$$

*and* $p^r + (k-1)p^{r-1}(p-1)$ *is the minimal power of* $e^r_{i,k}R_i$ *that is zero except possibly in the case* $p = 2, r = 1, k > 2$. ■

In the case $p = 2$, $r = 1$, it is not always the case that $k + 1$ is the minimal power of $e^1_{i,k}R_i$ that is zero, for instance when $k = 5$ and $N = 30$ and for $k = 14$ and $N = 7$. However we have the following:

**Remark 5.1.5** *If* $k = 2^l$, *integer* $l \geq 1$ *then the minimal power of* $e^1_{i,2^l}R_I$ *that is zero is* $2^l + 1$. ■

## 5.2 Dynamics in $e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$ when $U = 0$

We begin with a lemma which links the maximum orbit length under a unit $\mathbb{T}_k \in e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$ with that under $\Lambda^i_{k,k-n} \in e_{i,k-n}\frac{\mathbb{Z}_{/p^{k-n}}[x]}{(x^N-1)\mathbb{Z}_{/p^{k-n}}[x]}$ for each integer $n$, $0 < n < k$, the proof can be found in appendix B, as can that of lemma 5.2.2.

**Lemma 5.2.1** *Let* $\{\mathbb{T}_k\}_{k\in\mathbb{N}\setminus\{0\}}$ *be such that* $\mathbb{T}_k \in e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$ *and* $\Lambda^i_{k+1,k}(\mathbb{T}_{k+1}) = \mathbb{T}_k$. *Suppose that* $\mathbb{T}_1^{\Pi_N} = e_{i,1}$, $\Pi_N$ *minimal, and let* $s^*$ *be the least integer greater than one such that* $\mathbb{T}_{s^*}^{\Pi_N} = e_{i,s^*} + g$ *where* $g$ *is non-zero, if such an integer exists. Then for all* $k \geq s^*$

$$\Pi_N(\mathbb{T}_k) = p^{k-s^*+1}\Pi_N(\mathbb{T}_1). \quad \blacksquare$$

We can use lemma 5.2.1 and lemma 5.1.12 to obtain a result about the periods of the orbits of the elements of Ker $\Lambda^i_{k,1}$ under a unit $\mathbb{T}_k \in e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$ for any integer $k > 1$.

**Lemma 5.2.2** *Let* $\{\mathbb{T}_k\}_{k\in\mathbb{N}\setminus\{0\}}$ *be such that* $\mathbb{T}_k \in e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$, $\mathbb{T}_k$ *a unit and* $\Lambda^i_{k+1,k}(\mathbb{T}_{k+1}) = \mathbb{T}_k$ *for all integers* $k > 0$. *Let* $s^*$ *be the least integer greater than* 1 *(if such an integer exists) such that* $\mathbb{T}_{s^*}^{\Pi_N} \neq e_{i,s^*}$, *where* $\Pi_N = \Pi_N(\mathbb{T}_1)$. *Then for* $k \leq s^*$, *or all integers* $k > 0$ *if* $s^*$ *does not exist, all elements of Ker* $\Lambda^i_{k,1}$ *have prime period that divides* $\Pi_N$ *under* $\mathbb{T}_k$. *For* $k > s^*$ *the elements of*

$$C^i_{k,k-s^*+1} \cup C^i_{k,k-s^*+2} \cup \ldots \cup C^i_{k,k-1} \cup \{0\}$$

*have prime period dividing* $\Pi_N$ *under* $\mathbb{T}_k$ *while the elements of* $C^i_{k,k-s^*+1-j}$ *have prime periods dividing* $p^j\Pi_N$ *under* $\mathbb{T}_k$, $1 \leq j \leq k - s^*$. ■

When $\gcd(n,p) = 1$, then, as $e_{i,1}\frac{\mathbb{F}_p[x]}{(x^n-1)\mathbb{F}_p[x]}$ is a field in this case, one has that Ker $\Lambda^i_{k,1}$ is the maximal ideal consisting of nilpotent elements and any element $\alpha$ of $e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^n-1)\mathbb{Z}_{/p^k}[x]}$ such that $\Lambda^i_{k,1}(\alpha) \neq 0$ is a unit. In this case we can make lemma 5.2.2 more precise.

**Theorem 5.2.1** *Let* $\gcd(p,n) = 1$ *and* $\{\mathbb{T}_k\}_{k\in\mathbb{N}\setminus\{0\}}$ *be such that* $\mathbb{T}_k \in e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^n-1)\mathbb{Z}_{/p^k}[x]}$, $\mathbb{T}_k$ *a unit and* $\Lambda^i_{k+1,k}(\mathbb{T}_{k+1}) = \mathbb{T}_k$ *for all integers* $k > 0$. *Let* $s^*$ *be the least integer greater than* 1 *such that* $\mathbb{T}_{s^*}^{\Pi_n} = e_{i,s^*}$, *if such an integer exists, where* $\Pi_n = \Pi_n(\mathbb{T}_1)$. *Then for* $k \leq s^*$, *or all integers* $k > 0$ *if* $s^*$ *does not exist, all elements of Ker* $\Lambda^i_{k,1}$ *have prime period* $\Pi_n$ *under* $\mathbb{T}_k$. *For* $k > s^*$ *the elements of*

$$C^i_{k,k-s^*+1} \cup C^i_{k,k-s^*+2} \cup \ldots \cup C^i_{k,k-1} \cup \{0\}$$

*have prime period* $\Pi_n$ *under* $\mathbb{T}_k$ *while the elements of* $C^i_{k,k-s^*+1-j}$ *have prime period* $p^j\Pi_n$ *under* $\mathbb{T}_k$, $1 \leq j \leq k - s^*$.

Proof:

For $k \leq s^*$, or all integers $k > 0$ if $s^*$ does not exist, any $\alpha \in \text{Ker } \Lambda^i_{k,1}$ satisfies $\mathbb{T}^{\Pi_n}_k \alpha = \alpha$ hence, where $\alpha = p^\mu \hat{\alpha}$ and $\hat{\alpha}$ is a unit and $1 \leq \mu < k$, $\mathbb{T}^{\Pi_n}_k p^\mu \hat{\alpha} = p^\mu \hat{\alpha}$. Suppose there is an integer $J$, $1 \leq J \leq \Pi_n$, such that $\mathbb{T}^J_k p^\mu \hat{\alpha} = p^\mu \hat{\alpha}$, then

$$(\mathbb{T}^J_k - e_{i,k}) p^\mu \hat{\alpha} = 0 \Rightarrow p^{k-\mu} | \mathbb{T}^J_k - e_{i,k} \Rightarrow \Lambda^i_{k,1}(\mathbb{T}^J_k - e_{i,k}) = 0 \Rightarrow \mathbb{T}^J_1 - e_{i,1} = 0,$$

contradicting the minimality of $\Pi_n$. If $k > s^*$ and $\alpha \in C^i_{k,k-s^*+1} \cup C^i_{k,k-s^*+2} \cup \ldots \cup C^i_{k,k-1} \cup \{0\}$ then an entirely similar argument yields the result. If $\alpha \in C^i_{k,k-s^*+1-j}$, $0 < j < k - s^*$, we have by lemma 5.2.2 that, with $\alpha = p^{k-s^*+1-j}\hat{\alpha}$ where $\hat{\alpha}$ is a unit, $\mathbb{T}^{p^j \Pi_n}_k p^{k-s^*+1-j}\hat{\alpha} = p^{k-s^*+1-j}\hat{\alpha}$. If there is an integer $J$, $0 < J < p^j \Pi_n$, such that $\mathbb{T}^J_k \alpha = \alpha$ then

$$\begin{aligned}
(\mathbb{T}^J_k - e_{i,k}) p^{k-s^*+1-j}\hat{\alpha} &= 0 \\
\Rightarrow \quad p^{s^*+j-1} | \mathbb{T}^J_k - e_{i,k} & \\
\Rightarrow \quad \Lambda^i_{k,s^*+j-1}(\mathbb{T}^J_k - e_{i,k}) &= 0 \\
\Rightarrow \quad \mathbb{T}^J_{s^*+j-1} - e_{i,s^*+j-1} &= 0,
\end{aligned}$$

but, by lemma 5.2.1, $\Pi_n(\mathbb{T}_{s^*+j-1}) = p^j \Pi_n$, hence we have arrived at a contradiction and the result holds. ■

We can now write down the cycle set of a unit $\mathbb{T}_k \in e_{i,k} \frac{\mathbb{Z}_{/p^k}[x]}{(x^n-1)\mathbb{Z}_{/p^k}[x]}$ when $p$ and $n$ are coprime.

**Theorem 5.2.2** *Under the conditions of theorem 5.2.1 if $k < s^*$ or for all integers $k > 0$ if $s^*$ does not exist one has*

$$\Sigma(\mathbb{T}_k) = 1[1] + \frac{p^{kd_i} - 1}{\Pi_n}[\Pi_n].$$

*If $s^*$ exists then*

$$\Sigma(\mathbb{T}_{s^*}) = 1[1] + \frac{p^{(s^*-1)d_i} - 1}{\Pi_n}[\Pi_n] + \frac{p^{s^* d_i} - p^{(s^*-1)d_i}}{p\Pi_n}[p\Pi_n]$$

*and if $k > s^*$ then*

$$\begin{aligned}
\Sigma(\mathbb{T}_k) &= 1[1] + \frac{p^{(s^*-1)d_i} - 1}{\Pi_n}[\Pi_n] + \sum_{j=1}^{k-s^*} \frac{p^{(k-j)d_i} - p^{(k-j-1)d_i}}{p^j \Pi_n}[p^j \Pi_n] \\
&\quad + \frac{p^{kd_i} - p^{(k-1)d_i}}{p^{k-s^*+1}\Pi_n}[p^{k-s^*+1}\Pi_n],
\end{aligned}$$

*where* $\Pi_n = \Pi_n(\Lambda^i_{k,1}(\mathbb{T}))$.

Proof:

In all cases the units have prime period $\Pi_n(\mathbb{T}_k)$, given by lemma 5.2.1 and are counted using lemma 5.1.14. For $k < s^*$ or all integers $k > 0$ if $s^*$ does not exist one has, using theorem 5.2.1 and lemma 5.1.14,

$$\Sigma(\mathbb{T}_k) = 1[1] + \frac{|(\mathrm{Ker}\ \Lambda^i_{k,1}) \setminus \{0\}| + p^{kd_i} - p^{(k-1)d_i}}{\Pi_n}[\Pi_n]$$

and the result follows on using corollary 5.1.2. For $k \geq s^*$ (if $s^*$ exists) then $\Pi_n(\mathbb{T}_k) = p^{k-s^*+1}\Pi_n$ by lemma 5.2.1 and the result follows in a similar manner to the above on using theorem 5.2.1, lemma 5.1.14 and lemma 5.1.12. ■

Note that putting $k = 1$ in theorem 5.2.2 gives the correct result for $e_{i,1}\frac{\mathbb{F}_p[x]}{(x^n-1)\mathbb{F}_p[x]}$.

When $N = np^r$, integer $r > 0$ and $\gcd(p, n) = 1$ the situation is more complicated and we are not able to give a general formula for the cycle set under unit $\mathbb{T} \in e^r_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$, this is because, in contrast to the case where $r = 0$ or the finite field case, the ideal consisting of all the nilpotent elements in $e^r_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$ is not principal but is generated by the elements $e^r_{i,k}p$ and $e_{i,k}R_i$. However we can still provide quite a large amount of information in general and give an example that shows how one goes about finding exact results for specific $\mathbb{T}$ and which highlights the problems caused by the non-principality of the ideal of nilpotent elements.

**Theorem 5.2.3** *For* $\mathbb{T}$ *a unit in* $e^r_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$, *let* $\mathbb{T}_1 = \Lambda^i_{k,1}(\mathbb{T})$, *then the orbit lengths of the non-zero elements of* $e^r_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$ *under* $\mathbb{T}$ *are of the form* $Lp^j$, $0 \leq j \leq S + k - 1$, *where* $L$ *is the minimum orbit length occurring for non-zero elements of* $e^r_{i,1}\frac{\mathbb{F}_p[x]}{(x^n-1)\mathbb{F}_p[x]}$ *under* $\mathbb{T}_1$ *and* $\Pi_{np^r}(\mathbb{T}_1) = Lp^S$.

Proof:

We first show that $\mathbb{T}$ has period $L$ orbits and that no non-zero element of $e^r_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$ has an orbit length less than $L$. We have that $\mathbb{T}_1 = \Lambda^i_{k,1}(\mathbb{T})$ and $\mathbb{T}_1^L - e^r_{i,1}$ is nilpotent so $\mathbb{T}_1^L - e^r_{i,1} = \alpha R_i^I$ where $\alpha$ is a unit and $p^r > I > 0$, hence

$$\mathbb{T}^L - e^r_{i,k} = e^r_{i,k}\alpha R_i^I + p\gamma,$$

for some $p\gamma \in e^r_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$, it is immediate that the element $p^{k-1}e^r_{i,k}R_i^{p^r-I}$ has period $L$ under $\mathbb{T}$. Now suppose that there is some non-zero element $a \in e^r_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$ such that $(\mathbb{T}^s - e^r_{i,k})a = 0$, where $0 < s < L$, there are two cases to consider. (i) If $a \notin \text{Ker } \Lambda^i_{k,1}$, then $\mathbb{T}^s a = a$ implies that

$$\mathbb{T}_1^s \Lambda^i_{k,1}(a) = \Lambda^i_{k,1}(a) \neq 0$$

which contradicts the minimality of $L$ for $\mathbb{T}_1$. (ii) If $a \in \text{Ker } \Lambda^i_{k,1} \setminus \{0\}$ then $a = p^v \hat{a}$ for some $\hat{a} \notin \text{Ker } \Lambda^i_{k,1}$ and $0 < v \leq k-1$. Then

$$\begin{aligned}(\mathbb{T}^s - e^r_{i,k})p^v\hat{a} = 0 \quad &\Rightarrow \quad (\mathbb{T}^s - e^r_{i,k})\hat{a} \in \text{Ker } \Lambda^i_{k,1} \\ &\Rightarrow \quad \mathbb{T}_1^s \Lambda^i_{k,1}(\hat{a}) = \Lambda^i_{k,1}(\hat{a}) \neq 0,\end{aligned}$$

again contradicting the minimality of $L$ for $\mathbb{T}_1$.

Now suppose that $\sigma$ is the prime period of some non-zero element $a$ so that

$$(\mathbb{T}^\sigma - e^r_{i,k})a = 0, \quad \sigma \text{ minimal.}$$

We show that $\sigma = Lp^j$ with $0 \leq j \leq S + k - 1$. From lemma 5.2.1 we know that $\sigma | \Pi_{np^r}(\mathbb{T}) = p^{J+S}L$ where $0 \leq J < K$, again there are two cases. (i) If $a \notin \text{Ker } \Lambda^i_{k,1}$, then $\mathbb{T}^\sigma a = a$ implies that

$$\mathbb{T}_1^\sigma \Lambda^i_{k,1}(a) = \Lambda^i_{k,1}(a) \neq 0$$

so if $(\phi_{\Lambda^i_{k,1}(a)})_0 = Lp^\iota$, $0 \leq \iota \leq S$, then $Lp^\iota | \sigma$ hence $\sigma = uLp^\iota$ and $p^{J+S}\not\!L = v\sigma$ for some integers $u, v > 0$, hence $p^{J+S}\not\!L = vuLp^\iota$ hence $vu = p^{J+S-\iota}$, thus $v$ and $u$ must both be powers of $p$, hence $\sigma = Lp^{\iota+i_u}$, where $u = p^{i_u}$, and clearly $0 \leq \iota + i_u < S + k - 1$. (ii) If $a \in \text{Ker } \Lambda^i_{k,1} \setminus \{0\}$ then $a = p^v\hat{a}$ for some $\hat{a} \notin \text{Ker } \Lambda^i_{k,1}$ and $0 < v \leq k-1$. Hence one finds that $(\mathbb{T}^\sigma - e^r_{i,k})\hat{a} \in \text{Ker } \Lambda^i_{k,1}$ and the same argument as in case (i) gives $\sigma = Lp^j$, $\iota \leq j \leq J + S$ where $(\phi_{\Lambda^i_{k,1}(\hat{a})})_0 = Lp^\iota$. ■

**Definition 5.2.1** *The p−reduction of* $a \in e^r_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]} \setminus \{0\}$ *is*

$$P(a) = \begin{cases} a & \text{if } a \notin \text{Ker } \Lambda^i_{k,1}; \\ \\ \hat{a} & \text{if } a \in \text{Ker } \Lambda^i_{k,1}, a = p^v\hat{a}, \hat{a} \notin \text{Ker } \Lambda^i_{k,1}. \end{cases}$$

Thus if $(\phi_{\Lambda^i_{k,1}(P(a))})_0 = Lp^\iota$ the proof of theorem 5.2.3 shows that $Lp^\iota|(\phi_a)_0$. With $\mathbb{T} = \mathbb{T}_k$, let $\{\mathbb{T}_K\}_{1\leq K\leq k}$ be such that $\mathbb{T}_K = \Lambda^i_{k,K}(\mathbb{T}_k)$. Let $s^*$ be the least integer less than or equal to $k$ such that $\mathbb{T}^{Lp^S}_{s^*} \neq e^r_{i,s^*}$, if such an integer exists, otherwise set $s^* = k$, then by lemma 5.2.2 the elements of $C^i_{k,k-s^*} \cup \ldots \cup C^i_{k,k-1}$ have orbit lengths dividing $Lp^S$ and of those elements

$$(s^* - 1)(p^{p^r d_i} - p^{Jp^{S-1}d_i})$$

are such that their $p-$reductions are on orbits of length $Lp^S$,where

$$J = \begin{cases} \mathcal{I}_i(\mathbb{T}^L_1 - e^r_{i,1}) & \text{if } \mathcal{I}_i(\mathbb{T}^L_1 - e^r_{i,1}) < p^r \\ \\ 0 & \text{if } \mathcal{I}_i(\mathbb{T}^L_1 - e^r_{i,1}) = p^r \end{cases}$$

and deg $R_i(x) = d_i$ and we have used theorem 3.3.2 and $\mathcal{I}_i(\alpha) = \mathcal{I}_i(\epsilon_i(\alpha))$ for any $\alpha \in \frac{\mathbb{F}_p[x]}{(x^{np^r}-1)\mathbb{F}_p[x]}$. Hence, by the comments above, all such elements are on orbits of length $Lp^S$ under $\mathbb{T}$. For all other elements the orbit length of the $p-$reduction provides a lower bound on the orbit length and for elements of Ker $\Lambda^i_{k,1}$ not considered above lemma 5.2.2 can provide a better upper bound on the orbit length than $\Pi_{np^r}(\mathbb{T})$. The following example, whilst comparatively simple, illustrates the complications caused by the fact that the ideal of nilpotent elements is not principal.

**Example 5.2.1**

Let $p = 2$, $k = 2$ and $r = 1$ and suppose that deg $R_i(x) = d$ and that unit $\mathbb{T}$ is such that

$$\mathbb{T}^L - e^1_{i,2} = \alpha e^1_{i,2} R_i + 2\beta e^1_{i,2}$$

where $\alpha e^1_{i,2} R_i$ and $\beta e^1_{i,2}$ are canonical pre-images and $\beta e^1_{i,2}$ is a unit. We wish to determine the cycle set of $\mathbb{T}$, we begin by determining how many elements are on orbits of length $L$. Clearly $2\gamma e^1_{i,2} R_i$ is fixed by $\mathbb{T}^L$ for each canonical pre-image $\gamma e^1_{i,2} R_i$, by lemma 3.3.9 there are $|\mathcal{D}_{R_i}(2d-1, 1)| = 2^d - 1$ such elements. Suppose $\gamma$ is any nilpotent element in $e^1_{i,2}\frac{\mathbb{Z}_{/4}[x]}{(x^{2n}-1)\mathbb{Z}_{/4}[x]}$, barring those considered above, then

$$\gamma = f R_i e^1_{i,2} + 2g R^j_i e^1_{i,2}$$

where $j \in \{0,1\}$ and $fR_ie^1_{i,2} \neq 0$ if $j = 1$. Then $\mathbb{T}^L\gamma = \gamma$ implies that

$$2\alpha\alpha_1 fe^1_{i,2}R_i + 2\alpha g e^1_{i,2}R_i^{1+j} + 2f\beta e^1_{i,2}R_i = 0$$

where we have used $e^1_{i,2}R_i^2 = 2\alpha_1 e^1_{i,2}R_i$ for some unit $\alpha_1 e^1_{i,2}$ (by remark 5.1.4), compare this to the $k = 1$ case. When $j = 1$ this reduces to

$$2fe^1_{i,2}R_i(\alpha\alpha_1 e^1_{i,2} + \beta e^1_{i,2}) = 0,$$

hence $fe^1_{i,2}R_i(\alpha\alpha_1 e^1_{i,2} + \beta e^1_{i,2}) \in \text{Ker } \Lambda^i_{2,1}$. Now, as $fR_ie^1_{i,2} \neq 0$, $fe^1_{i,2}$ must be a unit and hence we have $e^1_{i,2}R_i(\alpha\alpha_1 e^1_{i,2} + \beta e^1_{i,2}) \in \text{Ker } \Lambda^i_{2,1}$ which is independent of $\gamma$, thus if $e^1_{i,2}R_i(\alpha\alpha_1 e^1_{i,2} + \beta e^1_{i,2}) \in \text{Ker } \Lambda^i_{2,1}$ then all $\gamma$ with $j = 1$ have orbit length $L$ under $\mathbb{T}$, including $gR^j_ie^1_{i,2}$ there are $(2^d-1)2^d$ such elements. If $e^1_{i,2}R_i(\alpha\alpha_1 e^1_{i,2}+\beta e^1_{i,2}) \notin \text{Ker } \Lambda^i_{2,1}$ then $\alpha\alpha_1 e^1_{i,2} + \beta e^1_{i,2}$ is a unit and no $\gamma$ of the above form, with $j = 1$, has orbit length $L$.

Now suppose that $j = 0$, then we have

$$2e^1_{i,2}R_i(\alpha\alpha_1 f + \alpha g + \beta f) = 0$$

hence we require $e^1_{i,2}R_i(\alpha\alpha_1 f + \alpha g + \beta f) \in \text{Ker } \Lambda^i_{2,1}$ and thus, applying $\Lambda^i_{2,1}$, that

$$fe^1_{i,1}R_i(\alpha\alpha_1 + \beta) = -\alpha g R_i e^1_{i,1}. \tag{5.2.1}$$

If $\alpha\alpha_1 e^1_{i,2} + \beta e^1_{i,2}$ is a unit then so is $e^1_{i,1}(\alpha\alpha_1 + \beta)$ and in this case for each choice of $ge^1_{i,1}$ there will only one $e^1_{i,1}fR_i$ satisfying (5.2.1). The $ge^1_{i,1}$ are units or zero, but we can exclude zero is that case implies that $e^1_{i,1}fR_i = 0$ thus $\gamma = 0$. Hence there are $|U_p(R_i,1)| = 2^d(2^d-1)$ such $\gamma$. When $e^1_{i,1}(\alpha\alpha_1 + \beta)$ is not a unit one has

$$2e^1_{i,2}fR_i(\alpha\alpha_1 + \beta) = 0 = -2\alpha g e^1_{i,2}R_i,$$

and, as $ge^1_{i,1}$ is a unit or zero it must be zero for this to hold, and we have already covered that case. To summarise, there are two cases: $e^1_{i,1}(\alpha\alpha_1 + \beta)$ is a unit and $e^1_{i,1}(\alpha\alpha_1 + \beta)$ is not a unit, however adding up the solutions we have found to $(\mathbb{T}^L - e^1_{i,2})\gamma = 0$ we find in both cases that there are exactly $2^{2d} - 1$ elements on orbits of length $L$, unless $L = 1$ when we include 0.

One finds that $\mathbb{T}^{2L} - e^1_{i,2} = 2\alpha R_i e^1_{i,2}(\alpha\alpha_1 + e^1_{i,2})$ which is zero if and only if $\alpha R_i e^1_{i,2}(\alpha\alpha_1 + e^1_{i,2}) \in \text{Ker } \Lambda^i_{2,1}$ if and only if $e^1_{i,1}\alpha\alpha_1 + e^1_{i,2}$ is nilpotent. When $\mathbb{T}^{2L} - e^1_{i,2} \neq 0$ it is clear that all the nilpotent elements not already accounted for will be on orbits of length $2L$, using (5.1.5) we see that there are $2^{3d} - 2^{2d}$ such elements and the elements on orbits of length $4L$ are the units, of which there are $2^{4d} - 2^{3d}$. Thus when $e^1_{i,1}(\alpha\alpha_1 + \beta)$ is nilpotent one has

$$\Sigma(\mathbb{T}) = 1[1] + \frac{2^{2d} - 1}{L}[L] + \frac{2^{4d} - 2^{2d}}{2L}[2L],$$

and when $e^1_{i,1}(\alpha\alpha_1 + \beta)$ is a unit

$$\Sigma(\mathbb{T}) = 1[1] + \frac{2^{2d} - 1}{L}[L] + \frac{2^{3d} - 2^{2d}}{2L}[2L] + \frac{2^{4d} - 2^{3d}}{4L}[4L].$$

We consider a particular case, let $a_i \mapsto a_{i-1} + a_{i+1}$ be the local rule of an additive cellular automata with state alphabet $\mathbb{Z}_{/4}$, and let $N = 6$ so that we are considering, using example 5.1.2,

$$\frac{\mathbb{Z}_{/4}[x]}{(x^6 - 1)\mathbb{Z}_{/4}[x]} \cong e^1_{1,2}\frac{\mathbb{Z}_{/4}[x]}{(x^6 - 1)\mathbb{Z}_{/4}[x]} \times e^1_{2,2}\frac{\mathbb{Z}_{/4}[x]}{(x^6 - 1)\mathbb{Z}_{/4}[x]},$$

where

$$\begin{aligned} e^1_{1,2} &= 3(1 + x^2 + x^4) + (x^6 - 1)\mathbb{Z}_{/4}[x], \\ e^1_{2,2} &= 2 + x^2 + x^4 + (x^6 - 1)\mathbb{Z}_{/4}[x], \end{aligned}$$

and the stated local rule has representative

$$\mathbb{T} = x + x^5 + (x^6 - 1)\mathbb{Z}_{/4}[x].$$

One finds that the image of $\mathbb{T}$ in $e^1_{1,2}\frac{\mathbb{Z}_{/4}[x]}{(x^6-1)\mathbb{Z}_{/4}[x]}$ is nilpotent, whereas the image of $\mathbb{T}$ in $e^1_{2,2}\frac{\mathbb{Z}_{/4}[x]}{(x^6-1)\mathbb{Z}_{/4}[x]}$ is

$$\hat{\mathbb{T}} = 3x + 2x^3 + 3x^5 + (x^6 - 1)\mathbb{Z}_{/4}[x].$$

We note that $R_2(x) = 1 + x + x^2$ and find that

$$\epsilon_2(\Lambda^2_{2,1}(\hat{\mathbb{T}})) = x^3 + R_2(x)^2\mathbb{F}_2[x],$$

a unit hence $\hat{\mathbb{T}}$ is a unit. Moreover $x^3 - 1 = (x-1)R_2(x)$ in $\mathbb{F}_2[x]$ hence $\epsilon_2(\Lambda^2_{2,1}(\hat{\mathbb{T}} - 1))$ is nilpotent thus $L = 1$ and $\hat{\mathbb{T}} - e^1_{2,2}$ is nilpotent, one finds that, in terms of canonical pre-images,

$$\hat{\mathbb{T}} - e^1_{2,2} = e^1_{2,2}(x)(x-1)R_2(x) + 2e^1_{2,2}(x)x^3 + (x^6 - 1)\mathbb{Z}_{/4}[x],$$

which is of the general form considered above. One finds that

$$e^1_{2,2}R^2_2 = 2(x^2+1)R_2(x) + (x^6-1)\mathbb{Z}_{/4}[x],$$

and that

$$(x-1)(x^2+1) + e^1_{2,2}(x) + (x^6-1)\mathbb{Z}_{/4}[x] = 1 + x + x^3 + x^4 + (x^6-1)\mathbb{Z}_{/4}[x],$$

which is nilpotent, hence

$$\Sigma(\mathbb{T}) = \Sigma(\hat{\mathbb{T}}) = 16[1] + 120[2]. \quad \blacklozenge$$

We note that changing increasing $p$, $r$ and especially $k$ in the above example will increase the complexity of the calculations needed to determine the cycle set, and it seems difficult to write down a general formula.

## 5.3 Dynamics in $e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$ when $U \neq 0$

We first consider the case $N = n$, $\gcd(p,n) = 1$, we shall assume throughout this section that $\deg R_i(x) = d_i$.

**Lemma 5.3.1** *Let $\mathbb{T} \in e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^n-1)\mathbb{Z}_{/p^k}[x]}$ be a unit, then $\mathbb{T}$ has non-zero fixed points if and only if $\mathbb{T} = e_{i,k} + b$, $b \in \text{Ker } \Lambda^i_{k,1}$. If $\mathbb{T}$ is a unit of the form $e_{i,k} + p^\mu \hat{b}$ where $\hat{b} \notin \text{Ker } \Lambda^i_{k,1}$, then $\mathbb{T}_U$ has a fixed point if and only if $U = p^j P(U)$ where $j \geq \mu$. There are $p^{(k-\mu)d_i}$ such $U \in e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^n-1)\mathbb{Z}_{/p^k}[x]}$.*

Proof:

For any $a \in e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^n-1)\mathbb{Z}_{/p^k}[x]} \setminus \{0\}$ one has that $(\mathbb{T} - e_{i,k})a = 0$ if and only if $\mathbb{T} - e_{i,k}$ is nilpotent if and only if $\mathbb{T} - e_{i,k} \in \text{Ker } \Lambda^i_{k,1}$.

If $\mathbb{T} = e_{i,k} + p^{\mu}\hat{b}$ where $\hat{b} \notin Ker\ \Lambda^{i}_{k,1}$ and $\mathbb{T}_U$ has a non-zero fixed point $a$ then

$$\mathbb{T}a + U = a \ \Rightarrow\ -U = (\mathbb{T} - e_{i,k})a = p^{\mu}\hat{b}a,$$

hence $p^{\mu}|U$. Conversely suppose that $p^{\mu}|U$, say $U = p^{\mu+j}P(U)$ so $P(U)$ is a unit, then let $a = -p^{j}P(U)\hat{b}^{-1}$, then

$$\mathbb{T}a + U = a + p^{\mu}\hat{b}(-p^{j}P(U)\hat{b}^{-1}) + p^{\mu+j}P(U) = a.$$

As we require that $p^{\mu}|U$, $U \in$ Ker $\Lambda^{i}_{k,\mu}$, hence by corollary 5.1.2 there are $p^{(k-\mu)d_i}$ such $U$. ■

Thus whenever unit $\mathbb{T}$ has non-zero fixed points then $\mathbb{T} = e_{i,k} + p^{\mu}\hat{b}$ and by lemma 5.2.1

$$\Pi_n(e_{i,k} + p^{\mu}\hat{b}) = p^{k-\mu}. \tag{5.3.1}$$

When $\mathbb{T}_U$ has no non-zero fixed points then $\mathbb{T}$ and $\mathbb{T}_U$ are not QDS and we concentrate on this case, by lemma 5.3.1 this implies that $U = p^{j}\hat{U}$, $\hat{U}$ a unit and $0 \leq j \leq \mu$. We shall need the following lemma:

**Lemma 5.3.2** *Let* $\mathbb{T} = e_{i,k} + p^{\mu}\hat{b}$, $\hat{b}$ *a unit and* $1 \leq \mu < k$. *Then*

$$\mathbb{T}^{p^j}_{e_{i,k}}(0) = p^{j}\alpha_j$$

*where* $0 \leq j \leq k-1$ *and each* $\alpha_j$ *is a unit, and*

$$\mathbb{T}^{p^k}_{e_{i,k}}(0) = 0.$$

Proof:

For $j = 0$ the result holds with $\alpha_0 = e_{i,k}$. Suppose the result holds for some $J < k$ so that $\mathbb{T}^{p^J}_{e_{i,k}}(0) = p^{J}\alpha_J$ with $\alpha_J$ a unit, then $\mathbb{T}^{p^J} - e_{i,k} = (\mathbb{T} - e_{i,k})\mathbb{T}^{p^J}_{e_{i,k}}(0)$ hence $p^{J+\mu}|\mathbb{T}^{p^J} - e_{i,k}$ but $p^{J+\mu+1} \nmid \mathbb{T}^{p^J} - e_{i,k}$. By lemma 5.1.4

$$\mathbb{T}^{p^{J+1}} - e_{i,k} = (\mathbb{T}^{p^J} - e_{i,k})^{p} + p\eta_p(\mathbb{T}^{p^J})(\mathbb{T}^{p^J} - e_{i,k})$$

and $p \nmid \eta_p(\mathbb{T}^{p^J})$, hence $p^{J+\mu+1}|\mathbb{T}^{p^{J+1}} - e_{i,k}$ but $p^{J+\mu+2} \nmid \mathbb{T}^{p^{J+1}} - e_{i,k}$ and as $\mathbb{T}^{p^{J+1}} - e_{i,k} = (\mathbb{T} - e_{i,k})\mathbb{T}^{p^{J+1}}_{e_{i,k}}(0)$ one must have that $p^{J+1}|\mathbb{T}^{p^{J+1}}_{e_{i,k}}(0)$ but $p^{J+2} \nmid \mathbb{T}^{p^{J+1}}_{e_{i,k}}(0)$ hence the result holds for $J+1$ and thus it holds for all $j$ with $0 \leq j \leq k-1$ and the above argument also shows that $\mathbb{T}^{p^k}_{e_{i,k}}(0) = 0$. ■

**Corollary 5.3.1** *Let* $\mathbb{T} = e_{i,k} + p^{\mu}\hat{b}$, $\hat{b}$ *a unit and* $1 \leq \mu < k$ *and let* $U = p^{j}\hat{U}$, $\hat{U}$ *a unit and* $0 \leq j < \mu$. *Then*

$$(\phi_0)_U = p^{k-j}.$$

Proof:

Immediate from lemma 5.3.2. ■

**Theorem 5.3.1** *Let* $\mathbb{T} = e_{i,k} + p^{\mu}\hat{b}$, $\hat{b}$ *a unit and* $1 \leq \mu < k$ *and let* $U = p^{j}\hat{U}$, $\hat{U}$ *a unit and* $0 \leq j < \mu$. *Then*

$$\Sigma(\mathbb{T}) = \frac{p^{kd_i}}{p^{k-j}}[p^{k-j}],$$

*where* $d_i = deg\ R_i(x)$.

Proof:

By lemma 2.3.6 (and its proof) $U \sim_1 U^*$ where $U^* = U - (\mathbb{T} - e_{i,k})a$ and $m = (\phi_a)_U$ is minimal and $(\phi_0)_{U^*} = m$. Clearly $p^j | U^*$ but $p^{j+1} \nmid U^*$ hence, by corollary 5.3.1, $m = (\phi_0)_{U^*} = (\phi_0)_U = p^{k-j}$ and $j < \mu$ so $p^{k-\mu} | p^{k-j}$ hence by lemma 2.1.12, (i), $(\phi_a)_U | (\phi_0)_U$ for all $a \in e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^n-1)\mathbb{Z}_{/p^k}[x]}$ and we have shown that $(\phi_0)_U$ is minimal so $(\phi_a)_U = (\phi_0)_U = p^{k-j}$ for all $a \in e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^n-1)\mathbb{Z}_{/p^k}[x]}$. ■

We note that theorem 5.3.1 shows that for $\mathbb{T}$ with non-zero fixed points the condition of theorem 2.3.3 is satisfied so that $\mathbb{T}_U$ and $\mathbb{T}_V$ are QDS if and only if the minimal orbit length under $\mathbb{T}_U$ is the same as that under $\mathbb{T}_V$ if and only if $(\phi_0)_U = (\phi_0)_V$. We now turn our attention to the case $N = np^r$, integer $r > 0$, theorem 5.2.3 shows that in this case unit $\mathbb{T}$ has non-zero fixed points if and only if $\Lambda^i_{k,1}(\mathbb{T})$ has non-zero fixed points. As in the $U = 0$ case exact results seem difficult to obtain in general and we content ourselves with showing that the condition of theorem 2.3.3 is satisfied, *i.e.* that for any input $U$ the minimal orbit length under $\mathbb{T}_U$ divides all other orbit lengths occurring under $\mathbb{T}_U$.

**Theorem 5.3.2** *Let* $\mathbb{T} \in e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$, *a unit, where* $r > 0$, *then for any* $U \in e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^n-1)\mathbb{Z}_{/p^k}[x]}$, *the minimal orbit length under* $\mathbb{T}_U$ *divides all other orbit lengths occurring under* $\mathbb{T}_U$.

Proof:

If $\mathbb{T}$ has no non-zero fixed points then, for all $U \in e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$, $\mathbb{T}_U$ has a fixed point and the result holds trivialy. If $\mathbb{T}$ has non-zero fixed points then $L = 1$, let the minimal orbit length under $\mathbb{T}_U$ be $m$, then by lemma 2.3.6 $U \sim_1 U^*$ where $(\phi_0)_{U^*} = m$ and, by remark 2.2.1, $(\phi_{U^*})_0|(\phi_0)_{U^*}$ and by lemma 2.1.13 $(\phi_0)_{U^*}|p^k(\phi_{U^*})_0$ and by theorem 5.2.3 $(\phi_{U^*})_0 = p^j$ for some $j$, $0 \leq j \leq S + k - 1$, where $\Pi_{np^r}(\Lambda^i_{k,1}(\mathbb{T})) = p^S$. Hence we must have $(\phi_0)_{U^*} = p^{j+j^*}$, $0 \leq j^* \leq S+k-j-1$, and if $a \in e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$ is such that $(\phi_a)_0 = p^\iota$, $\iota \leq j + j^*$, then by the minimality of $(\phi_0)_{U^*}$ and lemma 2.1.12, (i), $(\phi_a)_{U^*} = (\phi_0)_{U^*}$. If $a \in e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$ is such that $(\phi_a)_0 = p^J$, $J > j + j^*$, then clearly one has $(\phi_0)_{U^*}|(\phi_0)_a$ so $(\phi_a)_{U^*} = (\phi_a)_0$ and thus $(\phi_0)_{U^*}|(\phi_a)_{U^*}$, the result follows as $\mathbb{T}_U$ and $\mathbb{T}_{U^*}$ are QDS. ■

**Corollary 5.3.2** *Let* $\mathbb{T} \in e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$, *a unit, where* $r > 0$, *then for any* $U, V \in e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^n-1)\mathbb{Z}_{/p^k}[x]}$, $\mathbb{T}_U$ *and* $\mathbb{T}_V$ *are QDS if and only if the minimal orbit length occurring under* $\mathbb{T}_U$ *is equal to that occurring under* $\mathbb{T}_V$.

Proof:

Immediate from theorem 5.3.2 and theorem 2.3.3. ■

We note that, in contrast to the finite field case, when $\mathbb{T}_U$ and $\mathbb{T}$ are not QDS it is possible for the minimal orbit length under $\mathbb{T}_U$ and the maximal orbit length under $\mathbb{T}_U$ to be different. Also note that the proof of theorem 5.3.2 also shows that all orbit lengths occurring under $\mathbb{T}_U$ divide the maximum orbit length occurring under $\mathbb{T}_U$

## 5.4 Additive cellular automata over $\mathbb{Z}_{/p^k}$

In this section we combine results from earlier in the chapter to obtain results for $\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$ and hence for additive cellular automata on $N$ cells with periodic boundary conditions and state alphabet $\mathbb{Z}_{/p^k}$. This section follows similar lines to chapter 4, sections 4.2 and 4.3, however results like corollary 4.2.2 and corollary 4.2.4 are lacking, this is not because such results do not exist, for they may well exist, though probably in weaker forms, but because they are much harder to find in the present case and we have not pursued them at this time.

Throughout the rest of this section we take $N = np^r$ where $r \in \mathbf{N}$ and $\gcd(p, n) = 1$, we recall from theorem 5.1.1 that

$$\begin{aligned} \frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]} &\cong \prod_{i=1}^{m} e_{i,k}^r \frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]} \\ a &\mapsto (ae_{1,k}^r, \ldots, ae_{m,k}^r) \end{aligned} \tag{5.4.1}$$

and for $1 \leq i \leq m$

$$e_{i,k}^r \frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]} \xrightarrow{\Lambda_{k,1}^i} e_{i,1}^r \frac{\mathbb{F}_p[x]}{(x^{np^r}-1)\mathbb{F}_p[x]} \overset{\epsilon^{-1}}{\cong} \frac{\mathbb{F}_p[x]}{R_i(x)^{p^r}\mathbb{F}_p[x]}. \tag{5.4.2}$$

The degree of $R_i(x)$, $1 \leq i \leq m$, will be denoted by $d_i$ and as in chapter 4 we set $M = \{1, \ldots, m\}$ and write the image of any $a \in \frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$ under the isomorphism of (5.4.1) as $\{a_i\}$. We shall identify across the isomorphism and use $\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$ and $\prod_{i=1}^m e_{i,k}^r \frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$ interchangeably without further comment. Given a unit $\mathbb{T}_i \in e_{i,k}^r \frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$ we shall write $L_i$ for the minimal orbit length of any non-zero element under $\mathbb{T}_i$, then by theorems 5.2.2 and 5.2.3 this is exactly the minimal orbit length of any non-zero element of $e_{i,1}^r \frac{\mathbb{F}_p[x]}{(x^{np^r}-1)\mathbb{F}_p[x]}$ under $\Lambda_{k,1}^i(\mathbb{T}_i)$, calculated by the methods of chapters 3 and 4, similarly $S_i$ is the integer $S(\Lambda_{k,1}^i(\mathbb{T}_i))$ for the $\mathbb{F}_p$ case (and $S_i = 0$ always when $r = 0$). As usual we shall write $\Pi_{np^r}(\mathbb{T}_i)$ for the maximum orbit length occurring under $\mathbb{T}_i$ *etc.*.

We wish to define $(x^n - 1)$-sets as we did in chapter 4, however we need to make a slightly modified definition:

**Definition 5.4.1** *A $(x^n-1)$-set is a set $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$ such that $\mathbb{T}_r \in \frac{\mathbb{Z}_{/p^k}[x]}{(x^n-1)\mathbb{Z}_{/p^k}[x]}$ for each $r \in \mathbb{N}$ and for each $r \in \mathbb{N}$*

$$\Gamma_{r+1,r}^k(\mathbb{T}_{r+1}) = \mathbb{T}_r.$$

Given an $(x^n - 1)$-set $\{\mathbb{T}_r\}_{r\in\mathbf{N}}$ we define the $m$ *associated* $e_{i,k}$-sets to be

$$\{\mathbb{T}_{r,i}\}_{r\in\mathbf{N}} = \{E_r^i(\mathbb{T}_r)\}_{r\in\mathbf{N}} = \{e_{i,k}^r \mathbb{T}_r\}_{r\in\mathbf{N}}$$

for each $i \in M$.

**Lemma 5.4.1** *Let* $f : a_i \mapsto \sum_{s=-l}^{l} \alpha_s a_{i+s}$ *be the local rule of an additive cellular automata over* $\mathbb{Z}_{/p^k}$ *and let* $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$ *be such that* $\mathbb{T}_r$ *is the representative of* $f$ *on* $np^r$ *cells with periodic boundary conditions. Then* $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$ *is an* $(x^n-1)$*-set.*

Proof:

This follows because lemma 4.1.1 holds over $\mathbb{Z}_{/p^k}$ (and indeed over any commutative ring) as its proof did not use any properties peculiar to finite fields, thus the lemma holds in exactly the same manner as lemma 4.2.2. ■

**Definition 5.4.2** *Let* $f$ *be the local rule of an additive cellular automata over* $\mathbb{Z}_{/p^k}$*, let* $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$ *be the* $(x^n-1)$*-set consisting of the representatives of* $f$ *on* $np^r$ *cells,* $r \in \mathbb{N}$*, then* $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$ *is the* $(x^n-1)$*-set of* $f$ *and the associated* $e_{i,k}$ *sets are the* $e_{i,k}$*-sets of* $f$ *on* $np^r$ *cells.*

**Definition 5.4.3** *Let* $f$ *be the local rule of an additive cellular automata over* $\mathbb{Z}_{/p^k}$*,* $f : a_i \mapsto \sum_{s=-l}^{l} \alpha_s a_{i+s}$*, then the reduced local rule* $f_R$ *is the local rule*

$$f_R : a_i \mapsto \sum_{s=-l}^{l} \lambda_{k,1}(\alpha_s) a_{i+s},$$

*the local rule of an additive cellular automata over* $\mathbb{F}_p$*.*

**Lemma 5.4.2** *If* $\mathbb{T} \in \frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$ *is the representative of local rule* $f$ *on* $np^r$ *cells and* $\hat{\mathbb{T}} \in \frac{\mathbb{F}_p[x]}{(x^{np^r}-1)\mathbb{F}_p[x]}$ *is the representative of local rule* $f_R$ *on* $np^r$ *cells then*

$$\hat{\mathbb{T}} = \Lambda_{k,1}(\mathbb{T}).$$

Proof:

This is a simple verification. ■

We shall not generally be considering local rules of the form

$$f : a_i \mapsto \sum_{j=-l}^{l} \alpha_j a_{i+j}, \quad \text{each } \alpha_j \in \text{Ker } \lambda_{k,1}, \tag{5.4.3}$$

for such rules are clearly nilpotent, with $f^k$ being the zero rule, note that for such a rule $f_R$ is the zero rule and conversely if $f_R$ is the zero rule then $f$ must be the zero rule or of the form (5.4.3). Lemma 5.4.2 shows that given the $(x^n-1)$-set, $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$,

of a local rule of an additive cellular automata $f$ over $\mathbb{Z}_{/p^k}$ we have the corresponding $(x^n-1)$-set of local rule $f_R$ over $\mathbb{F}_p$, $\{\Lambda_{k,1}(\mathbb{T}_r)\}_{r\in\mathbb{N}}$.

**Lemma 5.4.3** *Let $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$ be the $(x^n-1)$-set of an additive cellular automata over $\mathbb{Z}_{/p^k}$, $k>1$, then the following statements are equivalent:*

(i) $\mathbb{T}_r$ *is reversible for all* $r\in\mathbb{N}$;

(ii) $\mathbb{T}_0$ *is reversible;*

(iii) $\Lambda_{k,1}(\mathbb{T}_0)$ *is reversible.*

*The same holds with reversible replaced with irreversible.*

Proof:

Recall that $\mathbb{T}_r$ is reversible as a cellular automata if and only if $\mathbb{T}_r$ is a unit. That $\mathbb{T}_r$ is reversible if and only if $\Lambda_{k,1}(\mathbb{T}_r)$ is reversible follows from lemma 5.1.1, $\Lambda_{k,1}(\mathbb{T}_r)$ is reversible if and only if $\Lambda_{k,1}(\mathbb{T}_0)$ is reversible, by lemma 5.4.2 and corollary 4.2.1, and $\Lambda_{k,1}(\mathbb{T}_0)$ is reversible if and only if $\mathbb{T}_0$ is reversible, by lemma 5.1.1. Similarly with reversible replaced by irreversible. ■

Thus, as in the $\mathbb{F}_{p^q}$ case, an additive cellular automata over $\mathbb{Z}_{/p^k}$ is reversible on $np^r$ cells, any $r\in\mathbb{N}$, if and only if it is reversible on $n$ cells. Moreover we can test for reversibility by looking at the representative of the reduced local rule over $\mathbb{F}_p$ on $n$ cells.

As in the finite field case we define

$$\begin{aligned} M_0^r(\mathbb{T}) &= \{j\in M : \mathbb{T}_j \text{ is nilpotent}\};\\ M_1^r(\mathbb{T}) &= \{j\in M\setminus M_0^r(\mathbb{T}) : \mathbb{T}_j - e_{i,k}^r \text{ is nilpotent}\}, \end{aligned}$$

one sees immediately that

$$M_0^r(\mathbb{T}) = M_0^r(\Lambda_{k,1}(\mathbb{T})); \tag{5.4.4}$$

$$M_1^r(\mathbb{T}) = M_1^r(\Lambda_{k,1}(\mathbb{T})). \tag{5.4.5}$$

It follows from lemma 4.2.3 and lemma 5.4.2 that if $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$ is the $(x^n-1)$-set of an additive cellular automata over $\mathbb{Z}_{/p^k}$ then for each $r\in\mathbb{N}$

$$M_0^r(\mathbb{T}_r) = M_0^0(\Lambda_{k,1}(\mathbb{T}_0)); \tag{5.4.6}$$

$$M_1^r(\mathbb{T}_r) = M_1^0(\Lambda_{k,1}(\mathbb{T}_0)), \tag{5.4.7}$$

in this case we shall write $M_0(\mathbb{T})$ and $M_1(\mathbb{T})$ for $M_0^0(\Lambda_{k,1}(\mathbb{T}_0))$ and $M_1^0(\Lambda_{k,1}(\mathbb{T}_0))$ respectively.

We have the analogue of lemma 4.2.4 for the present case.

**Lemma 5.4.4** *Let $f$ be the local rule of an additive cellular over $\mathbb{Z}_{/p^k}$ such that $f_R$ is not the zero rule. Let $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$ be the $(x^n-1)$-set of $f$. If $M_0(\mathbb{T}) \neq \emptyset$ then for any $i \in M_0(\mathbb{T})$ the associated $e_{i,k}$-set is non-trivial.*

Proof:
As $f_R$ is not the zero rule the result follows from lemma 4.2.4 and lemma 5.4.2. ■

We shall denote the set of units in $\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$ by $U(p^k,N)$ (rather than $U_{p^k}(N)$ which could cause confusion with the finite field case) and the set of zero-divisors by $ZD(p^k,N)$.

**Lemma 5.4.5** *For any $r \in \mathbb{N}$ one has*

$$|U(p^k,n)| = p^{(k-1)n}\prod_{i=1}^{m}(p^{d_i}-1), \qquad |U(p^k,np^r)| = p^{(p^r-1)kn}|U(p^k,n)|$$

$$|ZD(p^k,n)| = p^{kn}-|U(p^k,n)|, \qquad |ZD(p^k,np^r)| = p^{(p^r-1)kn}|ZD(p^k,n)|.$$

Proof:

This follows from lemma 5.1.14. ■

**Lemma 5.4.6** *Let $\{\mathbb{T}_r\}_{r\in\mathbb{N}}$ be the $(x^n-1)$-set of an additive cellular automata over $\mathbb{Z}_{/p^k}$. Then*

$$Fix(\mathbb{T}_r)=\{0\} \Leftrightarrow Fix(\mathbb{T}_0)=\{0\} \Leftrightarrow M_1(\mathbb{T})=\emptyset.$$

Proof:

It is clear that $Fix(\mathbb{T}_r)=\{0\} \Leftrightarrow M_1^r(\mathbb{T}_r)=\emptyset$ but $M_1^r(\mathbb{T}_r) = M_1^0(\Lambda_{k,1}(\mathbb{T})) = M_1^0(\mathbb{T}_0)$ and the result follows. ■

As in the finite field case we can define an equivalence relation on the set of linear local rules by $f \sim_N g$ if $f$ and $g$ have the same representative on $N$ cells, we denote the equivalence class of $f$ by $[f]_N$ and say that $[f]_N$ is reversible if $\mathbb{T}_f$ is a unit *etc.*.

**Lemma 5.4.7** *On $np^r$ cells there are $p^{(kp^r-1)n}\prod_{j\in M}(p^{d_i}-1) \sim_{np^r}$ equivalence classes with no non-zero fixed points, of which $p^{(kp^r-1)n}\prod_{j\in M}(p^{d_i}-2)$ are reversible.*

Proof:

This follows from lemma 5.4.6 annd lemma 4.2.7 by counting pre-images and using (5.1.5). ■

**Corollary 5.4.1** *When $p = 2$ any additive cellular automata which is reversible on $N$ cells has non-zero fixed points on $N$ cells.*

Proof:

Follows from lemma 5.4.7 on putting $p = 2$ and noting that at least one of the $d_i$. $1 \leq i \leq m$, is equal to 1. ■

Given $\mathbb{T} \in \frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$ if $j \in M \setminus M_0^r(\mathbb{T})$ define $s_j^*$ as follows: Let $\Pi_{np^r}^j = \Pi_{np^r}(\Lambda_{k,1}^j(\mathbb{T}_j))$, then if $\mathbb{T}_j^{\Pi_{np^r}^j} \neq e_{j,k}^r$ let $(\mathbb{T}_j)_i = \Lambda_{k,i}^j(\mathbb{T}_j)$, $2 \leq i \leq k$, then $s_j^*$ is the least such $i$ with $(\mathbb{T}_j)_i^{\Pi_{np^r}^j} \neq e_{j,i}^r$. If $\mathbb{T}_j^{\Pi_{np^r}^j} = e_{j,k}^r$ then set $s_j^* = k+1$. From lemma 5.2.1 we have that $\Pi_{np^r}(\mathbb{T}_j) = p^{k-s_j^*+1}\Pi_{np^r}^j$. The following theorem describes the maximal cycle length and the invariant set of an additive cellular automata over $\mathbb{Z}_{/p^k}$ on $np^r$ cells.

**Theorem 5.4.1** *Let* $\mathbb{T} \in \frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$, *then*

(i) $\Pi_{np^r}(\mathbb{T}) = p^{k-s^*+1}\Pi_{np^r}(\Lambda_{k,1}(\mathbb{T}))$, *where $s^*$ is the minimum of the $s_j^*$, $j \in M \setminus M_0^r(\mathbb{T})$.*

(ii) $Att(\mathbb{T}) = \{a : a_i = 0 \ \forall \ i \in M_0^r(\mathbb{T})\}$ *and*

$$|Att(\mathbb{T})| = p^{kp^r \sum_{j \in M \setminus M_0^r(\mathbb{T})} d_i} = |Att(\Gamma_{r,0}^k(\mathbb{T}))|^{p^r}.$$

Proof:

(i) We have

$$\begin{aligned}
\Pi_{np^r}(\mathbb{T}) &= \mathrm{lcm}_{j \in M \setminus M_0^r(\mathbb{T})}(\Pi_{np^r}(\mathbb{T}_j) \\
&= \mathrm{lcm}_{j \in M \setminus M_0^r(\mathbb{T})}(p^{k-s_j^*+1}\Pi_{np^r}(\Lambda_{k,1}^j(\mathbb{T}_j))) \\
&= p^{k-s^*+1}\mathrm{lcm}_{j \in M \setminus M_0^r(\mathbb{T})}(\Pi_{np^r}(\Lambda_{k,1}^j(\mathbb{T}_j))) \\
&= p^{k-s^*+1}\Pi_{np^r}(\Lambda_{k,1}(\mathbb{T}))
\end{aligned}$$

by lemma 5.4.2 and lemma 4.2.8.

(ii) That $Att(\mathbb{T}) = \{a : a_i = 0 \forall i \in M_0^r(\mathbb{T})\}$ is clear, it follows that, using lemma 5.1.11, $|Att(\mathbb{T})| = p^{kp^r \sum_{j \in M \setminus M_0^r(\mathbb{T})} d_i}$ and as $M_0^r(\mathbb{T}) = M_0^0(\Gamma_{r,0}^k(\mathbb{T}))$ it follows that $|Att(\mathbb{T})| = |Att(\Gamma_{r,0}^k(\mathbb{T}))|^{p^r}$. ■

It is clear that, with $s^*$ as defined in theorem 5.4.1, if $s^* \neq k+1$ then $s^*$ is the least integer greater than 1 such that

$$(\Lambda_{k,s^*}(\mathbb{T}))^{\Pi_{np^r}(\Lambda_{k,1}(\mathbb{T}))} \neq 1, \tag{5.4.8}$$

hence if all one is interested in is $\Pi_{np^r}(\mathbb{T})$ then it is easier to calculate $s^*$ using (5.4.8) rather than by calculating the $s_j^*$ and finding their minimum.

The analysis of corollary 4.2.5 clearly still holds in the present case, that is if an additive cellular automata is irreversible on $n$ cells then the fraction of configurations on cycles on $np^r$ cells vanishes as $r \longrightarrow \infty$.

If one can find the $\Sigma(\mathbb{T}_j)$, $j \in M \backslash M_0^r(\mathbb{T})$, then of course one can compute $\Sigma(\mathbb{T})$ using the cycle product. In any case it is clear that the orbit lengths occurring under $\mathbb{T}$ are of the form $p^j \mathrm{lcm}_{i \in I}(L_i)$ where $I \subseteq M$ and $0 \leq j \leq k - s^* + 1 + S$, $S = \max_{i \in M \backslash M_0^r(\mathbb{T})}(S_i)$. We know from theorem 2.1.1 that additive cellular automata over $\mathbb{Z}_{/p^k}$ with periodic boundary conditions on $N$ cells cannot have orbits of length $p^{kN} - 1$ for $N > 1$ and by the comments directly preceding theorem 2.1.1 the above is also true for $N = 1$ when $k > 1$. Of course the above is also the case when time independent inputs are allowed, we show below that in that case orbits of length $p^{kN}$ are also impossible for $N > 1$.

**Theorem 5.4.2** *Additive cellular automata with state alphabet $\mathbb{Z}_{/p^k}$ and periodic boundary conditions and time independent inputs cannot have cycles of length $p^{kN}$ on $N > 1$ cells.*

Proof:

It suffices to prove the result for units $\mathbb{T} \in \frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$, by theorem 5.4.1 one has $\Pi_{np^r}(\mathbb{T}) = p^{k-s^*+1}\Pi_{np^r}(\Lambda_{k,1}(\mathbb{T}))$ where $s^* \geq 2$, hence $\Pi_{np^r}(\mathbb{T}) \leq p^{k-1}\Pi_{np^r}(\Lambda_{k,1}(\mathbb{T})) \leq p^{k+r-1}\mathrm{lcm}_{i \in M}(L_i)$. Now by lemma 2.1.13 we have

$$(\phi_0)_U | p^k \Pi_{np^r}(\mathbb{T}) \leq p^{2k+r-1}\mathrm{lcm}_{i \in M}(L_i)$$

and $p^{2k+r-1} < p^{knp^r}$ for $np^r > 1$ unless $p = 2$ and $N = 2$. Suppose for the moment that either $p > 2$ or if $p = 2$ then $N > 2$. If $L_i = 1$ for all $i \in M$ then from the above $(\phi_0)_U < p^{knp^r}$ and the result holds, if any of the $L_i$ are greater than one the result holds by the same argument as that used in the proof of theorem 4.3.2.

Now suppose that $p = 2$ and $N = 2$, one finds that for any unit $\mathbb{T}$, $\Pi_2(\Lambda_{k,1}(\mathbb{T})) \in \{1, 2\}$. When $\Pi_2(\Lambda_{k,1}(\mathbb{T})) = 1$ then

$$(\phi_0)_U | 2^k 2^{k-s^*+1} \leq 2^{2k-1}$$

so the result holds. When $\Pi_2(\Lambda_{k,1}(\mathbb{T})) = 2$, if $s^* > 2$ then

$$(\phi_0)_U | 2^k 2^{k-s^*+1} 2 \leq 2^{2k}$$

so it suffices to show that $s^* > 2$ for any unit with $\Pi_2(\Lambda_{k,1}(\mathbb{T})) = 2$. For $k = 2$ the required units are the preimages (under $\Lambda_{2,1}$) of $x + (x^2 - 1)\mathbb{F}_2[x]$, these are

$$\begin{aligned}\mathbb{T} \in \{&x + (x^2-1)\mathbb{Z}_{/4}[x], 3x + (x^2-1)\mathbb{Z}_{/4}[x],\\ &2 + x + (x^2-1)\mathbb{Z}_{/4}[x], 2 + 3x + (x^2-1)\mathbb{Z}_{/4}[x]\}\end{aligned}$$

It is easy to check that for these choices of $\mathbb{T}$, $\Pi_2(\mathbb{T}) = 2$ and hence $s^* > 2$. ■

We now turn our attention to the case of non-zero input $U$. As usual we have from theorem 2.3.1 that $\mathbb{T}$ and $\mathbb{T}_U$ are QDS if and only if $Fix(\mathbb{T}_U) \neq \emptyset$ and thus concentrate on the case of $\mathbb{T}$ with non-zero fixed points so that $Fix(\mathbb{T}_U) = \emptyset$ is possible.

**Lemma 5.4.8** *For any* $\mathbb{T} \in \frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$, $\mathbb{T}$ *and* $\mathbb{T}_U$ *are* QDS *for all* $U \in \frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$ *if and only if* $M_1^r(\mathbb{T}) = \emptyset$.

Proof:

Follows from corollary 2.3.3 and lemma 5.4.6. ■

When $r > 0$ we do not have the necessary results at our disposal to say precisely which inputs $U$ are such that $\mathbb{T}$ and $\mathbb{T}_U$ are QDS. When $r = 0$ we know from lemma 5.3.1 that $\mathbb{T}_i$ has non-zero fixed points if and only if $\mathbb{T}_i = e_{i,k} + p^{\mu_i} b$, $b \notin \text{Ker } \Lambda^i_{k,1}$, $1 \leq \mu_i \leq k$ (we include $k$ for $\mathbb{T}_i = e_{i,k}$) and that if $\mathbb{T}_i$ is of this form then $(\mathbb{T}_i)_{U_i}$ has fixed points if and only if $U \in \text{Ker } \Lambda^i_{k,\mu_i}$. It follows that the inputs $U$ such that $\mathbb{T}$ and $\mathbb{T}_U$ are QDS are the elements of the Cartesian product

$$\prod_{i \in M_1^0(\mathbb{T})} \text{Ker } \Lambda^i_{k,\mu_i} \prod_{j \in M \setminus M_1^0(\mathbb{T})} e_{j,k} \frac{\mathbb{Z}_{/p^k}[x]}{(x^n - 1)\mathbb{Z}_{/p^k}[x]}.$$

In general we can prove the following result and content ourselves with doing so for the purposes of this publication.

**Theorem 5.4.3** *Let* $\mathbb{T}, U, V \in \frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$, *then* $\mathbb{T}_U$ *and* $\mathbb{T}_V$ *are* QDS *if and only if the minimum orbit length that occurs under* $\mathbb{T}_U$ *is equal to the minimum orbit length that occurs under* $\mathbb{T}_V$.

Proof:

This result follows from theorem 2.3.3 if we can show that, for any $U$, the minimal orbit length under $\mathbb{T}_U$ divides all other orbit lengths occurring under $\mathbb{T}_U$ which is of

course trivially true if $Fix(\mathbb{T}_U) \neq \emptyset$. In each of the rings $e^r_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$, $1 \leq i \leq m$, it is true that the minimal orbit length divides all other orbit lengths for any input, by theorems 5.3.1 and 5.3.2. Put $R_i = e^r_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$, $1 \leq i \leq m$, and consider the image of $\mathbb{T}_U$ in $R_1 \times R_2$, we know that the minimal cycle length under $(\mathbb{T}_1)_{U_1}$, $\phi_1$ say, divides all other cycle lengths occurring under $(\mathbb{T}_1)_{U_1}$ and that the minimal cycle length under $(\mathbb{T}_2)_{U_2}$, $\phi_2$ say, divides all other cycle lengths occurring under $(\mathbb{T}_2)_{U_2}$. It follows that $\text{lcm}(\phi_1, \phi_2)$ divides the lcm of every pair of cycle lengths, one occurring under $(\mathbb{T}_1)_{U_1}$ and the other under $(\mathbb{T}_2)_{U_2}$. The result now follows by induction. ■

## 5.5 Additive cellular automata over $\mathbb{Z}_{/m}$ for any integer $m > 1$

For any integer $m > 1$ we can write $m = \prod_{i=1}^{I} p_i^{k_i}$ for some integer $I > 0$ and primes $p_i$ and integers $k_i > 0$ and then from theorem 1.5.3 one has that

$$\frac{\mathbb{Z}_{/m}[x]}{(x^N-1)\mathbb{Z}_{/m}[x]} \cong \prod_{i=1}^{I} \frac{\mathbb{Z}_{/p_i^{k_i}}[x]}{(x^N-1)\mathbb{Z}_{/p_i^{k_i}}[x]}.$$

We shall denote $\frac{\mathbb{Z}_{/p_i^{k_i}}[x]}{(x^N-1)\mathbb{Z}_{/p_i^{k_i}}[x]}$ by $R_i(N)$, and will identify across the isomorphism and use $\frac{\mathbb{Z}_{/m}[x]}{(x^N-1)\mathbb{Z}_{/m}[x]}$ and $\prod_{i=1}^{I} R_i(N)$ interchangeably. Given the representative $\mathbb{T}$ of an additive cellular automata over $\mathbb{Z}_{/M}$ on $N$ cells and given any input $U$, the cycle set of $\mathbb{T}_U$ is given by

$$\Sigma(\mathbb{T}_U) = \prod_{i=1}^{I} \Sigma((\mathbb{T}_i)_{U_i})$$

and if $m$ is square free we can always calculate the $\Sigma((\mathbb{T}_i)_{U_i})$ using the methods of chapters 3 and 4. If $m$ is not square free we may not be able to compute all the $\Sigma((\mathbb{T}_i)_{U_i})$ (at least not easily) but one can still obtain a great deal of information about the behaviour of the system by using the results of chapter 5 in conjunction with those of chapters 3 and 4. For instance one can test for reversibility easily by just testing whether or not each $\mathbb{T}_i$ is a unit, which we know how to do, similarly we can compute the maximal cycle length occurring under the $\mathbb{T}_i$, $1 \leq i \leq I$, then the maximal cycle

length under $\mathbb{T}$ is just the lcm of these. If $n$ is coprime to $p_i$, $1 \leq i \leq I$, one can set up various $(x^n - 1)$ sets, corresponding to, for instance, the representatives of a given rule on $n$ cells, $np_i$ cells, $np_i^2$ cells, *etc.* or on $n$ cells, $np_ip_j$ cells, *etc.* and so forth. We will not go into further details but just note that when $m$ is square free anything that was done in chapter 4 can be done in the present case and if $m$ is not square free then anything that was done in section 5.4 of the present chapter can be done in the present case. We do present two results as examples.

**Theorem 5.5.1** *Additive cellular automata with periodic boundary conditions and state alphabet $\mathbb{Z}_{/m}$ and time independent inputs cannot have cycles of length $m^N$ on $N > 1$ cells.*

Proof:

For non-zero input $U$ and additive cellular automata represented by $\mathbb{T}$ let $\phi_m$ denote the maximum cycle length under $\mathbb{T}_U$ and let $\phi_{m,i}$ denote the maximum cycle length under $(\mathbb{T}_i)_{U_i}$ in $R_i(N)$, $1 \leq i \leq I$, then

$$\phi_m = \mathrm{lcm}_{i \in I}(\phi_{m,i}) \leq \prod_{i \in I} \phi_{m,i} \leq m^N.$$

Now $\prod_{i \in I} \phi_{m,i} = m^N$ if and only if $\phi_{m,i} = p_i^{k_i N}$ for each $i \in I$, which is only possible for $N = 1$ by theorem 4.3.2 and theorem 5.4.2. ■

**Theorem 5.5.2** *Let $\mathbb{T}, U, V \in \frac{\mathbb{Z}_{/m}[x]}{(x^N-1)\mathbb{Z}_{/m}[x]}$, then $\mathbb{T}_U$ and $\mathbb{T}_V$ are* QDS *if and only if the minimum orbit length that occurs under $\mathbb{T}_U$ is equal to the minimum orbit length that occurs under $\mathbb{T}_V$.*

Proof:

This follows from theorem 5.4.3 in the same manner as theorem 5.4.3 followed from theorems 5.3.1 and 5.3.2. ■

We note that one can generalise from state alphabet $\mathbb{Z}_{/m}$ to state alphabet $R$ where $R = \prod_{i=1}^{I} S_i$ where each $S_i$ is either a finite field or $\mathbb{Z}_{/p^k}$ for some prime $p$ and $k > 1$, in particular one can consider "vector states" where each of the $S_i$ is a copy of the same ring.

More generally, referring to appendix A, section A.1.3, we see that for any finite ring $R$ (lemma A.1.4) there is a ring monomorphism from $\mathbb{Z}/m\mathbb{Z}$ into $Z(R)$, $a + m\mathbb{Z} \mapsto a1_R$, where $m$ is the characteristic of $R$. If $m$ is composite any set of non-trivial pairwise

orthogonal idempotents in $\mathbb{Z}/m\mathbb{Z}$ maps to a set of non-trivial pairwise orthogonal idempotents in $R$ and if the sum of the idempotents in $\mathbb{Z}/m\mathbb{Z}$ is 1 then the sum of their images in $R$ will be $1_R$ hence $R$ decomposes into a direct product of rings of prime power characteristic (theorem A.5.3). Given any ring $R$ with characteristic $p^k$, some $k \geq 1$, we have a monomorphism as above into $Z(R)$, this monomorphism induces a homomorphism (see lemma A.2.3) from $\frac{\mathbb{Z}/p^k\mathbb{Z}[x]}{(x^N-1)\mathbb{Z}/p^k\mathbb{Z}[x]}$ into the center of $R_N$ for each integer $N > 0$ and one can easily show that this homomorphism is injective and thus in the same manner as above one can map idempotents to idempotents and obtain a direct product decomposition of $R_N$ from that of $\frac{\mathbb{Z}/p^k\mathbb{Z}[x]}{(x^N-1)\mathbb{Z}/p^k\mathbb{Z}[x]}$. Of course one may be able to decompose still further but the above gives a good start to the process of decomposing $R_N$ into a direct product when $R$ is any finite ring, and thus for investigating additive cellular automata with periodic boundary conditions and state alphabet $R$.

# Chapter 6

# Generalisations

In this chapter we briefly discuss two important generalisations of the work in earlier chapters. In section 6.1 we consider time dependent inputs in the case where the inputs are periodic or eventually periodic, focusing as usual on the periodic boundary condition case. The results in this section are for $R$ a general finite commutative ring, as in chapter 2. We show how the results from chapter 2 can be used to obtain results for time dependent inputs. Only periodic behaviour is considered.

Section 6.2 is a preliminary investigation of the extension of our results to two or more dimensional linear cellular automata in the periodic boundary condition case. We concentrate on the case of state alphabet a finite field (of course results from this case can then be extended using idempotent lifting to results for $\mathbb{Z}_{/p^k}$ *etc.*). We content ourselves with obtaining the direct product decomposition in this case and highlighting the similarities and differences to the one dimensional case.

## 6.1 Periodic inputs

In this section we consider non-constant periodic or eventually periodic inputs. These inputs will be represented as

$$U(t) = U(t, x) + (x^N - 1)R_N[x].$$

The obvious analogous definitions are made for null boundary conditions, and results in that case hold with the same qualifications (if any) as stated in chapter 2.

We shall see that results in this case can be obtained from those for time independent inputs. We consider only the general case as considered for time independent inputs in chapter 2, also we consider only periodic behaviour. An interesting case of periodic inputs is that of "semi-coupled" cellular automata, where the input to an additive cellular automata is supplied by one or more cellular automata running independently.

We make the following definition:

**Definition 6.1.1** *The sequence of inputs* $\{U(1), U(2), \ldots\}$ *is eventually periodic with period* $P_{U(t)} > 0$ *if there is an integer* $T_{U(t)} \geq 0$ *(the transient time), chosen to be minimal, such that*

$$U(T_{U(t)} + k + P_{U(t)}) = U(T_{U(t)} + k), \text{ all } 1 < k \leq P_{U(t)}.$$

*The sequence is periodic with period* $P_{U(t)}$ *if* $T_{U(t)} = 0$.

We shall denote the global mapping corresponding to a rule $\mathbb{T}$ acting with input sequence $U(t)$ by $\mathbb{T}_{U(t)}$. The $k-th$ iterate will be written, for any $a \in R_N$, as

$$\begin{aligned}\mathbb{T}^k_{U(t)}(a) &= \mathbb{T}_{U(k)}(\mathbb{T}_{U(k-1)}(\ldots(\mathbb{T}_{U(1)}(a))\ldots)) \\ &= \mathbb{T}^k a + \sum_{i=1}^{k} \mathbb{T}^{k-i} U(i).\end{aligned}$$

We can now examine the reoccurrence of states of the system. For time-independent inputs it is no longer sufficient to say that $a \in R_N$ is periodic with period $k$ if $\mathbb{T}^k_{U(t)}(a) = a$.

**Definition 6.1.2** *Say $a \in R_N$ is eventually periodic under $\mathbb{T}_{U(t)}$ with period $P(U(t), a)$ if there is some integer $n(a) > 0$ such that for each $k, 1 \leq k \leq P(U(t), a)$, we have*

$$\mathbb{T}^{n(a)+k+P(U(t),a)}_{U(t)}(a) = \mathbb{T}^{n(a)+k}_{U(t)}(a).$$

*When $n(a) = 0$, $a$ is said to be periodic.*

Of course, as $R_N$ is finite every element $a \in R_N$ is eventually periodic.

**Lemma 6.1.1** *For any global rule $\mathbb{T}$ and periodic input $U(t)$*

$$P_{U(t)} \mid P(U(t), a)$$

*for each $a \in R_N$ and $T_{U(t)} \leq n$ where $n$ is the maximum of the integers $n(a)$ defined in definition 6.1.2.*

Proof:

Let $T = n$, then for any $a \in R_N$ let $k = P(U(t), a)$, then $\mathbb{T}^{T+k}_{U(t)}(a) = \mathbb{T}^T_{U(t)}(a)$. Put $a_0 = a$ then we have

$$\begin{array}{ccccc}
\mathbb{T}^{T+k}_{U(t)}(a_0) & = & \mathbb{T}^{T}_{U(t)}(a_0) & = & a_T \\
\mathbb{T}^{T+k+1}_{U(t)}(a_0) & = & \mathbb{T}^{T+1}_{U(t)}(a_0) & = & a_{T+1} \\
\vdots & & \vdots & & \vdots \\
\mathbb{T}^{T+2k-1}_{U(t)}(a_0) & = & \mathbb{T}^{T+k-1}_{U(t)}(a_0) & = & a_{T+k-1} \\
\mathbb{T}^{T+2k}_{U(t)}(a_0) & = & \mathbb{T}^{T}_{U(t)}(a_0) & = & a_T
\end{array}$$

and so on, hence for $0 \leq i \leq k-1$ and all $m \in \mathbb{N}$

$$\begin{aligned} a_{T+i} &= \mathbb{T}_{u(t)}^{T+mk+i}(a_0) \\ &= \mathbb{T}^i \mathbb{T}_{U(t)}^{T+mk}(a_0) + U(T+mk+i) \\ &= \mathbb{T}^i a_T + U(T+mk+i). \end{aligned}$$

It follows that $U(T+i) = U(T+mk+i)$ for each $i$, $0 \leq i \leq k-1$ and all $m \in \mathbb{N}$ hence $P_{U(t)} \mid P(U(t), a)$ and $\mathbb{T}_{U(t)} \leqslant T = n$. ■

**Corollary 6.1.1** *For any global rule $\mathbb{T}$ and periodic input $U(t)$ there are no fixed points unless $P_{U(t)} = 1$.*

Proof:

If $P(U(t), a) = 1$ then as $P_{U(t)} | P(U(t), a)$ by lemma 6.1.1 it follows that $P_{U(t)} = 1$.

■

Consider first the case $U(t)$ periodic, *i.e.* $T_{U(t)} = 0$. Consider a cycle $C$ of length $nP_{U(t)}$ for some integer $n > 0$;

$$C = \{a, \mathbb{T}_{U(t)}(a), \ldots, \mathbb{T}_{U(t)}^{nP_{U(t)}-1}(a)\}.$$

Points on such a cycle fall into two classes, those occurring at times $t \equiv 0$ modulo $P_{U(t)}$ and those occurring at times $t \not\equiv 0$ modulo $P_{U(t)}$. Those in the first class behave as one would normally expect a periodic point to do, *i.e.* if $b = \mathbb{T}_{U(t)}^{lP_{U(t)}}(a)$ then if $b$ is taken as initial condition it evolves to the same cycle $C$. However those in the second class are different, their presence on $C$ tells us nothing about their behaviour when taken as initial conditions. We shall describe points of the first type as *primary periodic points* and those of the second type as *secondary periodic points.*

**Example 6.1.1**

Let $R = \mathbb{F}_2$, $N = 3$ and let $\mathbb{T} = 1 + x \ + (x^3 - 1)\mathbb{F}_2[x]$. Let $U(t) = (t + 1 \text{ Mod } 2)x + (x^3 - 1)\mathbb{F}_2[x]$ (so $U(2n+1) = 0, U(2n) = x$ for all positive integers $n$). Then $P_{U(t)} = 2$. We shall omit the "$+(x^3 - 1)\mathbb{F}_2[x]$" for the sake of brevity. With initial condition $x^2$ one obtains the cycle

$$x^2 \to 1 + x^2 \to x^2$$

However with $1 + x^2$ as initial condition the system evolves to the cycle

$$1 \to 1 + x \to 1 + x + x^2 \to 0 \to x \to x + x^2 \to 1$$

where the primary periodic points are $1, 1 + x + x^2, x$. ♦

We note that in this case, as $P_{U(t)}|P(U(t), a)$ the qualitative behaviour under $\mathbb{T}_{U(t)}$ is completely determined by the behaviour of the primary periodic points.

When $T_{U(t)} > 0$ we define the primary periodic points as those elements of $R_N$ that occur on cycles under $\mathbb{T}_{U(t)}$ at times $t = T_{U(t)} + LP_{U(t)}$, $L \geq 0$. It is no longer true that if $b$ is a primary periodic point then $b$ or other primary periodic points on the same cycle will evolve to that cycle if taken as initial conditions, as the following example shows.

**Example 6.1.2**

Let $R = \mathbb{F}_2$, $N = 3$, $\mathbb{T} = 1 + x + (x^3 - 1)\mathbb{F}_2[x]$. Let $U(t)$ be defined by (omiting the "$+(x^3 - 1)\mathbb{F}_2[x]$" for brevity) $U(1) = 0$, $U(2) = 1$, $U(3) = x$, $U(4 + 2i) = 1 + x$ and $U(5 + 2i) = x^2$ for each $i \geq 0$. Then $T_{U(t)} = 3$ and $P_{U(t)} = 2$. With initial condition 0 one obtains, after three time steps, the cycle

$$1 \to 0 \to x^2 \to x + x^2 \to 1 + x + x^2 \to 1 + x \to 1$$

with primary periodic points $1, x^2$ and $1 + x + x^2$. If we use $x^2$ as an initial condition we do not regain the above cycle, instead the system evolves, again after three time steps, to the cycle

$$x \to 1 + x^2 \to x. \quad ♦$$

Despite the above example the primary periodic points are still important when $T_{U(t)} > 0$ and we shall see that they still determine the qualitative behaviour of the system.

The next lemma relates the dynamics under $\mathbb{T}_{U(t)}$ to that of the cellular automata rule on $N$ cells represented by $\mathbb{T}^{P_{U(t)}}$ with a constant input, the proof can be found in appendix B.

**Lemma 6.1.2** *For the additive cellular automata rule over $R$ represented by $\mathbb{T}$ on $N$ cells, let $U(t)$ be a periodic input sequence, and let*

$$W(U) = \mathbb{T}^{P_{U(t)}-1}U(1) + \ldots + \mathbb{T}U(P_{U(t)} - 1) + U(P_{U(t)}).$$

*Then for each* $a \in R_N$ *and each integer* $n > 0$

$$\mathbb{T}_{U(t)}^{nP_{U(t)}}(a) = (\mathbb{T}^{P_{U(t)}})_{W(U)}^{n}(a).$$

*More generally let* $U(t)$ *be eventually periodic with transient time* $T_{U(t)}$ *and let*

$$W(U) = \mathbb{T}^{P_{U(t)}-1}U(T_{U(t)}+1) + \ldots + \mathbb{T}U(T_{U(t)}+P_{U(t)}-1) + U(T_{U(t)}+P_{U(t)})$$

*and let*

$$S(U) = \mathbb{T}^{T_{U(t)}-1}U(1) + \ldots + \mathbb{T}U(T_{U(t)}-1) + U(T_{U(t)}),$$

*then*

$$\mathbb{T}_{U(t)}^{T_{U(t)}+nP_{U(t)}}(a) = (\mathbb{T}^{P_{U(t)}})_{W(U)}^{n}(\mathbb{T}^{T_{U(t)}}a + S(U)),$$

*for each* $a \in R_N$ *and all integers* $n > 0$. ■

**Corollary 6.1.2** *When* $T_{U(t)} = 0$, $a \in R_N$ *is a primary periodic point of prime period* $nP_{U(t)}$ *under* $\mathbb{T}_{U(t)}$ *if and only if* $a$ *is on a cycle of length* $n$ *under* $(\mathbb{T}^{P_{U(t)}})_{W(U)}$.

Proof:

Suppose that $a \in R_n$ is a primary periodic point of $\mathbb{T}_{U(t)}$ of prime period $nP_{u(t)}$ for integer $n > 0$, then

$$\mathbb{T}_{U(t)}^{nP_{U(t)}}(a) = a \;\Rightarrow\; (\mathbb{T}^{P_{U(t)}})_{W(U)}^{n}(a) = a$$

and if there is an integer $m$, $0 < m < n$ such that $(\mathbb{T}^{P_{U(t)}})_{W(U)}^{m}(a) = a$ then $\mathbb{T}_{U(t)}^{mP_{U(t)}}(a) = a$ which contradicts the minimality of $n$. The converse is just the reverse of the above argument. ■

Thus the set of primary periodic points under $\mathbb{T}_{U(t)}$ when $T_{U(t)} = 0$ is equal to $Att((\mathbb{T}^{P_{U(t)}})_{W(U)})$, the same is true when $T_{U(t)} > 0$ as we show in the following result, the proof is in appendix B.

**Lemma 6.1.3** *When* $T_{U(t)} > 0$ *the set of primary periodic points under* $\mathbb{T}_{U(t)}$ *is equal to* $Att((\mathbb{T}^{P_{U(t)}})_{W(U)})$. ■

As, by corollary 6.1.1, $P_{U(t)}|P(U(t),a)$ for all $a \in R_N$, the above result completely determines the qualitative behaviour of $\mathbb{T}_{U(t)}$ when $T_{U(t)} > 0$, corollary 6.1.2 does the same when $\mathbb{T}_{U(t)} = 0$, hence one has:

**Theorem 6.1.1** *If*

$$\Sigma((\mathbb{T}^{P_{U(t)}})_{W(U)}) = \sum_{i=1}^{k} n_i[m_i],$$

*then*

$$\Sigma(\mathbb{T}_{U(t)}) = \sum_{i=1}^{k} n_i[m_i P_{U(t)}]. \quad \blacksquare$$

Thus the cycle set for $\mathbb{T}_{U(t)}$ can be obtained from that of $\mathbb{T}' = (\mathbb{T}^{P_{U(t)}})_{W(U)}$ whatever the value of $T_{U(t)}$.

The full set of points lying on cycles under $\mathbb{T}_{U(t)}$, for any value of $T_{U(t)}$ is given in terms of $Att((\mathbb{T}^{P_{U(t)}})_{W(U)})$ as follows.

**Lemma 6.1.4** *The set* $Att(\mathbb{T}_{U(t)})$ *of all elements of* $R_N$ *lying on cycles under* $\mathbb{T}_{U(t)}$ *is given by*

$$Att(\mathbb{T}_{U(t)}) = Att((\mathbb{T}^{P_{U(t)}})_{W(U)}) \cup_{i=1}^{P_{U(t)}-1} \mathbb{T}^i_{U(t)}(Att((\mathbb{T}^{P_{U(t)}})_{W(U)}))$$

*when* $T_{U(t)} = 0$ *and by*

$$Att(\mathbb{T}_{U(t)}) = Att((\mathbb{T}^{P_{U(t)}})_{W(U)}) \cup_{i=1}^{P_{U(t)}-1} (\mathbb{T}^i)_{V(T_{U(t)}+i)}(Att((\mathbb{T}^{P_{U(t)}})_{W(U)}))$$

*otherwise, where*

$$V(T_{U(t)} + i) = \sum_{j=1}^{i} \mathbb{T}^{i-j} U(T_{U(t)} + j).$$

Proof:

When $T_{U(t)} = 0$ every secondary periodic point is of the form $\mathbb{T}^i_{U(t)}(a)$ where $a \in Att((\mathbb{T}^{P_{U(t)}})_{W(U)})$ is a primary periodic point and $1 \leq i \leq P_{U(t)} - 1$, the result follows immediately.

When $T_{U(t)} > 0$, let $a$ be a primary periodic point, then $a \in Att((\mathbb{T}^{P_{U(t)}})_{W(U)})$ by lemma 6.1.3 and $a = \mathbb{T}^{T_{U(t)}+nP_{U(t)}}_{U(t)}(b)$ for some $b \in R_N$ and integer $n \geq 0$, thus the elements $\mathbb{T}^{T_{U(t)}+nP_{U(t)}+i}_{U(t)}(b)$, $1 \leq i \leq P_{U(t)} - 1$ are secondary periodic points and all

secondary periodic points are of this form. We have

$$\begin{aligned}\mathbb{T}_{U(t)}^{T_{U(t)}+nP_{U(t)}+i}(b) &= \mathbb{T}^i a + U(T_{U(t)}+i) + \mathbb{T}U(T_{U(t)}+i-1) + \ldots + \mathbb{T}^{i-1}U(T_{U(t)}+1) \\ &= \mathbb{T}^i a + V(T_{U(t)}+i),\end{aligned}$$

where $V(T_{U(t)}+i) = \sum_{j=1}^{i} \mathbb{T}^{i-j}U(T_{U(t)}+j)$ and the result follows. ■

As in the case of constant inputs we can define qualitative dynamical similarity (QDS) for periodic and eventually periodic inputs.

**Definition 6.1.3** *Let $U(t)$ and $V(t)$ both have period $P > 1$, then $\mathbb{T}_{U(t)}$ and $\mathbb{T}_{V(t)}$ are* QDS *if*

$$\Sigma(\mathbb{T}_{U(t)}) = \Sigma(\mathbb{T}_{V(t)}).$$

From theorem 6.1.1 we have that

$$\Sigma(\mathbb{T}_{U(t)}) = \Sigma(\mathbb{T}_{V(t)})$$

if and only if

$$\Sigma((\mathbb{T}^{P_{U(t)}})_{W(U)}) = \Sigma((\mathbb{T}^{P_{V(t)}})_{W(V)})$$

and $P_{U(t)} = P_{V(t)}$. With theorem 6.1.1 in mind we also make the following definition:

**Definition 6.1.4** *Say that $\mathbb{T}_{U(t)}$ and $\mathbb{T}_{V(t)}$ are semi-*QDS *if*

$$\Sigma((\mathbb{T}^{P_{U(t)}})_{W(U)}) = \Sigma((\mathbb{T}^{P_{V(t)}})_{W(V)}).$$

Clearly QDS $\Rightarrow$ semi-QDS

The next result follows immediately.

**Theorem 6.1.2** *If $P_{U(t)} = P_{V(t)}$ then $\mathbb{T}_{U(t)}$ and $\mathbb{T}_{V(t)}$ are* QDS *if and only if $(\mathbb{T}^{P_{U(t)}})_{W(U)}$ and $(\mathbb{T}^{P_{V(t)}})_{W(V)}$ are* QDS. *More generally $\mathbb{T}_{U(t)}$ and $\mathbb{T}_{V(t)}$ are semi-*QDS *if and only if $(\mathbb{T}^{P_{U(t)}})_{W(U)}$ and $(\mathbb{T}^{P_{V(t)}})_{W(V)}$ are* QDS. ■

Thus we can use the results from chapter 2, section 2.3 to determine if $\mathbb{T}_{U(t)}$ and $\mathbb{T}_{V(t)}$ are QDS for time dependent inputs $U(t)$ and $V(t)$. Note that in particular $\mathbb{T}_{U(t)}$ and $\mathbb{T}_{W(U)}^{P_{U(t)}}$ are semi-QDS and that the cycles occurring under $\mathbb{T}_{U(t)}$ can be thought of as the cycles under $\mathbb{T}_{W(U)}^{P_{U(t)}}$ "stretched" by a factor $P_{U(t)}$ and in general if $\mathbb{T}_{U(t)}$ and $\mathbb{T}_{V(t)}$ are semi-QDS with $P_{U(t)} > P_{V(t)}$ then the cycles occurring under $\mathbb{T}_{U(t)}$ can be thought of as those occurring under $\mathbb{T}_{V(t)}$ "stretched" by a factor $P_{U(t)}/P_{V(t)}$.

**Example 6.1.3**

Let $N = 4$, $R = \mathbb{F}_2$, $\mathbb{T} = 1+x+x^2+(x^4-1)\mathbb{F}_2[x]$. We shall omit the "$+(x^4-1)\mathbb{F}_2[x]$"for the rest of this example. Let $U(t)$ be defined by $U(1) = 1$, $U(2i) = x$, $U(2i+1) = x^2$ for $i \geq 1$, so $T_{U(t)} = 1$ and $P_{U(t)} = 2$. Then

$$W(U) = \mathbb{T}U(2) + U(3) = x + x^3.$$

Let $V(t)$ be defined by $V(1) = 1$,$V(2) = 1 + x$, $V(2i-1) = x^3$ and $V(2i) = x^2$ for all $i \geq 2$. Thus $T_{V(t)} = 2$ and $P_{U(t)} = 2$. Then

$$W(V) = \mathbb{T}V(3) + V(4) = 1 + x + x^2 + x^3.$$

Now,

$$\mathbb{T}^{P_{U(t)}} = \mathbb{T}^{P_{V(t)}} = \mathbb{T}^2 = x^2$$

and one finds that

$$(\mathbb{T}^2)_{W(U)-W(V)} = (\mathbb{T}^2)_{1+x^2},$$

which has a fixed point, hence $\mathbb{T}_{U(t)}$ and $\mathbb{T}_{V(t)}$ are QDS by theorem 2.3.2 and theorem 6.1.2. Moreover, one finds that $(\mathbb{T}^2)_{W(U)}$ is QDS to $\mathbb{T}^2$ and

$$\Sigma(\mathbb{T}^2) = 4[1] + 6[2].$$

Hence

$$\Sigma((\mathbb{T}^2)_{W(U)}) = \Sigma((\mathbb{T}^2)_{W(V)}) = 4[2] + 6[4]$$

by theorem 6.1.1. ♦

## 6.2 Additive cellular automata in higher dimensions

In this section we briefly discuss the extension of our methods to cellular automata in two or more dimensions with periodic boundary conditions. Martin *et.al.*, [3], showed that the state of a linear cellular automata in $D$ dimensions with cells arranged on a rectangular lattice of $N_i$ cells in the $i-th$ direction, $1 \leq i \leq D$, with periodic boundary conditions can be represented as polynomials in $D$ commuting indeterminates $x_1, \ldots, x_D$ of degree at most $N_i$ in $x_i$. The action of the global rule is represented by multiplication by a (Laurent) polynomial in $x_1, \ldots, x_D$ derived from the local rule and

then taking the results modulo $x_i^{N_i} - 1$, $1 \leq i \leq D$. By similar arguments to those used in chapter 1, section 1.5.3, this is equivalent to representing the states of the cellular automata as the elements of

$$R(N_1, \ldots, N_D) = \frac{R[x_1, \ldots, x_D]}{(x^{N_1} - 1, \ldots, x^{N_D} - 1)R[x_1, \ldots, x_D]},$$

where $(x^{N_1} - 1, \ldots, x^{N_D} - 1)R[x_1, \ldots, x_D] \lhd R[x_1, \ldots, x_D]$ is the ideal generated by $x^{N_1} - 1, \ldots, x^{N_D} - 1$, and representing the action of the global rule by multiplication by an element $\mathbb{T} \in R(N_1, \ldots, N_D)$. External time independent inputs are represented as elements of $R(N_1, \ldots, N_D)$ in the obvious way. By remark 2.1.1 nearly all the results of chapter 2 apply in the present case on just replacing $R_N$ with $R(N_1, \ldots, N_D)$ and such results will be used if necessary without further comment.

We concentrate on the $D = 2$ case for clarity, the extension to $D > 2$ is relatively straight forward. The results in this section are by way of a preliminary investigation, we consider only the case of state alphabet a finite field and do little more than obtain a direct product decomposition of $R(N_1, N_2)$ into a direct product of completely primary rings, of course idempotent lifting will enable one to obtain a direct product decomposition in the case of state alphabet $\mathbb{Z}_{/p^k}$, $k > 1$, also, as in chapter 5 for the one dimensional case. We shall see that for $D = 2$, as long as one of $N_1$ and $N_2$ is coprime to $p$ when $R = \mathbb{F}_{p^q}$, then all of the rings in the direct product decomposition will be of types considered in chapter 3 and thus one can employ the method and results of chapters 3 and 4. For $D > 3$ this will be the case as long as only one of the $N_i$, $1 \leq i \leq D$, is not coprime to $p$. Returning to $D = 2$, if $N_1 = n_1 p^r$ and $N_2 = n_2 p^s$ where both $r$ and $s$ are greater than zero and $n_1, n_2$ are coprime to $p$ we must consider rings of a form not considered in chapter 3, while these rings are completely primary the ideal of nilpotent elements is not principal and one can expect similar difficulties to those that arose in chapter 5 when $N$ and $p$ were not coprime. It may be that the method of Guan and He [27] is better for finding cycle sets in the higher dimensional case, however we expect our technique to be useful for at least obtaining qualitative information on reversibility, maximal cycle lengths *etc.*.

We are considering linear local rules of the form

$$f : a_{i_1,i_2} \mapsto \sum_{j_1=-l_1}^{l_1} \sum_{j_2=-l_2}^{l_2} \alpha_{j_1,j_2} a_{i_1+j_1,i_2+j_2} \tag{6.2.1}$$

where $\alpha_{j_1,j_2} \in \mathbb{F}_{p^q}$, $-l_1 \leq j_1 \leq l_1$, $-l_2 \leq j_2 \leq l_2$, and $a_{i,j}$ is that state of cell with

cordinates $(i,j)$ relative to the (arbitrarily chosen) origin. On $N_1 \times N_2$ cells local rule (6.2.1) gives rise to the global rule represented by

$$\mathbb{T} = \sum_{j_1=-l_1}^{l_1} \sum_{j_2=-l_2}^{l_2} \alpha_{j_1,j_2} x_1^{N_1-j_1} x_2^{N_2-j_2} + (x_1^{N_1}-1, x_2^{N_2}-1)\mathbb{F}_{p^q}[x_1,x_2], \qquad (6.2.2)$$

an element of $\frac{\mathbb{F}_{p^q}[x_1,x_2]}{(x_1^{N_1}-1,x_2^{N_2}-1)\mathbb{F}_{p^q}[x_1,x_2]}$, an $N_1N_2$ dimensional $\mathbb{F}_{p^q}-$algebra. The $N_1$ dimensional subalgebra with basis $x_1^i + (x_1^{N_1}-1, x_2^{N_2}-1)\mathbb{F}_{p^q}[x_1,x_2]$, $0 \le i \le N_1-1$, is clearly isomorphic to $\frac{\mathbb{F}_{p^q}[x]}{(x^{N_1}-1)\mathbb{F}_{p^q}[x]}$ and the $N_2$ dimensional subalgebra with basis $x_2^i + (x_1^{N_1}-1, x_2^{N_2}-1)\mathbb{F}_{p^q}[x_1,x_2]$, $0 \le i \le N_2-1$, is clearly isomorphic to $\frac{\mathbb{F}_{p^q}[x]}{(x^{N_2}-1)\mathbb{F}_{p^q}[x]}$. Clearly $\frac{\mathbb{F}_{p^q}[x_1,x_2]}{(x_1^{N_1}-1,x_2^{N_2}-1)\mathbb{F}_{p^q}[x_1,x_2]}$ has a basis

$$\{x_1^i x_2^j + (x_1^{N_1}-1, x_2^{N_2}-1)\mathbb{F}_{p^q}[x_1,x_2] : 0 \le i \le N_1-1, 0 \le j \le N_2-1\}$$

and, refering to theorem A.6.1,

$$\left|\frac{\mathbb{F}_{p^q}[x_1,x_2]}{(x_1^{N_1}-1,x_2^{N_2}-1)\mathbb{F}_{p^q}[x_1,x_2]}\right| = p^{qN_1N_2} = \left|\frac{\mathbb{F}_{p^q}[x_1]}{(x^{N_1}-1)\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{(x^{N_2}-1)\mathbb{F}_{p^q}[x_2]}\right|$$

which suggests that one might have

$$\frac{\mathbb{F}_{p^q}[x_1,x_2]}{(x_1^{N_1}-1,x_2^{N_2}-1)\mathbb{F}_{p^q}[x_1,x_2]} \cong \frac{\mathbb{F}_{p^q}[x_1]}{(x^{N_1}-1)\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{(x^{N_2}-1)\mathbb{F}_{p^q}[x_2]},$$

this is in fact the case.

**Lemma 6.2.1** *For all integers $N_1, N_2 > 0$ and any finite field $\mathbb{F}_{p^q}$*

$$\frac{\mathbb{F}_{p^q}[x_1,x_2]}{(x_1^{N_1}-1,x_2^{N_2}-1)\mathbb{F}_{p^q}[x_1,x_2]} \cong \frac{\mathbb{F}_{p^q}[x_1]}{(x^{N_1}-1)\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{(x^{N_2}-1)\mathbb{F}_{p^q}[x_2]} \quad \blacksquare$$

The proof of lemma 6.2.1 can be found in appendix B.

Applying lemma A.6.1 we obtain the following

**Theorem 6.2.1** *For all integers $n_1, n_2 > 0$ and coprime to $p$ and any $r, s \in \mathbb{N}$*

$$\frac{\mathbb{F}_{p^q}[x_1,x_2]}{(x_1^{n_1p^r}-1,x_2^{n_2p^s}-1)\mathbb{F}_{p^q}[x_1,x_2]} \cong \prod_{i=1}^{m_1}\prod_{j=1}^{m_2} \frac{\mathbb{F}_{p^q}[x_1]}{R_i(x_1)^{p^r}\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{S_j(x_2)^{p^s}\mathbb{F}_{p^q}[x_2]},$$

*where*

$$\frac{\mathbb{F}_{p^q}[x_1]}{(x^{N_1}-1)\mathbb{F}_{p^q}[x_1]} \cong \prod_{i=1}^{m_1} \frac{\mathbb{F}_{p^q}[x_1]}{R_i(x_1)^{p^r}\mathbb{F}_{p^q}[x_1]}$$

$$\frac{\mathbb{F}_{p^q}[x_2]}{(x^{N_2}-1)\mathbb{F}_{p^q}[x_2]} \cong \prod_{j=1}^{m_2} \frac{\mathbb{F}_{p^q}[x_2]}{S_j(x_2)^{p^s}\mathbb{F}_{p^q}[x_2]} \quad \blacksquare$$

By the same argument as that in the proof of lemma 6.2.1 one finds that

$$\frac{\mathbb{F}_{p^q}[x_1]}{R_i(x_1)^{p^r}\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{S_j(x_2)^{p^s}\mathbb{F}_{p^q}[x_2]} \cong \frac{\mathbb{F}_{p^q}[x_1,x_2]}{(R_i(x_1)^{p^r}, S_j(x_2)^{p^s})\mathbb{F}_{p^q}[x_1,x_2]} \tag{6.2.3}$$

for each $i$ and each $j$. It follows that instead of theorem 6.2.1 we could work with the isomorphism induced by the the projection homomorphisms

$$\theta_{i,j} : \frac{\mathbb{F}_{p^q}[x_1,x_2]}{(x_1^{n_1p^r}-1, x_2^{n_2p^s}-1)\mathbb{F}_{p^q}[x_1,x_2]} \longrightarrow \frac{\mathbb{F}_{p^q}[x_1,x_2]}{(R_i(x_1)^{p^r}, S_j(x_2)^{p^s})\mathbb{F}_{p^q}[x_1,x_2]},$$

$1 \leq i \leq m_1$, $1 \leq j \leq m_2$, however it is conveinent to use the tensor product representation, as from (A.6.1) in appendix A and the discussion preceding it we have, with

$K = \frac{\mathbb{F}_{p^q}[x_1]}{R(x_1)^{p^r}\mathbb{F}_{p^q}[x_1]}$,

$$\frac{K[x_2]}{S(x_2)^{p^s}K[x_2]} \cong K \otimes \frac{\mathbb{F}_{p^q}[x_2]}{S(x_2)^{p^s}\mathbb{F}_{p^q}[x_2]}$$

(of course one could just as well take $K = \frac{\mathbb{F}_{p^q}[x_2]}{S(x_2)^{p^s}\mathbb{F}_{p^q}[x_2]}$). There are two cases:

(i) Either $r = 0$ or $s = 0$, we can suppose without loss of generality that $r = 0$ hence $K = \frac{\mathbb{F}_{p^q}[x_1]}{R(x_1)^{p^r}\mathbb{F}_{p^q}[x_1]} \cong \mathbb{F}_{p^{qd_R}}$, where the degree of $R$ is $d_R$, then

$$\frac{\mathbb{F}_{p^q}[x_1]}{R(x_1)\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{S(x_2)^{p^s}\mathbb{F}_{p^q}[x_2]} \cong \frac{\mathbb{F}_{p^{qd_R}}[x_2]}{S(x_2)^{p^s}\mathbb{F}_{p^q}[x_2]}.$$

Thus if $S(x)$ is irreducible over $\mathbb{F}_{p^{qd_R}}$ then $\frac{\mathbb{F}_{p^q}[x_1]}{R(x_1)\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{S(x_2)^{p^s}\mathbb{F}_{p^q}[x_2]}$ is a completely primary ring of the form considered in chapter 3 and if $S(x)$ factorises over $\mathbb{F}_{p^{qd_R}}$ then $\frac{\mathbb{F}_{p^q}[x_1]}{R(x_1)\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{S(x_2)^{p^s}\mathbb{F}_{p^q}[x_2]}$ is a direct product of completely primary rings of the form considered in chapter 3, in particular if $s = 0$ then $\frac{\mathbb{F}_{p^q}[x_1]}{R(x_1)\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{S(x_2)\mathbb{F}_{p^q}[x_2]}$ is either a field or a direct product of fields. In fact one can say a great deal about when and

how $S(x)$ factorises over $\mathbb{F}_{p^{qd_R}}$ but for reasons of brevity we do not go into such details here.

(ii) Both $r$ and $s$ are greater than zero. The map

$$\pi_{r,0} \otimes \pi_{s,0} : \frac{\mathbb{F}_{p^q}[x_1]}{R(x_1)^{p^r}\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{S(x_2)^{p^s}\mathbb{F}_{p^q}[x_2]} \longrightarrow \frac{\mathbb{F}_{p^q}[x_1]}{R(x_1)\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{S(x_2)\mathbb{F}_{p^q}[x_2]}$$

is a ring epimorphism (where $\pi_{r,0} : \frac{\mathbb{F}_{p^q}[x_1]}{R(x_1)^{p^r}\mathbb{F}_{p^q}[x_1]} \longrightarrow \frac{\mathbb{F}_{p^q}[x_1]}{R(x_1)\mathbb{F}_{p^q}[x_1]}$ is the ring epimorphism defined in chapter 3 *etc.*), as are the maps

$$\pi_{r,0} \otimes Id : \frac{\mathbb{F}_{p^q}[x_1]}{R(x_1)^{p^r}\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{S(x_2)^{p^s}\mathbb{F}_{p^q}[x_2]} \longrightarrow \frac{\mathbb{F}_{p^q}[x_1]}{R(x_1)\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{S(x_2)^{p^s}\mathbb{F}_{p^q}[x_2]}$$

and

$$Id \otimes \pi_{s,0} : \frac{\mathbb{F}_{p^q}[x_1]}{R(x_1)\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{S(x_2)^{p^s}\mathbb{F}_{p^q}[x_2]} \longrightarrow \frac{\mathbb{F}_{p^q}[x_1]}{R(x_1)\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{S(x_2)\mathbb{F}_{p^q}[x_2]},$$

one must have that $\pi_{r,0} \otimes \pi_{s,0} = Id \otimes \pi_{s,0} \circ \pi_{r,0} \otimes Id$. If $\frac{\mathbb{F}_{p^q}[x_1]}{R(x_1)\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{S(x_2)^{p^s}\mathbb{F}_{p^q}[x_2]}$ is a field it is easy to show that $\frac{\mathbb{F}_{p^q}[x_1]}{R(x_1)^{p^r}\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{S(x_2)^{p^s}\mathbb{F}_{p^q}[x_2]}$ is completely primary. If $\frac{\mathbb{F}_{p^q}[x_1]}{R(x_1)\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{S(x_2)^{p^s}\mathbb{F}_{p^q}[x_2]}$ is a direct product then it is a direct product of completely primary rings of the form $\frac{\mathbb{F}_{p^q}[x_1,x_2]}{(R(x_1),S_i(x_2)^{p^s})\mathbb{F}_{p^q}[x_1,x_2]}$, where $S(x) = \prod_{i=1}^{m} S_i(x)$ over $\mathbb{F}_{p^{qd_R}}$. One sees that $\alpha \in \text{Ker } \pi_{r,0} \otimes Id$ implies that $R(x_1)|\alpha(x_1,x_2)$ or $S_i(x_2)|\alpha(x_1,x_2)$ for $1 \leq i \leq m$, in either case $\alpha$ is nilpotent so Ker $\pi_{r,0} \otimes Id$ is a nil ideal and hence idempotent lifting (by lemma A.5.3) and one can lift idempotents in a similar manner to that in theorem 5.1.1 to show that $\frac{\mathbb{F}_{p^q}[x_1]}{R(x_1)^{p^r}\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{S(x_2)^{p^s}\mathbb{F}_{p^q}[x_2]}$ is a direct product of completely primary rings, themselves of the form $\frac{\mathbb{F}_{p^q}[x_1]}{R(x_1)^{p^r}\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{\hat{S}(x_2)^{p^s}\mathbb{F}_{p^q}[x_2]}$ where $\hat{S}(x)$ is an irreducible factor of $S(x)$ over $\mathbb{F}_{p^{qd_R}}$. Thus we need consider only the case $\frac{\mathbb{F}_{p^q}[x_1]}{R(x_1)^{p^r}\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{S(x_2)^{p^s}\mathbb{F}_{p^q}[x_2]}$ is completely primary. It is clear that Ker $\pi_{r,0} \otimes \pi_{s,0}$ is the ideal generated by $R \otimes 1$ and $1 \otimes S$, not principal. At this point we merely give the following result as an example and leave further investigation to future publications.

**Lemma 6.2.2** *Let* $\mathbb{T}$ *be a unit in* $\frac{\mathbb{F}_{p^q}[x_1]}{R(x_1)^{p^r}\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{S(x_2)^{p^s}\mathbb{F}_{p^q}[x_2]}$ *where* $\frac{\mathbb{F}_{p^q}[x_1]}{R(x_1)\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{S(x_2)\mathbb{F}_{p^q}[x_2]}$ *is a field. Then the minimum orbit length that occurs under* $\mathbb{T}$ *for any*

*non-zero element is equal to the order of the image,* $\hat{\mathbb{T}}$*, of* $\mathbb{T}$ *under* $\pi_{r,0} \otimes \pi_{s,0}$ *in the muliplicative group of* $\frac{\mathbb{F}_{pq}[x_1]}{R(x_1)\mathbb{F}_{pq}[x_1]} \otimes \frac{\mathbb{F}_{pq}[x_2]}{S(x_2)\mathbb{F}_{pq}[x_2]}$.

Proof:

From chapter 3 we know that $\hat{\mathbb{T}}^L = 1$ first for $L$ equal to the order of $\hat{\mathbb{T}}$ in the cyclic group of units and the only element on an orbit of length less than $L$ is zero. It follows that $\mathbb{T}^L = 1 + n$ where $n$ is nilpotent, say $n^t = 0$, then $n^{t-1}$ has period $L$ under $\mathbb{T}$. If $\mathbb{T}^k a = a$ for some non-zero element $a$ then $\mathbb{T}^k - 1$ is nilpotent and thus $\hat{\mathbb{T}}^k = 1$ which contradicts the minimality of $L$. ■

# Appendix A

# A review of the relevant algebra

In this appendix we briefly review some of the algebra relevant to this thesis. We assume that the reader is familiar with elementary group theory, ring theory and module theory, though some of the more relevant aspects are discussed briefly. For more details we refer the reader to those texts we have found most useful, namely [28], [30], [31], [25], [26] and [32].

## A.1 Rings

We shall assume that the reader is familiar with the definition of a ring, for definiteness we note that we require that our rings to have an identity element $1_R$ which satisfies

$$1_R a = a 1_R = a \text{ for all } a \in R.$$

We shall also require that $1_R \neq 0_R$. We shall normally write 1 for $1_R$.

The *center* of a ring $R$ is the set

$$Z(R) = \{z \in R : rz = zr \text{ for every } r \in R\}.$$

It is easily verified that $Z(R)$ is a subring, clearly if $R$ is commutative then $Z(R) = R$.

**Definition A.1.1** *Let $R$ be a ring.*

(i) *An element $a \in R$ is a unit if there is some $b \in R$ such that $ab = ba = 1$.*

(ii) *An element $a \in R \setminus \{0\}$ is a zero-divisor if there is some $b \in R \setminus \{0\}$ such that $ab = 0$.*

(iii) *An element $a \in R$ is nilpotent if there is some natural number $t$ such that $a^t = 0$.*

Let $a \in R$ be a unit, the element $b \in R$ such that $ab = ba = 1$ is referred to as the inverse of $a$ and denoted by $a^{-1}$, we shall sometimes call a unit $a \in R$ an invertible element. Note that the set of units in a commutative ring forms a multiplicative group, sometimes denoted by $R^*$. We recall that a *integral domain* is a commutative ring $R$ that has no zero-divisors. A *field* is a integral domain $F$ such that $F^* = F \setminus \{0\}$.

The Binomial theorem holds in a commutative ring (see any basic algebra text).

**Lemma A.1.1** *Let $R$ be a commutative ring, $a, b \in R$ and $n > 0$ an integer, then*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i. \quad \blacksquare$$

Let $R$ be a commutative ring and $A \subseteq R$, by $AR$ we shall mean the set of finite sums

$$AR = \{\sum ar : a \in A, r \in R\}.$$

Let $R$ be a commutative ring, an *ideal* of $R$ is a subgroup $\mathfrak{A}$ of the additive group $R$ which satisfies

$$\mathfrak{A}R \subseteq \mathfrak{A}.$$

An ideal $\mathfrak{A}$ of $R$ is proper if $\mathfrak{A} \neq \{0\}$ and $\mathfrak{A} \neq R$. When $\mathfrak{A}$ is an ideal of $R$ we shall write $\mathfrak{A} \lhd R$.

As an example of an ideal consider the following:

**Lemma A.1.2** *Let $R$ be a commutative ring, then the set $\mathfrak{N}$ of nilpotent elements in $R$ is an ideal.*

Proof:

We have to show that $\mathfrak{N}$ is a subgroup and that $\mathfrak{N}R \subseteq \mathfrak{N}$. Clearly $0 \in \mathfrak{N}$, so to show that $\mathfrak{N}$ is a subgroup it suffices to show that $\mathfrak{N}$ is closed under addition (the other group axioms will hold because they do in $R$). Let $a, b \in \mathfrak{N}$ with $a^{t_1} = 0$ and $b^{t_2} = 0$, then

$$\begin{aligned}
(a+b)^{t_1+t_2} &= \sum_{i=0}^{t_1+t_2} \binom{t_1+t_2}{i} a^{t_1+t_2-i} b^i \\
&= \sum_{i=0}^{t_2} \binom{t_1+t_2}{i} a^{t_1+t_2-i} b^i + \sum_{i=t_2+1}^{t_1+t_2} \binom{t_1+t_2}{i} a^{t_1+t_2-i} b^i \\
&= a^{t_1} \sum_{i=0}^{t_2} \binom{t_1+t_2}{i} a^{t_2-i} b^i + b^{t_2} \sum_{j=1}^{t_1} \binom{t_1+t_2}{j+t_2} a^{t_1+t_2-j} b^j \\
&= 0.
\end{aligned}$$

Thus $\mathfrak{N}$ is closed under addition. Let $a \in \mathfrak{N}$ with $a^t = 0$ and $r \in R$, then

$$(ar)^t = a^t r^t = 0 r^t = 0$$

hence $\mathfrak{N}R \subseteq \mathfrak{N}$. ■

**Remark A.1.1** *If $a \in R$ is nilpotent, $a^t = 0$, $t \in \mathbb{N}$, then $1 - a$ is a unit.*

Proof:

As $a^t = 0$ one has

$$1 = 1 - a^t \Rightarrow 1 = (1-a)(a^{t-1} + a^{t-2} + \ldots + a + 1)$$

hence $(1-a)$ is a unit. ■

An important class of ideals are those generated by a single element, known as principal ideals. Let $a \in R$, a commutative ring, then the principal ideal generated by $a$ is

$$aR = \{ar : r \in R\}.$$

$aR$ is sometimes denoted by $(a)$. A ring $R$ is a principal ideal ring if every ideal in $R$ is principal.

### A.1.1 Ring homomorphisms and quotient rings

Ring homomorphisms are structure preserving mappings between rings, we recall that

**Definition A.1.2** *Let $R, S$ be rings, a ring homomorphism from $R$ to $S$ is a map $\phi : R \longrightarrow S$ such that for all $a, b \in R$ one has*

$$\phi(a+b) = \phi(a) + \phi(b),\ \phi(ab) = \phi(a)\phi(b),\ \phi(0_R) = 0_S,\ \phi(1_R) = 1_S.$$

It follows immediately from the definition that, for any $a \in R$, $\phi(a_n) = \phi(a)^n$, $n \in \mathbb{N}$ and that $\phi(-a) = -\phi(a)$. For a unit $r \in R$ one has $\phi(r^{-1}) = \phi(r)^{-1}$ and for nilpotent $r \in R$ such that $r^n = 0$ for integer $n > 0$ then $\phi(r)^n = 0$.

The *kernel* of a ring homomorphism $\phi$, written Ker $\phi$, is the set of pre-images of 0, *i.e.* the set $\{a \in R : \phi(a) = 0_S\}$. It is easily verified that Ker $\phi$ is an ideal of $R$ and that the image of $\phi$, Im $\phi$ is a subring of $S$. Also easily verified is the fact that a homomorphism $\phi$ is injective if and only if Ker $\phi = \{0\}$.

A bijective ring homomorphism $\phi : R \longrightarrow S$ is known as a ring isomorphism and one says $R$ is isomorphic to $S$ and writes $R \cong S$. An injective homomorphism is known as a monomorphism, a surjective homomorphism is known as an epimorphism, a ring endomorphism is a homomorphism from a ring to itself. The following remark is easily verified.

**Remark A.1.2** *If $R$ and $S$ are finite with $|R| = |S|$ then for a homomorphism $\phi : R \longrightarrow S$ the following statements are equivalent:*

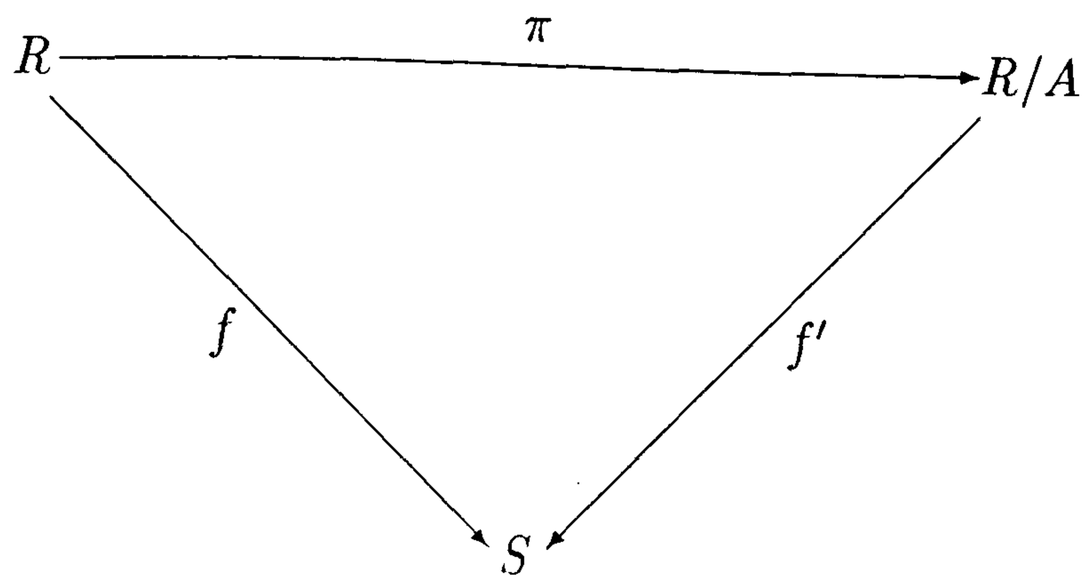


Figure A.1: $f = f' \circ \pi$.

(i) *$\phi$ is an isomorphism;*

(ii) *$\phi$ is injective;*

(iii) *$\phi$ is surjective.* ■

Given an ideal $A$ of a ring $R$ we may form the quotient ring $R/A$ in a similar manner to that in which a quotient group is formed from a group and a normal subgroup. Briefly given an ideal $A$, $R/A$ is the set of cosets $r + A$, $r \in R$, $r + A = \{r + a : a \in A\}$. The set of distinct cosets partitions $R$ and the operations in $R/A$ are defined in terms of those in $R$ by

$$\begin{aligned}(x + A) + (y + A) &= x + y + A \\ (x + A)(y + A) &= xy + A.\end{aligned}$$

These operations are well defined in the sense that they do not depend on the representatives $x, y$ chosen (see any basic algebra text). $0_{R/A} = 0_R + A$ and $1_{R/A} = 1_R + A$. Given an ideal $A$ of $R$ there is a natural homomorphism $\pi : R \longrightarrow R/A$ given by $r \mapsto r + R/A$ and Ker $\pi = A$. If $R$ is commutative then so is $R/A$. The proofs of the following theorems can be found in most algebra texts.

**Theorem A.1.1** [Factor Theorem]

*Let $f : R \longrightarrow S$ be a homomorphism of rings and let $A$ be an ideal of $R$ with $A \subseteq Ker\ f$, then there is a unique ring homomorphism $f' : R/A \longrightarrow S$ such that $f' \circ \pi = f$ (see figure A.1). $f'$ is injective if and only if $A = Ker\ f$.* ■

Note that $f'$ satisfies $f'(r + A) = f(r)$.

**Theorem A.1.2** [First Isomorphism Theorem]

*Given any ring homomorphism $f : R \longrightarrow S$ there is a factorisation $f = \alpha f_1 \beta$,*

*$\alpha : R \longrightarrow R/\mathrm{Ker}f$ is the natural homomorphism, $\beta : \mathrm{Im}f \longrightarrow S$ is inclusion and $f_1 : R/\mathrm{ker}f \longrightarrow \mathrm{Im}f$ is an isomorphism.* ■

### A.1.2 Factorisation in commutative rings

**Definition A.1.3** *A non-zero element $a$ of a commutative ring $R$ is said to divide $b \in R$ if there is some $c \in R$ such that $ac = b$, in this case one writes $a|b$. If $a, b \in R$ are such that $a|b$ and $b|a$ then $a$ and $b$ are called associates.*

The concept of divisibility is closely linked to principal ideals. The proof of the following theorem is easy.

**Theorem A.1.3** *Let $a, b, u$ be elements of a commutative ring $R$, then*

(i) $a|b \Leftrightarrow (b) \subseteq (a)$.

(ii) *$a$ and $b$ are associates* $\Leftrightarrow (a) = (b)$.

(iii) *$u$ is a unit* $\Leftrightarrow u|r$ *for all* $r \in R$.

(iv) *$u$ is a unit* $\Leftrightarrow (u) = R$.

(v) *The relation $a$ is an associate of $b$ is an equivalence relation on $R$.*

(vi) *If $a = br$, $r \in R$ a unit then $a$ and $b$ are associates. If $R$ is an integral domain then the converse is true.* ■

**Definition A.1.4** *Let $R$ be a commutative ring, then a non-zero, non-unit element $c \in R$ is*

(a) *irreducible if $c = ab \Rightarrow$ $a$ or $b$ is a unit;*

(b) *prime if $c|ab \Rightarrow c|a$ or $c|b$.*

### A.1.3 The characteristic of a ring

**Definition A.1.5** *The characteristic of a ring $R$ is the additive order $1_R$ (the least integer $m > 1$ such that $m1_R = 0$), if the additive order is infinite (there is no integer $m > 0$ such that $m1_R = 0$) then $R$ is said to have characteristic zero.*

We shall denote the characteristic of $R$ by *char* $R$. Note that we do not allow *char* $R = 1$ for then $1_R = 0_R$.

**Lemma A.1.3** *If $R$ is finite then $R$ has non-zero characteristic.*

Proof:

Suppose that $R$ has characteristic zero, as $R$ is finite there must be integers $m > n > 0$ such that $m1_R = n1_R$ hence $(m - n)1_R = 0$ which contradicts *char* $R = 0$. ■

**Theorem A.1.4** *If $R$ is an integral domain then either char $R = 0$ or char $R = p$ where $p$ is prime.*

Proof:

Suppose that *char* $R = mn$ for some integers $m, n > 1$, then $m1_R n1_R = 0$ so $m1_R$, $n1_R$ are zero-divisors but $R$ is an integral domain so we have a contradiction. ■

**Lemma A.1.4** *If char $R = m > 1$ then there is a subring of $Z(R)$ isomorphic to $\mathbb{Z}/m\mathbb{Z}$.*

Proof:

If *char* $R = m > 1$ then define a map from $\mathbb{Z}/m\mathbb{Z}$ into $Z(R)$ by $n + m\mathbb{Z} \mapsto n1_R$, it is easy to see that this map is a homomorphism and if $n1_R = \hat{n}1_R$ then $(n - \hat{n})1_R = 0$ so $n - \hat{n} = n'm$ for some integer $n'$ hence $n - \hat{n} \in m\mathbb{Z}$ so $n + m\mathbb{Z} = \hat{n} + m\mathbb{Z}$, hence we have a monomorphism and thus $\mathbb{Z}/m\mathbb{Z} \cong S$, (note that $S$ is the subring generated by $1_R$). ■

**Lemma A.1.5** *If $R$ is a commutative ring with prime characteristic $p$, then*

$$(a + b)^p = a^p + b^p$$

Proof:

This follows from the binomial theorem (lemma A.1.1) as $p \mid \binom{p}{i}$ for $1 \leq i \leq p$.

■

## A.2 Rings of polynomials in one indeterminate

We assume that the reader is familiar with the definition of the polynomial ring $R[x]$ over $R$. We recall that if $R$ is commutative then so is $R[x]$ and that if $R$ is an integral domain then so is $R[x]$. The proofs of the next two results can be found in Hungerford [30], pages 158-159.

**Theorem A.2.1** *Let $R$ be a ring and $f, g \in R[x]$.*

(i) *$deg(f + g) \leq max(degf, deg\ g)$.*

(ii) *$deg(fg) \leq deg\ f + deg\ g$.*

(iii) *If the leading coefficient of $f$ or $g$ is not a zero-divisor in $R$ then $deg(fg) = deg\ f + deg\ g$.* ■

**Theorem A.2.2** [The Division Algorithm]

*Let $R$ be a ring, let $f, g \in R[x]$ be non-zero and such that the leading coefficient of $g$ is a unit in $R$. Then there are unique $q, r \in R[x]$ such that*

$$f = qg + r, \text{ and } deg\ r < \ deg\ g. \quad \blacksquare$$

It is clear that if $f \in R[x]$ is such that there is some $b \in R$ such that $ba_i = 0, 0 \leq i \leq$ deg $f$ then $f$ is a zero-divisor in $R[x]$, the next result shows that if $R$ is commutative this is a necessary and sufficient condition.

**Lemma A.2.1** *Let $R$ be a commutative ring, then $f = \sum_{i=0}^{n} a_i x^i$ is a zero-divisor $\Rightarrow$ there is some $b \in R$, $b \neq 0$ such that $ba_i = 0$, $0 \leq i \leq n$.*

Proof:

Let $f \in R[x]$ be a zero-divisor, suppose $fg = 0$, $g \in R[x]$, $g \neq 0$. Suppose that

$$f = \sum_{i=0}^{n} a_i x^i, \qquad g = \sum_{j=0}^{m} b_j x^j.$$

If $a_i g = 0$, $0 \leq i \leq n$, then $a_i b_j = 0$, $0 \leq i \leq n$, $0 \leq j \leq m$, so any non-zero $b_j$ satisfies the claim. If there are some $k \in \{0, 1, \ldots, n\}$ such that $a_k g \neq 0$ let $i$ be maximal amongst these indicies. Then the coefficient of $x^{i+m}$ if $fg = 0$ is

$$a_{i+m} b_0 + a_{i+m-1} b_1 + \ldots + a_i b_m = 0$$

and $a_{i+s} g = 0$ for $s > 0$ so it follows that $a_i b_m = 0$ so the degree of $a_i g$ is less than $m =$ deg $g$. Now, $f(a_i g) = 0$ and $a_i g \neq 0$, so one may repeat the above process, with $g_1 = a_i g$, at each step producing a new non-zero polynomial $g_n$ with deg $g_n <$ deg $g_{n-1}$ and $f g_n = 0$. The degree of $g$, $m$, is finite and the degree of $g_n$ cannot be negative for any $n$ so this process must terminate for some $n'$ with deg $g_{n'} = 0$ so $g_{n'} \in R \setminus \{0\}$ and $f g_{n'} = 0$. $\blacksquare$

We now describe some useful homomorphisms.

**Lemma A.2.2** *The map $\phi_m : R[x] \longrightarrow R[x]$, $a(x) \mapsto a(x^m)$ is a ring endomorphism for any $m \in \mathbb{N}$. If $m > 0$ then $\phi_m$ is injective.*

Proof:

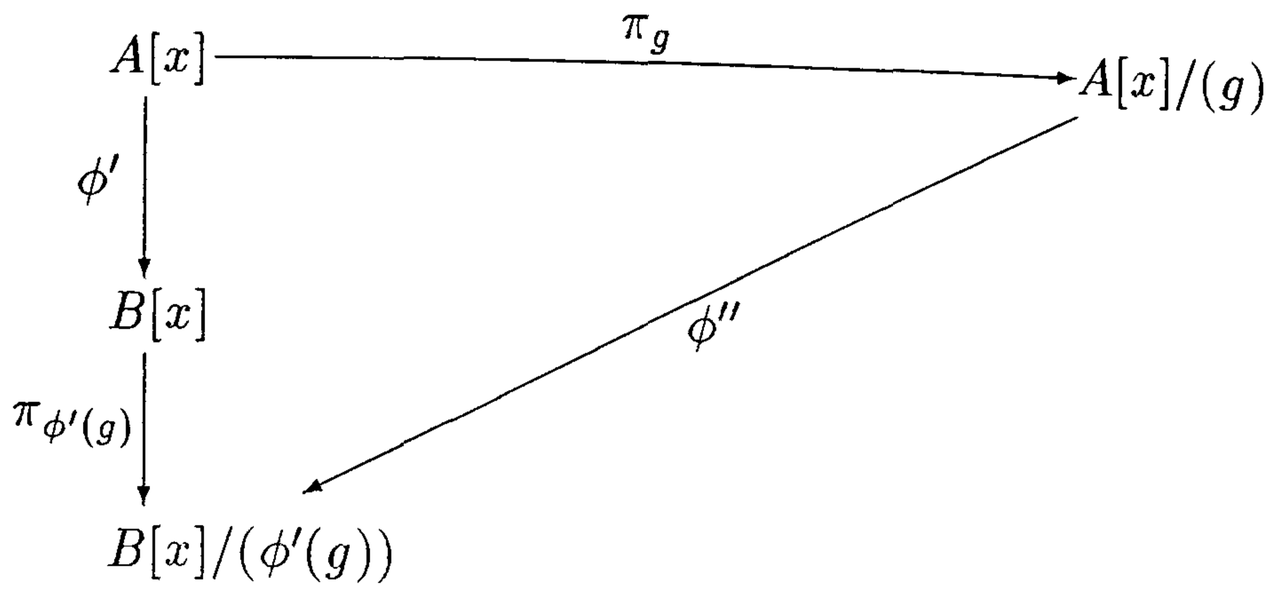


Figure A.2: Homomorphism $\phi'$ induces a homomorphism $\phi''$, surjective if $\phi'$ is surjective.

Let $a(x) = \sum_{i=0}^{d} a_i x^i$, $b(x) = \sum_{j=0}^{d'} b_j x^j$, then $\phi_m(a) = \sum_{i=0}^{d} a_i x^{mi}$ and $\phi_m(b) = \sum_{j=0}^{d'} b_j x^{mj}$. Now

$$a(x)b(x) = \sum_{k=0}^{d+d'} \left( \sum_{i+j=k} a_i b_j \right) x^k \quad \Rightarrow \quad \phi_m(a(x)b(x)) = \sum_{k=0}^{d+d'} \left( \sum_{i+j=k} a_i b_j \right) x^{mk}.$$

Let $y = x^m$ then

$$\phi_m(a)\phi_m(b) = a(y)b(y) = \sum_{k=0}^{d+d'} \left( \sum_{i+j=k} a_i b_j \right) y^k = \sum_{k=0}^{d+d'} \left( \sum_{i+j=k} a_i b_j \right) x^{mk} = \phi_m(ab).$$

It is clear that the other conditions for $\phi_m$ to be a homomorphism are satisfied. Note that $\phi_0$ is evaluation at 1. For $m > 0$ it is clear that $\phi_m$ is injective. ■

**Corollary A.2.1** *Let $R$ be a commutative ring, then for any integers $n, m > 0$ one has that $x^n - 1 | x^{nm} - 1$.*

Proof:

For any integers $m, n > 0$

$$\begin{aligned} x^m - 1 &= (x-1)(x^{m-1} + x^{m-2} + \ldots + x + 1) \\ \Rightarrow \quad \phi_n(x^m - 1) &= \phi_n(x-1)\phi_n(x^{m-1} + x^{m-2} + \ldots + x + 1) \\ \Rightarrow \quad x^{nm} - 1 &= (x^n - 1)\phi_n(x^{m-1} + x^{m-2} + \ldots + x + 1), \end{aligned}$$

hence $x^n - 1 | x^{nm} - 1$. ■

**Lemma A.2.3** *Let $A$ and $B$ be commutative rings and let $\phi : A \longrightarrow B$ be a ring homomorphism, then $\phi$ induces a ring homomorphism $\phi' : A[x] \longrightarrow B[x]$, $\sum_{i=0}^{n} a_i x^i \mapsto$*

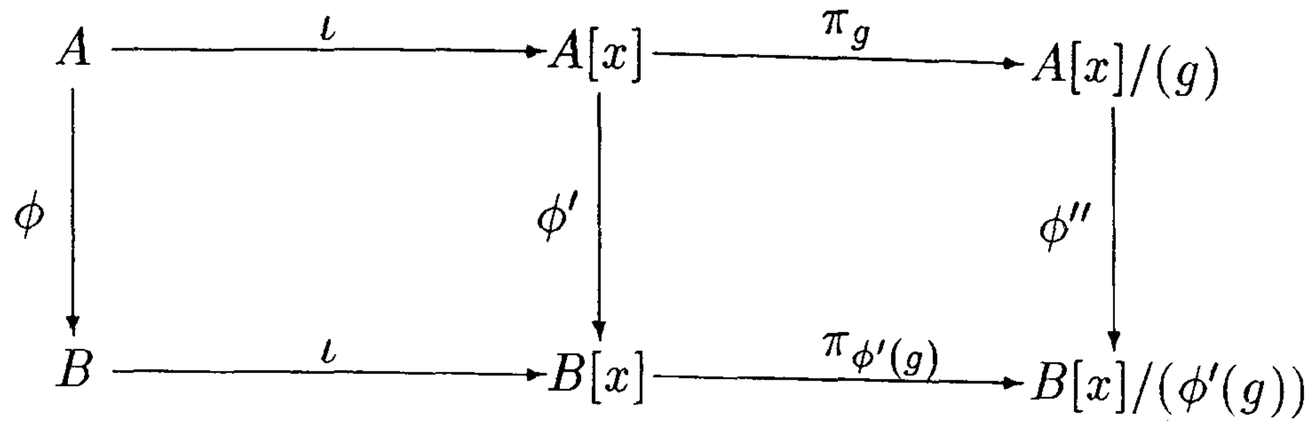


Figure A.3: Homomorphism $\phi$ induces homomorphism $\phi'$ which in turn induces homomorphism $\phi''$, if $\phi$ is surjective then so is $\phi'$ and if $\phi'$ is surjective then so is $\phi''$.

$\sum_{i=0}^{n} \phi(a_i)x^i$. *Further any ring homomorphism* $\phi' : A[x] \longrightarrow B[x]$ *induces a homomorphism* $\phi'' : A[x]/(g(x)) \longrightarrow B[x]/(\phi'(g(x)))$, *where* $(g(x)) = g(x)A[x]$ *the ideal of* $A[x]$ *generated by* $g(x)$ *etc., such that figure A.2 commutes.* ($\phi''$ *is given by* $a(x)+g(x)A[x] \mapsto \phi'(a(x)) + \phi'(g(x))B[x]$). *If* $\phi$ *is surjective then so is* $\phi'$ *and if* $\phi'$ *is surjective then so is* $\phi''$.

Proof:

It is simple to verify that $\phi'$ is a homomorphism. If $\phi$ is surjective and $b \in B[x]$, $b(x) = \sum_{i=0}^{n} b_i x^i$ then $b_i = \phi(a_i)$ for some $a_i$ in $A$ hence $b = \phi'(\sum_{i=0}^{n} a_i x^i)$. Given a homomorphism $\phi' : A[x] \longrightarrow B[x]$ the existence of a homomorphism $\phi'' : A[x]/(g(x)) \longrightarrow B[x]/(\phi'(g(x)))$ for any $g(x) \in A[x]$ such that figure A.2 commutes follows from the factor theorem as $\pi_{\phi'(g)} \circ \phi'(g(x)A[x]) = \pi_{\phi'(g)}(\phi'(g(x))B[x]) = \{0\}$, hence $g(x)A[x] \subseteq ker\pi_{\phi'(g)} \circ \phi'$. If $\phi'$ is surjective then let $b \in B[x]/(\phi'(g(x)))$, $b = b(x) + \phi'(g(x))B[x]$, then there is $a(x) \in A[x]$ such that $\phi'(a(x)) = b(x)$ so $b$ is the image of $a(x) + g(x)A[x]$ under $\phi''$ hence $\phi''$ is surjective. ■

Thus for any ring epimorphism $\phi : A \longrightarrow B$ we have the commuting diagram of figure A.3, where $g = g(x) \in A[x]$, $\iota$ is inclusion and $\pi_g$ and $\pi_{\phi'(g)}$ are the natural projections.

We shall also need to consider the ring of Laurent polynomials over $R$, $R[x, x^{-1}]$ which is defined in a similar way to the polynomial ring and the indeterminates $x$ and $x^{-1}$ satisfy $xx^{-1} = x^{-1}x = 1$, however we shall only be concerned with the quotient ring $\frac{R[x,x^{-1}]}{(x^N-1)R[x,x^{-1}]}$ where $N > 0$ is an integer.

**Lemma A.2.4** *For any ring* $R$ *the following holds for all* $N \in \mathbb{N} \setminus \{0\}$:

$$\frac{R[x, x^{-1}]}{(x^N - 1)R[x, x^{-1}]} \cong \frac{R[x]}{(x^N - 1)R[x]}.$$

Proof:

Let $\alpha$ be any element of $\frac{R[x,x^{-1}]}{(x^N-1)R[x,x^{-1}]}$, say

$$\alpha = \alpha(x, x^{-1}) + (x^N - 1)R[x, x^{-1}],$$

where $\alpha(x, x^{-1}) = \sum_{i=1}^{v} \alpha_{-i} x^{-i} + \beta(x)$. For $1 \leq i \leq v$ let $n(i)$ be the least positive integer satisfying $n(i)N > i$, then

$$\begin{aligned} \alpha(x, x^{-1}) &= \sum_{i=1}^{v} \alpha_{-i}(x^{-i} + x^{n(i)N-i} - x^{n(i)N-i}) + \beta(x) \\ &= \sum_{i=1}^{v} \alpha_{-i}(x^{n(i)N-i} - x^{-i}(x^{n(i)N} - 1)) + \beta(x) \end{aligned}$$

and so

$$\alpha(x, x^{-1}) + (x^N - 1)R[x, x^{-1}] = \sum_{i=1}^{v} \alpha_{-i} x^{n(i)N-i} + \beta(x) + (x^N - 1)R[x, x^{-1}],$$

as $x^N - 1 | x^{n(i)N} - 1$ by corollary A.2.1, hence each element $\alpha \in \frac{R[x,x^{-1}]}{(x^N-1)R[x,x^{-1}]}$ has a canonical representative which is an ordinary polynomial, say $\gamma(x)$. The map

$$\begin{aligned} \iota : \frac{R[x]}{(x^N - 1)R[x]} &\longrightarrow \frac{R[x, x^{-1}]}{(x^N - 1)R[x, x^{-1}]} \\ \gamma(x) + (x^N - 1)R[x] &\mapsto \gamma(x) + (x^N - 1)R[x, x^{-1}] \end{aligned}$$

is well defined and is thus clearly a homomorphism, and by the comments above it is surjective. Suppose $\gamma(x) \in R[x]$, $\gamma(x) \notin (x^N - 1)R[x]$, then $\gamma(x) = \delta(x) + g(x)(x^N - 1)$ for some $g(x)$ and $\delta(x) \neq 0$ with $\deg \delta(x) < N$. Then if $\iota(\gamma(x) + (x^N - 1)R[x]) = 0$ one has that $\delta(x) = a(x, x^{-1})(x^N - 1)$ for some $a(x, x^{-1}) \in R[x, x^{-1}]$ so we must have

$$\sum_{i=0}^{N-1} \delta_i x^i = (x^N - 1) \sum_{j=-L_1}^{L_2} a_j x^j$$

where not all the $\delta_i$ are zero, but if $L_2 \geq 0$ then there is a non-zero term in $x^{N+L_2}$ on the right hand side, which is clearly a contradiction and if $L_1 \geq 1$ then there is a term in $x^{-L_1}$ on the right hand side but on the left which again is a contradiction, hence there is no such $a(x, x^{-1})$ and thus Ker $\iota = \{0\}$ and $\iota$ is an isomorphism. ■

We shall always identify across the isomorphism described in lemma A.2.4 and so put

$$\frac{R[x,x^{-1}]}{(x^N-1)R[x,x^{-1}]} = \frac{R[x]}{(x^N-1)R[x]}.$$

## A.3 Modules and algebras

We recall the definition of an $R-$module:

**Definition A.3.1** *Let $R$ be a ring, a left $R-$module is an abelian group $M$, written additively, together with a map (called a left action) $R \times M \longrightarrow M$ written $(r,x) \mapsto rx$, $r \in R$, $x \in M$, such that for any $r,s \in R$ and $x,y \in M$ the following hold:*

$$r(x+y) = rx + ry,\ (r+s)x = rx + sx,\ r(sx) = (rs)x,\ 1_R x = x.$$

A right $R-$module is defined in the obvious way via a right action $M \times R \longrightarrow M$. If $R$ is commutative and $M$ is a left $R-$module then one can regard $M$ as a right $R-$module with right action given by $(x,r) \mapsto rx$ for all $r \in R, x \in M$, and hence one can ignore the distinction between right and left modules and just say $M$ is an $R-$module (or a module over $R$). When $R$ is not commutative we shall only consider left $R-$modules $M$ and just call $M$ an $R-$module.

A ring $R$ can be regarded as an $R-$module with left action given by the multiplication in $R$. A module over a field is a vector space. A submodule of an $R-$module $M$ is a subgroup $N$ of $M$ such that $rx \in N$ for all $r \in R$ and $x \in M$. When $R$ is commutative and considered as a module over itself the submodules of $R$ are the ideals of $R$. If $N$ is a submodule of $M$ we shall write $N \leq M$.

If $M$ and $N$ are $R-$modules then a map $f : M \longrightarrow N$ is a *$R-$module homomorphism* (or *$R-$homomorphism* or a *$R-$linear map*) if $f$ is a group homomorphism and for all $r \in R$ and $x \in M$ $f(rx) = rf(x)$. The kernel and image of $f$ are submodules of $M$ and $N$ respectively. As usual if $f$ is injective it is sometimes called a monomorphism *etc.*.

If $M \leq N$ then we can construct the quotient group $M/N$ and this is an $R-$module via the left action $R \times M/N \longrightarrow M/N$, $(r, x+N) \mapsto rx+N$, $M/N$ is called a *quotient module*. As for groups and rings one has the factor theorem and isomorphism theorems.

Let $M_i$, $i \in I$ where $I$ is some indexing set, be $R-$modules and $f_i : M_i \longrightarrow M_{i+1}$ be $R-$homomorphisms for each $i \in I$. The sequence of $R-$modules and homomorphisms

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \longrightarrow \cdots$$

is said to be *exact* at $M_i$ if Im $f_{i-1}$ = Ker $f_i$ and is said to be an *exact sequence* if it is exact at each $M_i$. In particular an exact sequence of the form

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

is called a *short exact sequence* and in this case $M/\text{Ker } g = M/\text{Im } f \cong M''$. We wish to define the *direct sum* of finitely many $R-$modules $M_i$, $i \in I$ a finite indexing set, in general the direct sum is the coproduct in the category of $R-$modules, however we shall give a simple definition which suffices for our purposes.

**Definition A.3.2** *Given a family of $R-$modules $M_i$ indexed by the finite set $I = \{1, \ldots, n\}$, the direct sum of the $M_i$ is the Cartesian product of the $M_i$ with left action defined componentwise and is written*

$$M_1 \oplus M_2 \oplus \ldots \oplus M_n.$$

We note that an $R-$module $M$ is the direct sum of submodules $M_i$, $1 \leq i \leq n$, $n \in \mathbb{N}$, if and only if every element of $M$ can be written uniquely as $x_1 + \cdots + x_n$, $x_i \in M_i$, $1 \leq i \leq n$.

Let $R$ be a commutative ring, an $R-$*algebra* (or an *algebra over* $R$) is a ring $A$ which is also a $R-$module, explicitly in addition to the ring axioms $A$ satisfies

$$(rx)y = x(ry) = r(xy)$$

for all $r \in R$ and $x, y \in A$. We note that if $f : R \longrightarrow$ is a ring homomorphism such that Im $f \subseteq Z(S)$ then $S$ can be viewed as a $R-$module with left action $(r, s) \mapsto f(r)s$ and clearly

$$(rs_1)s_2 = s_1(rs_2) = r(s_1s_2)$$

for all $r \in R$ and $s_1, s_2 \in S$, thus $S$ is a $R-$algebra. In particular lemma A.1.4 shows that any finite ring $R$ is a $\mathbb{Z}/m\mathbb{Z}-$algebra where $m$ is the characteristic of $R$. A homomorphism of $R-$algebras is a ring homomorphism which is $R-$linear.

## A.4 Finite fields

We begin by recalling some relevant facts concerning fields and field extensions, for more detail on finite fields the reader is referred to [26] and for fields and field extensions in general see [25], chapter 3. If $F$ is a field and $f \in F[x]$ then $F[x]/fF[x]$ is a field if and

only if $f$ is irreducible in $F[x]$. Suppose that $F$ has a subfield $K$ then $F$ is called an *extension* of $K$. It is well known that any field either has characteristic 0 or a prime $p$, the best known finite fields are $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ for each prime $p$. A field containing no proper subfields is called a *prime field*, for instance $\mathbb{F}_p$ is a prime field. The intersection of all subfields of a field $F$ is a field, the *prime subfield* of $F$, clearly a prime field, it is well known that the prime subfield of a field $F$ is isomorphic to either $\mathbb{F}_p$ for some prime $p$ or to $\mathbb{Q}$, depending upon the characteristic of $F$.

Let $K$ be a subfield of $F$ and let $\theta \in F$, then the field $K(\theta)$ is the intersection of all subfields of $F$ containing both $K$ and $\theta$ and is called a *simple extension* of $K$ with defining element $\theta$. If $\theta$ satisfies a non-trivial polynomial equation with coefficients in $K$ then $\theta$ is *algebraic over* $K$ and an extension $L$ of $K$ is called *algebraic* over $K$ (or an *algebraic extension*) if every element of $L$ is algebraic over $K$. If $\theta$ is algebraic over $K$ then there is a uniquely defined monic polynomial $g \in K[x]$, called the *minimal polynomial* of $\theta$ over $K$, such that (i) $g$ is irreducible in $K[x]$, (ii) $f \in K[x]$ has $f(\theta) = 0$ if and only if $g|f$, (iii) $g$ is the monic polynomial of least degree in $K[x]$ having $\theta$ as a root. The *degree* of $\theta$ over $K$ is the degree of its minimal polynomial. $K(\theta)$ can be viewed as a vector space over $K$ (in fact it is a $K-$algebra), the dimension of $K(\theta)$ is called the *degree* of $K(\theta)$ over $K$ and is denoted by $[K(\theta) : K]$. The proofs of the following two theorems can be found in [26].

**Theorem A.4.1** *Let $\theta \in F$ be algebraic of degree $n$ over $K$ and let $g$ be the minimal polynomial of $\theta$ over $K$. Then*

(i) $K(\theta) \cong K[x]/gK[x]$;

(ii) $[K(\theta) : K] = n$ *and* $\{1, \theta, \ldots, \theta^{n-1}\}$ *is a basis of* $K(\theta)$ *over* $K$;

(iii) *Every element* $\alpha \in K(\theta)$ *is algebraic over* $K$ *and its degree over* $K$ *is a divisor of* $n$. ■

**Theorem A.4.2** *Let $f \in K[x]$ be irreducible over a field $K$, then there is a simple algebraic extension of $K$ with a root of $f$ as a defining element. Suppose $\alpha, \beta$ are two roots of $f$, then $K(\alpha) \cong K(\beta)$* ■

The rest of this section consists of a collection of results concerning finite fields, the proofs can all be found in [26].

**Theorem A.4.3** *Let $F$ be a finite field, then $F$ has $p^n$ elements where prime $p$ is the characteristic of $F$ and $n$ is the degree of $F$ as a vector space over the prime subfield $\mathbb{F}_p$*

*of $F$. For every prime $p$ and every integer $n > 0$ there is a finite field with $p^n$ elements, unique up to isomorphism.* ■

The finite field with $p^n$ elements is usually denoted by $\mathbb{F}_{p^n}$ in this document.

**Theorem A.4.4** *The finite field $\mathbb{F}_{p^n}$ has exactly one subfield of order $p^m$ for each positive divisor $m$ of $n$ and these are all the subfields of $\mathbb{F}_{p^n}$.* ■

**Theorem A.4.5** *In the finite field $\mathbb{F}_{p^n}$ the group of units $\mathbb{F}_{p^n}^*$ is cyclic.* ■

Theorem A.4.5 shows that, where we use basic facts about cyclic groups, for each positive divisor $m$ of $p^n - 1$, $\mathbb{F}_{p^n}$ contains $\phi(m)$ elements of order $m$, where $\phi$ is eulers function, the value of $\phi(m)$ is the number of integers $j$ with $1 \leq j \leq m$ coprime to $m$.

We note that in $\mathbb{F}_p[x]$ there are irreducible monic polynomials of every positive degree, hence every finite field can be represented as $\mathbb{F}_p[x]/f\mathbb{F}_p[x]$ for some monic irreducible $f \in \mathbb{F}_p[x]$. If $f = \sum_{i=0}^{n} a_i x^i$, $a_n = 1$, then letting $\theta$ be a root of $f$ we can use $\{1, \theta, \ldots, \theta_{n-1}\}$ as a basis of $\mathbb{F}_{p^n} \cong \mathbb{F}_p[x]/f\mathbb{F}_p[x]$ as a $\mathbb{F}_p$ algebra and use the relation $\theta^n = -\sum_{i=0}^{n-1} a_i \theta^i$ to simplify expressions arising in arithmetic over $\mathbb{F}_{p^n}$. Similarly there are irreducible polynomials of every degree over $\mathbb{F}_{p^q}$, $q > 1$, and hence every field with $p^{qm}$ elements can be represented by $\mathbb{F}_{p^q}[x]/f\mathbb{F}_{p^q}[x]$ for some polynomial $f$ irreducible over $\mathbb{F}_{p^q}$.

## A.5 Direct products of rings, idempotents and idempotent lifting

### A.5.1 Direct products of rings

**Definition A.5.1** *Let $(R_i), i \in I$ be a family of rings. The direct product of $(R_i), i \in I$ is the Cartesian product of the sets $R_i, i \in I$*

$$R = \prod_{i \in I} R_i$$

*with operations defined component wise, explicitly $(x_i) + (y_i) = (x_i + y_i)$, $(x_i)(y_i) = (x_i y_i)$, $1_R = (1_{R_i})$ and $0_R = (0_{R_i})$.*

It is clear from definition A.5.1 that $R = \prod_{i \in I} R_i$ is a ring, commutative if and only if each $R_i$ is commutative. For $i \in I$ the natural projection $\pi_i : R \longrightarrow R_i$

is a homomorphism. The natural injections $\mu_i : R_i \longrightarrow R$ preserve addition and multiplication and zero but not the identity so the images $\mu_i(R_i)$ are not subrings of $R$ but are ideals of $R$. However $\mu_i(1_{R_i})$ acts as an identity with respect to the elements of $\mu_i(R_i)$ and in fact $\mu_i(R_i)$ is a ring. We shall only be interested in cases where $|I|$ is finite, *i.e.* finite direct products. The proof of the next theorem can be found in Cohn [25], page 171.

**Theorem A.5.1** *Let $R_1, \ldots, R_t$ be any rings and let $R$ be their direct product. With $\pi_i$ and $\mu_i$ as described above $\mathfrak{a}_i = \mathrm{Im}\mu_i$ is an ideal in $R$ and*

$$R = \mathfrak{a}_1 \oplus \ldots \oplus \mathfrak{a}_t. \tag{A.5.1}$$

*Further, $\mathfrak{a}_i\mathfrak{a}_j = 0$ if $i \neq j$ and $\mathfrak{a}_i\mathfrak{a}_i \subseteq \mathfrak{a}_i$. Conversely any ring $R$ of the form (A.5.1) where each $\mathfrak{a}_i$ is an ideal in $R$ may be expressed as a direct product of rings $R_1, \ldots, R_t$ where $R_i$ is isomorphic to $\mathfrak{a}_i$ as a ring.* ■

We shall say that a ring $R$ is *indecomposable* if it cannot be written as a direct product of two rings unless one of them is $R$ and the other is the trivial ring $\{0\}$. When a ring $R$ can be written non-trivially as a direct product it is natural to enquire as to the uniqueness of this direct product. To this end we have the following theorem, proved in Cohn [25], page 173. This theorem refers to *Artinian* and *Noetherian* rings, we shall not digress to define these here, suffice to say that any finite ring is both Artinian and Noetherian, which is sufficient for our purposes.

**Theorem A.5.2** *Any Artinian or Noetherian ring can be written uniquely as a direct product of a finite number of indecomposable rings.* ■

**Definition A.5.2** *A ring $R$ is called completely primary if every element of $R$ is either a unit or nilpotent.*

**Lemma A.5.1** *If $R$ is completely primary then $R$ is indecomposable.*

Proof:

Let $R$ be completely primary and suppose $R \cong R_1 \times R_2$ where $R_1$ and $R_2$ are non-trivial rings. Then the element $(0_{R_1}, 1_{R_2})$ is a non-nilpotent zero-divisor, so its pre-image in $R$ is a non-nilpotent zero-divisor but $R$ is completely primary so this is a contradiction. ■

### A.5.2 Idempotent elements

**Definition A.5.3** *An element $e \in R$ is idempotent if $e^2 = e$.*

Obviously 0 and 1 are always idempotents, the *trivial idempotents*. Let $e, e' \in R$ be idempotent, one says that they are *orthogonal* if $ee' = e'e = 0$. Note that if $e$ is idempotent then so is $1 - e$ and $1 - e$ is orthogonal to $e$. Clearly ring homomorphisms map idempotent elements to idempotent elements.

**Lemma A.5.2** *Let $R$ be a commutative ring and let $e \in R$ be a non-trivial idempotent, then $eR$ is a ring with operations those in $R$ but with identity element $e$ for multiplication.*

Proof:

The principal ideal $eR$ is closed under the operations of $R$ and $0 \in eR$. For any $a \in eR$, $a = eb, b \in R$ and $ea = e^2b = eb = a = be = be^2 = ae$ hence $e$ is the identity in $eR$. ■

Note that $eR$ is *not* a subring of $R$. Note that if $R = \prod_{i \in I} R_i$ then for each $i \in I$, $\mu_i(1_{R_i})$ is idempotent in $R$. This suggests a strong connection between the existence of non trivial idempotents and direct products. We have the following theorem, its proof can be found in Rowen [32].

**Theorem A.5.3** [Pierce Decomposition]

*Let $R$ be a ring, then $R \cong R_1 \times \ldots \times R_t$ as rings if and only if there are pairwise orthogonal idempotents $e_i$ in $Z(R)$ such that $\sum_{i=1}^{t} e_i = 1$ and $R_i \cong Re_i$ for each $i$.* ■

**Example A.5.1**

It is well known that if $m$ is an integer, $m > 0$, with unique factorisation into powers of prime integers $m = \prod_{i=1}^{s} q_i$ where $q_i = p_i^{k_i}$, $p_i$ prime and integer $k_i > 0$, then

$$\mathbb{Z}/m\mathbb{Z} \cong \prod_{i=1}^{s} \mathbb{Z}/q_i\mathbb{Z}.$$

By theorem A.5.3 there are pairwise orthogonal idempotents $e_i$, $1 \leq i \leq s$, such that $\sum_{i=1}^{m} e_i = 1$ and $\mathbb{Z}/q_i\mathbb{Z} \cong e_i\mathbb{Z}/q_i\mathbb{Z}$. For instance one has

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong (3 + 6\mathbb{Z})\mathbb{Z}/6\mathbb{Z} \times (4 + 6\mathbb{Z})\mathbb{Z}/6\mathbb{Z}. \quad \blacklozenge$$

Let $R$ be a commutative ring and suppose $A$ is an ideal in $R$. Under certain circumstances it is possible to lift the idempotents in $R/A$ to idempotents in $R$.

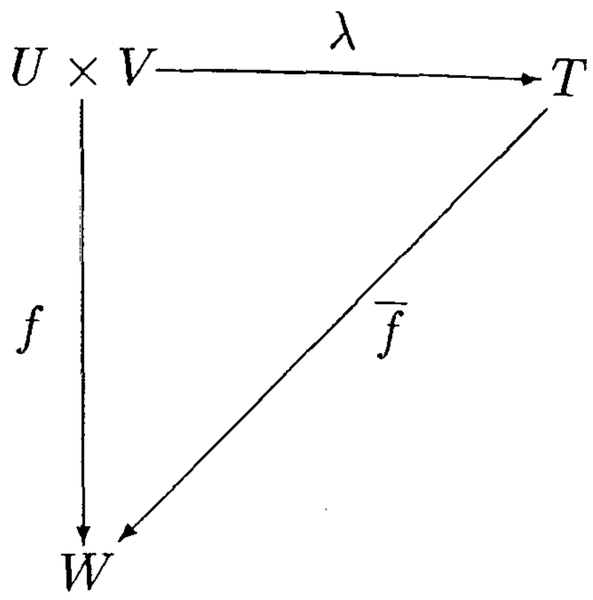


Figure A.4: $T$ is the tensor product of $U$ and $V$, for any bilinear map $f$ there is a unique homomorphism $\overline{f}$ such that $\overline{f} \circ \lambda = f$.

**Definition A.5.4** *An ideal $A \lhd R$ is idempotent lifting if*

(i) $1 - a$ *is a unit for all* $a \in A$;

(ii) *Every idempotent of* $R/A$ *has the form* $x + A$ *where* $x$ *is idempotent in* $R$.

Let $A \lhd R$ be a nil ideal, that is if $a \in A$ then $a$ is nilpotent. Then by remark A.1.1 $A$ satisfies the first condition of definition A.5.4. In fact $A$ also satisfies the second condition. The proof of the following result is in Rowen [32], page 41.

**Lemma A.5.3** *Every nil ideal of a ring $R$ is idempotent lifting, if $\bar{r} = r + A$ is idempotent in $R/A$ then there is an idempotent $e$ in the subring of $R$ generated by $r$ satisfying $\bar{e} = \bar{r}$.* ■

## A.6 The tensor product

Given $R-$modules $U, V$ and $W$, a *bilinear map* is a map $f : U \times V \longrightarrow V$ which is $R-$linear in each argument.

**Definition A.6.1** *Let $R$ be a commutative ring and let $U, V$ be $R-$modules. A tensor product of $U$ and $V$ is a $R-$module $T$ such that there is a bilinear map $\lambda : U \times V \longrightarrow T$ with the property that if $W$ is any $R-$module and $f$ is any bilinear map $f : U \times V \longrightarrow W$ then there is a unique homomorphism $\overline{f} : T \longrightarrow W$ such that (see figure A.4)*

$$\overline{f} \circ \lambda = f.$$

A $R-$module $T$ as in definition A.6.1 is known as a *tensor product* of $U$ and $V$ and is denoted $U \otimes_R V$ or $U \otimes V$ when no confusion can arise. If a tensor product exists then from the definition it follows that it is unique up to isomorphism, in fact the

tensor product always exists, see [25], chapter 4, for the proof of this and we refer the reader to that book for more details on the discussion in the next paragraph.

In definition A.6.1 the image of $(u, v)$ under the bilinear map $\lambda$ is written as $u \otimes v$ and the following relations hold:

$$\begin{aligned}
(u+u')\otimes v &= u\otimes v + u'\otimes v \quad \text{for all } u,u'\in U, v\in V\\
u\otimes(v+v') &= u\otimes v + u\otimes v' \quad \text{for all } u\in U, v,v'\in V\\
(\alpha u)\otimes v &= u\otimes(\alpha v) = \alpha(u\otimes v) \quad \text{for all } u\in U, v\in V, \alpha\in R,
\end{aligned}$$

further, every element of $U \otimes V$ can be written as $\sum_i u_i \otimes v_i$. Given $R-$modules $U, U', V, V'$ and $R-$homomorphisms

$$\alpha : U \longrightarrow U', \quad \beta : V \longrightarrow V',$$

there exists a $R-$homomorphism $\alpha \otimes \beta$:

$$\begin{aligned}
\alpha\otimes\beta : U\otimes V &\longrightarrow U'\otimes V',\\
u\otimes v &\mapsto \alpha(u)\otimes\beta(v).
\end{aligned}$$

**Theorem A.6.1** *Let $U, V, V_1, \ldots V_n$ be $R-$modules then*

(i) $U \otimes V \cong V \times U$;

(ii) $U \otimes (V_1 \oplus \ldots \oplus V_n) \cong (U \otimes V_1) \oplus \ldots \oplus (U \otimes V_n)$;

(iii) *If $R$ is a field and $U$ and $V$ are finite dimensional vector spaces over $R$ then $Dim(U \otimes V) = Dim\ U.Dim\ V$ and if $\{u_i\}$ is a basis for $U$ over $R$ and $\{v_j\}$ is a basis for $V$ over $R$ then $\{u_i \otimes v_j\}$ is a basis for $U \otimes V$ over $R$.*

Proof:

For (i) and (ii) see [25], chapter 4. For (iii) see either [25] or [33], chapter 1, pages 23 – 24. ■

We note that the proof of theorem A.6.1, (ii), when $n = 2$, starts from noting the existence of a bilinear map

$$\begin{aligned}
b : U\times(V_1\oplus V_2) &\longrightarrow (U\otimes V_1)\oplus(U\otimes V_2),\\
(u,(v_1,v_2)) &\mapsto (u\otimes v_1, u\otimes v_2)
\end{aligned}$$

and hence an $R-$homomorphism

$$\begin{aligned}
\overline{f} : U\otimes(V_1\oplus V_2) &\longrightarrow (U\otimes V_1)\oplus(U\otimes V_2),\\
u\otimes(v_1,v_2) &\mapsto (u\otimes v_1, u\otimes v_2),
\end{aligned}$$

and simarly for $n > 2$. We shall also need the following, its proof can be found in [28], pages $610 - 611$.

**Theorem A.6.2** *Let*

$$0 \longrightarrow M \xrightarrow{\phi} M \xrightarrow{\theta} M'' \longrightarrow 0$$

*be an exact sequence of $R-$modules and $F$ any $R-$module, then*

$$F \otimes M \xrightarrow{1\otimes\phi} F \otimes M \xrightarrow{1\otimes\theta} F \otimes M'' \longrightarrow 0$$

*is exact, where we have written 1 for the identity homomorphism on $F$.* ■

We now turn our attention to $R-$algebras, given $R-$algebras $A$ and $B$ one can define $A \otimes B$ and in fact $A \otimes B$ is an $R-$algebra, the proof of the following result can be found in [25], page 185:

**Theorem A.6.3** *Let $R$ be a commutative ring and $A, B$ be $R-$algebras. Then $A \otimes B$ is an $R-$algebra, commutative if $A$ and $B$ are, with identity $1_A \otimes 1_B$ and multiplication defined by*

$$(a_1 \otimes b_1)(a_2 \otimes b_2) = (a_1 a_2 \otimes b_1 b_2).$$ ■

It follows that given $R-$algebra homomorphisms $\alpha : A \longrightarrow A'$ and $\beta : B \longrightarrow B'$ then $\alpha \otimes \beta : A \otimes B \longrightarrow A' \otimes B'$ is an $R-$algebra homomorphism.

Suppose that $A, B, C$ are $R-$algebras and $f : A \otimes B \longrightarrow C$ is a $R-$homomorphism, then to prove that $f$ is a $R-$algebra homomorphism one must show that $f$ maps $1_A \otimes 1_B$ to $1_C$ and that

$$f(a_1 \otimes b_1) f(a_2 \otimes b_2) = f(a_1 a_2 \otimes b_1 b_2)$$

which then extends to every element of $A \otimes B$ by $R-$linearity (as every element of $A \otimes B$ can be written as a sum $\sum_i a_i \otimes b_i$).

**Lemma A.6.1** *Let $R$ be a commutative ring and let $U$ be an $R-$algebra and let $V \times W$ be the direct product of $R-$algebras $V$ and $W$ as rings (and hence a direct sum as modules) then*

$$U \otimes (V \times W) \cong (U \otimes V) \times (U \otimes W)$$

*as $R-$algebras.*

Proof:

The result holds for $U, V$ and $W$ as $R-$modules with $R-$isomorphism $\overline{f} : u \otimes (v, w) \mapsto (u \otimes v, u \otimes w)$. It is easy to see that

$$\overline{f}(u_1 \otimes (v_1, w_1))\overline{f}(u_2 \otimes (v_2, w_2)) = \overline{f}(u_1 u_2 \otimes (v_1 v_2, w_1 w_2)),$$

and this extends by $R-$linearity to the whole algebra, also clearly $\overline{f}(1 \otimes (1,1)) = (1,1) \otimes (1,1)$, hence $\overline{f}$ is an $R-$algebra isomorphism. ■

**Theorem A.6.4** *Suppose that $k$ is a field and $K$ is a commutative ring with $k \subseteq K$. Then $K \otimes_k k[x] \cong K[x]$.*

Proof:

We have a bilinear map $\lambda : (\gamma, g) \mapsto \gamma g$ inducing a $k-$linear map

$$\begin{array}{rcl} \overline{f} : K \otimes_k k[x] & \longrightarrow & K[x], \\ \gamma \otimes_k g & \mapsto & \gamma g. \end{array}$$

Given $h \in K[x]$, $h = \sum_{j=0}^{d} h_j x^j$, then $\sum_{j=0}^{d} h_j \otimes_k x^j$ is a pre-image of $h$ and hence $\overline{f}$ is surjective. Suppose that $\sum_i (\gamma_i \otimes_k g_i) \mapsto 0$, then

$$\sum_i \gamma_i g_i = 0 \;\Rightarrow\; \sum_i \gamma_i g_{i,0} + \sum_i \gamma_i g_{i,1} x + \ldots = 0 \;\Rightarrow\; \sum_i \gamma_i g_{i,j} = 0$$

for each $j$, but then

$$\begin{array}{rcl} \sum_i (\gamma_i \otimes_k g_i) & = & \sum_i (\gamma_i \otimes_k \sum_j g_{i,j} x^j) \\ & = & \sum_i \sum_j (\gamma_i \otimes_k g_{i,j} x^j) \\ & = & \sum_i \sum_j (g_{i,j} \gamma_i \otimes_k x^j) \\ & = & \sum_j (\sum_i g_{i,j} \gamma_i \otimes_k x^j) \\ & = & \sum_j (0 \otimes_k x^j) \\ & = & 0, \end{array}$$

thus Ker $\overline{f} = \{0\}$ and $\overline{f}$ is injective and hence a $k-$isomorphism. Clearly $1 \otimes_k 1 = 1$ and

$$\overline{f}(\gamma_1 \otimes_k g_1)\overline{f}(\gamma_2 \otimes_k g_2) = \overline{f}(\gamma_1\gamma_2 \otimes_k g_1 g_2),$$

which extends to all of $K \otimes_k k[x]$ by $k-$linearity, hence $\overline{f}$ is a $k-$algebra isomorphism.

■

Given a principal ideal $gk[x] \lhd k[x]$ we have the exact sequence

$$0 \longrightarrow gk[x] \xrightarrow{\iota} k[x] \xrightarrow{\pi} k[x]/gk[x] \longrightarrow 0,$$

where $\iota$ is inclusion and $\pi$ is the natural projection. Then by theorem A.6.2 we have an exact sequence

$$K \otimes_k gk[x] \xrightarrow{1\otimes\iota} K \otimes_k k[x] \xrightarrow{1\otimes\pi} K \otimes_k k[x]/gk[x] \longrightarrow 0.$$

Further, there is a natural isomorphism $K \otimes_k gk[x] \longrightarrow gK[x]$,

$$K \otimes_k gk[x] \longrightarrow (1 \otimes_k g)K \otimes_k k[x] \longrightarrow gK[x]$$

and we have the exact sequence

$$gK[x] \longrightarrow K[x] \longrightarrow K \otimes_k k[x]/gk[x] \longrightarrow 0$$

hence

$$K[x]/gK[x] \cong K \otimes_k k[x]/gk[x]. \tag{A.6.1}$$

# Appendix B

# Proofs of results omitted from the main text

## B.1 Proofs of results from chapter 2

**Proof of lemma 2.1.12**

Firstly $\mathbb{T}_U^T(a) = \mathbb{T}^T a + \mathbb{T}_U^T(0)$ and $\mathbb{T}^T a \in C_0(a)$, $\mathbb{T}_U^T(0) \in C_U(0)$. Hence

$$\mathbb{T}_U^{T+d}(a) = \mathbb{T}^{T+d} a + \mathbb{T}_U^{T+d}(0) = \mathbb{T}^T a + \mathbb{T}_U^T(0) = \mathbb{T}_U^T(a)$$

so $(\phi_a)_U | d$.

We prove (i), the other parts are similar:

If $(\phi_a)_U | (\phi_0)_U$ then

$$\begin{aligned} & T_U^{T+(\phi_0)_U}(a) = \mathbb{T}_U^T(a) \\ \Rightarrow \quad & \mathbb{T}^{T+(\phi_0)_U} a + \mathbb{T}_U^{T+(\phi_0)_U}(0) = \mathbb{T}^T a + \mathbb{T}_U^T(0) \\ \Rightarrow \quad & \mathbb{T}^{T+(\phi_0)_U} a = \mathbb{T}^T a \end{aligned}$$

so $(\phi_a)_0 | (\phi_0)_U$. Conversely, if $(\phi_a)_0 | (\phi_0)_U$ then

$$\begin{aligned} T_U^{T+(\phi_0)_U}(a) &= \mathbb{T}^{T+(\phi_0)_U} a + \mathbb{T}_U^T(0) \\ &= \mathbb{T}^T a + \mathbb{T}_U^T(0) \\ &= \mathbb{T}_U^T(a) \end{aligned}$$

So $(\phi_a)_U | (\phi_0)_U$. ■

**Proof of lemma 2.2.2**

((i) $\Rightarrow$ (ii)) This follows by theorem 2.2.2 as distinct cosets are disjoint.

((ii) $\Rightarrow$ (i)) Obvious.

((ii) $\Rightarrow$ (iv)) Let $Att(\mathbb{T}_U) = Att(\mathbb{T}_V)$ and let $a \in Att(\mathbb{T}_U)$ and let $k = \text{lcm}((\phi_a)_U, (\phi_a)_V)$ then

$$\begin{aligned} & \mathbb{T}_U^k(a) = \mathbb{T}_V^k(a) \\ \Rightarrow \quad & \mathbb{T}_{U-V}^k(0) = 0. \end{aligned}$$

Thus $0 \in C_{U-V}(0)$.

((iv) $\Rightarrow$ (ii)) We have that, for any $n \in \mathbb{N}$,

$$\begin{aligned} & \mathbb{T}_{U-V}^{n(\phi_0)_{U-V}}(0) = 0 \\ \Rightarrow \quad & \mathbb{T}_U^{n(\phi_0)_{U-V}}(0) = \mathbb{T}_V^{n(\phi_0)_{U-V}}(0). \end{aligned} \tag{B.1.1}$$

Let $a \in Att(\mathbb{T}_U)$ and let $l = \text{lcm}((\phi_0)_{U-V}, (\phi_a)_U) = n'(\phi_0)_{U-V}$ for some integer $n' > 0$. Then

$$\begin{aligned} \mathbb{T}_V^l a &= \mathbb{T}^l a + \mathbb{T}_V^l(0) \\ &= \mathbb{T}^l a + \mathbb{T}_U^l(0) \text{ by (B.1.1)} \\ &= a \end{aligned}$$

so $a \in Att(\mathbb{T}_V)$ for all $a \in Att(\mathbb{T}_U)$.

((iv) $\Rightarrow$ (iii)) Let $U - V = W$ then $0 \in C_W(0)$ so $\mathbb{T}_W^k(0) = 0$ for some integer $k > 0$, thus

$$(\mathbb{T}^{k-1} + \ldots + \mathbb{T} + 1)W = 0 \qquad \text{(B.1.2)}$$

$$(\mathbb{T}^k + \mathbb{T}^{k-1} + \ldots + \mathbb{T} + 1)W = W. \qquad \text{(B.1.3)}$$

Subtracting (B.1.2) from (B.1.3) gives $W = \mathbb{T}^k W$ so $W \in Att(\mathbb{T})$.

((iii) $\Rightarrow$ (iv)) Let $W \in Att(\mathbb{T})$ where $W = U - V$, let $k = (\phi_W)_0$, then $\mathbb{T}_W^k(0)$ is fixed by $\mathbb{T}$ by remark 2.1.3. This yields, with $c$ being the characteristic of $R$,

$$\begin{aligned} \mathbb{T}_W^k(0) &= (\mathbb{T}^{k-1} + \ldots + \mathbb{T} + 1)W \\ \mathbb{T}_W^{2k}(0) &= 2\mathbb{T}_W^k(0) \\ &\vdots \quad \vdots \\ \mathbb{T}_W^{ck}(0) &= c\mathbb{T}_W^k(0) = 0. \end{aligned}$$

Thus $0 \in C_{U-V}(0)$.

((v) $\Leftrightarrow$ (iv)) This follows since (ii) $\Leftrightarrow$ (iv), just take $U = U' - V'$ and $V = 0$ in (ii) and (iv). ■

## B.2 Proofs of results from chapter 3

**Proof of lemma 3.3.5**

(i) This is true by lemma 2.1.5.

(ii) If $a, b \in$ Ker $\pi_{r,0}$ and $(\phi_a)_0 \neq (\phi_b)_0$ then

$$\begin{aligned} a(x) &= R(x)^s f(x) \\ b(x) &= R(x)^{s'} f'(x) \end{aligned}$$

for some $f(x), f'(x) \in \mathbb{F}_{p^q}[x]$, $R(x) \nmid f(x)$, $R(x) \nmid f'(x)$ and $0 < s, s' < p^r$. Then

$$\mathbb{T}^{(\phi_a)_0} a = a \quad \Rightarrow \quad (\mathbb{T}(x)^{(\phi_a)_0} - 1)a(x) = \alpha(x)R(x)^{p^r}$$

for some $\alpha(x) \in \mathbb{F}_{p^q}[x]$ so $R(x)^{p^r-s} | (\mathbb{T}(x)^{(\phi_a)_0} - 1)$. Similarly $R(x)^{p^r-s'} | (\mathbb{T}(x)^{(\phi_b)_0} - 1)$. Suppose $s' \leq s$ then $R(x)^{p^r-s} | (\mathbb{T}(x)^{(\phi_b)_0} - 1)$ so for some $\beta(x) \in \mathbb{F}_{p^q}[x]$ one has

$$\begin{aligned}
(\mathbb{T}(x)^{(\phi_b)_0} - 1) &= \beta(x)R(x)^{p^r-s} \\
\Rightarrow \quad (\mathbb{T}(x)^{(\phi_b)_0} - 1)a(x) &= \beta(x)f(x)R(x)^{p^r} \\
\Rightarrow \quad (\mathbb{T}^{(\phi_b)_0} - 1)a &= 0 \\
\Rightarrow \quad (\phi_a)_0 | (\phi_b)_0.
\end{aligned}$$

If $s < s'$ a similar argument yields $(\phi_b)_0 | (\phi_a)_0$. ■

**Proof of lemma 3.3.7**

(i) The number of elements of $\mathbb{F}_{p^q}[x]$ with degree less than or equal to $l$ is clearly $p^{q(l+1)}$ for given $l$. The requirement that we exclude zero gives the result.

(ii) Let $a(x) \in \mathcal{D}_R(l, s)$, then $a(x) = \alpha(x)R(x)^s$ where deg $\alpha(x) \leq l - sd$ hence $a(x) \in R(x)^s A(l - sd)$ and $R(x)^{s+1} \nmid a(x)$ and so $R(x) \nmid \alpha(x)$ hence $a \notin R(x)^{s+1} A(l-(s+1)d)$.

Now suppose that $a \in R(x)^s A(l-sd) \backslash R(x)^{s+1} A(l-(s+1)d)$, then $a(x) = \alpha(x)R(x)^s$ for some $\alpha(x)$ with deg $\alpha(x) \leq l - sd$ and $R(x) \nmid \alpha(x)$ for if $R(x) \mid \alpha(x)$ then $a(x) \in R(x)^{s+1} A(l - (s + 1)d)$, which is not the case, hence $a(x) \in \mathcal{D}_R(l, s)$.

(iii) Using part (ii) we have

$$\begin{aligned}
|\mathcal{D}_R(p^r d - 1, s)| &= |R(x)^s A(l - sd) \setminus R(x)^{s+1} A(l - (s + 1)d)| \\
&= |R(x)^s A(l - sd)| - |R(x)^{s+1} A(l - (s + 1)d)|,
\end{aligned}$$

and hence using part (i) gives

$$|\mathcal{D}_R(p^r d - 1, s)| = p^{q(l-sd+1)} - p^{q(l-sd-d+1)} = p^{q(l-sd-d+1)}(p^{qd} - 1).$$

The last bit follows on putting $l = p^r d - 1$ in the above. ■

**Proof of lemma 3.3.13**

$\mathbb{T} \in \mathcal{D}_R(p^r d - 1, I), I > 0$ so $\mathbb{T} = \alpha R^I$ where $R(x) \nmid \alpha(x)$. We have

$$\begin{aligned}
\mathbb{T}^L \beta_1 R^{I_a} = \mathbb{T}^L \beta_2 R^{I_a} &\Leftrightarrow \mathbb{T}^L R^{I_a}(\beta_1 - \beta_2) = 0 \\
&\Leftrightarrow \alpha^L R^{IL+I_a}(\beta_1 - \beta_2) = 0 \\
&\Leftrightarrow R(x)^{p^r-(IL+I_a)} | \beta_1(x) - \beta_2(x).
\end{aligned}$$

Suppose that $I_{a'} \neq I_a$ where $IL + I_a < p^r$ and $IL + I_{a'} < p^r$. We can suppose, without loss of generality, that $I_{a'} = I_a + J$ for some $J > 0$, then

$$\begin{aligned} & \mathbb{T}^L \beta_1 R^{I_a} = \mathbb{T}^L \beta_2 R^{I_{a'}} \\ \Rightarrow \quad & \alpha^L R^{IL+I_a}(\beta_1 - R^J \beta_2) = 0 \\ \Rightarrow \quad & R(x) | \beta_1(x) - R^J(x)\beta_2(x) \end{aligned}$$

but $R(x) \nmid \beta_1(x)$ so $R(x) \nmid \beta_1(x) - R^J(x)\beta_2(x)$, a contradiction. ■

**Proof of lemma 3.3.18**

We first show that if $(\phi_U)_0 = p^e$, $e < S$, then $(\phi_0)_U = p^{e+1}$ for $(\phi_U)_0 = p^e \Rightarrow$ $Ip^e + I_U \geq p^r$ and $e < S \Rightarrow Ip^e < p^r$. If $\mathbb{T}_U^{p^e}(0) = 0$ then using lemma 3.3.15

$$(\mathbb{T} - 1)^{p^e - 1} U = 0 \;\Rightarrow\; Ip^e - I + I_U \geq p^r \;\Rightarrow\; Ip^e + I_U \geq p^r + I,$$

but $p^r + I > Ip^e + I > Ip^e + I_U$ so we have a contradiction hence $\mathbb{T}_U^{p^e}(0) \neq 0$ so by lemma 3.3.16 $\mathbb{T}_U^{p^{e+1}}(0) = 0$ and $(\phi_0)_U = p^{e+1}$.

We now consider the case $(\phi_U)_0 = p^S$, then with $Ip^S = p^r + V$, we claim that one has

$$\begin{aligned} (\phi_0)_U &= p^S \quad \text{if} \quad I_U + V \geq I \\ (\phi_0)_U &= p^{S+1} \quad \text{if} \quad I_U + V < I. \end{aligned}$$

for

$$\mathbb{T}_U^{p^S}(0) = 0 \;\Leftrightarrow\; I(p^S - 1) + I_U \geq p^r \;\Leftrightarrow\; p^r + V + I_U \geq p^r + I \;\Leftrightarrow\; V + I_U \geq I.$$

The claim now follows by lemma 3.3.16.

We now show that if $0 < I_U < I$ then $(\phi_U)_0 \in \{p^{S-1}, p^S\}$, for if $S = 0$ then $\mathbb{T} = 1$ and so clearly $(\phi_0)_U = p$ for non-zero $U$. If $S = 1$ then we must have $(\phi_U)_0 \in \{1, p\}$. With these cases dealt with it suffices to show that $Ip^{S-2} + I_U < p^r$ for $S \geq 2$, this is true as

$$Ip^{S-2} + I_U < Ip^{S-2} + I = I(p^{S-2} + 1) < Ip^{S-1} < p^r$$

by the definition of $S$. The result now follows. ■

**Proof of lemma 3.3.19**

Recall from theorem 3.3.1 that $p^n \leq I < p^{n+1} \Rightarrow S = r - n$. For $J = 0$ we have that $p^n(p^{r-n} - 1) = p^r - p^n < p^r$ for any integer $n$. If $n < r - n$ and $J > 0$ we examine $I(p^S - 1)$,

$$I(p^S - 1) = (p^n + J)(p^{r-n} - 1) = p^r + Jp^{r-n} - p^n - J,$$

now $J(p^{r-n} - 1) \geq p^{r-n} - 1 \geq p^n$ as $r - n > n$, hence $I(p^S - 1) \geq p^r$ for all allowed $J > 0$ when $n < r - n$. When $n = r - n$ one has

$$I(p^S - 1) = (p^n + J)(p^{r-n} - 1) = p^r + p^n(J - 1) - J,$$

which is less that $p^r$ if $J \leq 1$ but otherwise $J(p^n - 1) \geq 2p^n - 2 - p^n \geq p^n - 2 \geq 0$ (cannot have $n = 0$ in this case for then $r = 0$). When $n > r - n$ one has

$$I(p^S - 1) = p^r + Jp^{r-n} - p^n - J,$$

as a function of $J$ this is clearly linear and increasing, we find the least value of $J$ such that the expression is $\geq 0$. For $\overline{J} \in \mathbb{R}$ we have

$$\overline{J}p^{r-n} - p^n - \overline{J} = 0 \Rightarrow \overline{J} = \frac{p^n}{p^{r-n} - 1},$$

hence $J = \lceil \overline{J} \rceil$ (note that $J \geq 1$).

Now suppose that $\{\mathbb{T}_v\}_{v \in \mathbb{N}}$ is such that $\mathbb{T}_v \in \frac{\mathbb{F}_{p^q}[x]}{R(x)^{p^{r+v}}\mathbb{F}_{p^q}[x]}$ with $\pi_{r+v}(\mathbb{T}_v) = \mathbb{T}$, then by lemma 3.3.11 we have that for all $v \in \mathbb{N}$ that $L(\mathbb{T}_v) = L(\mathbb{T}) = L$, say, and as $I < p^r$ we have, for all $v \in \mathbb{N}$ that $\mathcal{I}(\mathbb{T}_v^L - 1) = I$, also $S_{\mathbb{T}_v} = S + v$. Clearly if $J = 0$ then

$$I(p^{S+v} - 1) = p^n(p^{r-n+v} - 1) = p^{r+v} - p^n < p^{r+v}$$

for all $v \in \mathbb{N}$, otherwise $J > 0$ and

$$I(p^{S+v} - 1) = (P^n + J)(p^{r-n+v} - 1) = p^{r+v} + Jp^{r-n+v} - p^n - J$$

and clearly there is some $v^* \in \mathbb{N}$ such that for all $v > v^*$ one has $Jp^{r-n+v} \geq p^n + J$ and hence $I(p^{S+v} - 1) \geq p^{r+v}$ for all $v > v^*$. ■

**Proof of lemma 3.3.20**

Under the conditions of the lemma let $W \in \mathcal{D}_R(p^{r+v}d - 1, I_U)$, $v \in \mathbb{N}$. We have that, by lemma 3.3.11, $S_{\mathbb{T}_v} = S + v$ and $\mathbb{T}_v - 1 \in \mathcal{D}_R(p^{r+v}d - 1, I)$. We showed in the

proof of lemma 3.3.18 that $(\phi_W)_0 \in \{p^{S+v-1}, p^{S+v}\}$. If $(\phi_W)_0 = p^{S+v-1}$ then we must have $Ip^{S+v-1} + I_U \geq p^{r+v}$ and so

$$I > I_U \geq p^{r+v} - Ip^{S+v-1}. \tag{B.2.1}$$

Now, $0 < I < p^r$, hence $p^n \leq I < p^{n+1}$ where $n < r$ so $I = p^n + J$, $0 \leq J < p^{n+1} - p^n$ so (B.2.1) is

$$I > I_U > p^{r+v}\left(1 - \frac{p^n + J}{p^{n+1}}\right)$$

but $J < p^{n+1} - p^n$ so $\frac{p^n+J}{p^{n+1}} < 1$ and so $p^{r+v}\left(1 - \frac{p^n+J}{p^{n+1}}\right) > 0$ for all $v \in \mathbb{N}$ and clearly increases with $v$, hence there must exist $v^*$ such that if $v \geq v^*$ then (B.2.1) is not satisfied, i.e. $I_U < p^{r+v} - Ip^{S+v-1}$ and thus for all $v \geq v^*$ and any $W \in \mathcal{D}_R(p^{r+v}d-1, I_U)$ one must have $(\phi_W)_0 = p^{S+v}$. ■

## B.3 Proofs of results from chapter 4

### Proof of lemma 4.2.4

Suppose $f$ has radius $l$, say

$$f(a_{i-l}, \ldots, a_{i+l}) = \alpha_0 a_i + \sum_{j=1}^{l} (\alpha_{-j} a_{i-j} + \alpha_j a_{i+j}).$$

$f$ is not the trivial rule so at least one of the $\alpha_s$, $-l \leq s \leq l$, is non-zero. Let $r'$ be the least $r \in \mathbb{N}$ with $np^{r'} > l$. For all $r \in \mathbb{N}$ one has

$$\mathbb{T}_r = \mathbb{T}_r(x) + (x^{np^r} - 1)\mathbb{F}_{p^q}[x]$$

and for $k \in \mathbb{N}$

$$\mathbb{T}_{r'+k}(x) = \sum_{j=0}^{l} \alpha_{-j} x^j + \sum_{j=1}^{l} \alpha_j x^{np^{r'+k}-j} = \sum_{j=0}^{l} \alpha_{-j} x^j + A_{r'+K}(x).$$

Now, for all $k \in \mathbb{N}$,

$$A_{r'+K}(x) = \sum_{j=1}^{l} \alpha_j x^{np^{r'+k}-j} = x^{np^{r'}(p^k-1)} \sum_{j=1}^{l} \alpha_j x^{np^{r'}-j} = x^{np^{r'}(p^k-1)} A_{r'}(x).$$

Suppose $R(x) = R_i(x)$ where $i \in M_0(\mathbb{T})$, let $D$ be the maximum power of $R(x)$ dividing $A_{r'}(x)$ ($D$ may be zero) then clearly $D$ is the maximum power of $R(x)$ dividing $A_{r'+k}(x)$ for all $k \in \mathbb{N}$.

We suppose that $\{\mathbb{T}_{r,i}\}_{r\in\mathbb{N}}$ is the trivial $R(x)$-set, then $R(x)^{p^{r'+k}} | \mathbb{T}_{r'+k}(x)$ for all $k \in \mathbb{N}$, let $e_{r'+k}$ be the maximum integer such that $R(x)^{p^{r'+k}+e_{r'+k}} | \mathbb{T}_{r'+k}(x)$. In particular

$$\mathbb{T}_{r'}(x) = R(x)^{p^{r'}+e_{r'}}\delta_{r'}(x), \quad R(x) \nmid \delta_{r'}(x).$$

First stage: We show that under the hypothesis that $\{\mathbb{T}_{r,i}\}_{r\in\mathbb{N}}$ is the trivial $R(x)$-set one must have $e_{r'+k} = D$ for all $k \in \mathbb{N}$. One has

$$\begin{aligned}
\mathbb{T}_{r'}(x) &= \sum_{j=0}^{l} \alpha_{-j}x^j + A_{r'}(x) \\
\mathbb{T}_{r'+1}(x) &= \mathbb{T}_{r'}(x) + (x^{n(p-1)} - 1)^{p^{r'}} A_{r'}(x) \\
\mathbb{T}_{r'+1}(x) &= \mathbb{T}_{r'+1}(x) + (x^{n(p-1)} - 1)^{p^{r'+1}} A_{r'+1}(x) \\
&= \mathbb{T}_{r'}(x) + (x^{n(p-1)} - 1)^{p^{r'}} A_{r'}(x) + (x^{n(p-1)} - 1)^{p^{r'+1}} x^{np^{r'}(p-1)} A_{r'}(x),
\end{aligned}$$

and inductively for all $k \in \mathbb{N}$

$$\mathbb{T}_{r'+k}(x) = \mathbb{T}_{r'}(x) + \left(\sum_{i=0}^{k-1}(x^{n(p-1)} - 1)^{p^{r'}+i}x^{v_i}\right) A_{r'(x)} \tag{B.3.1}$$

where $v_i = np^{r'}(p^i - 1)$. The maximum power of $R(x)$ dividing the second term of (B.3.1) is $D+p^{r'}$ for, as $\gcd(p, n(p-1)) = 1$, $(x^{n(p-1)}-1)$ is separable and $x^n - 1 | x^{n(p-1)} - 1$, by corollary A.2.1, hence $R(x)$ divides $x^{n(p-1)} - 1$ only once (by separability) and so divides $(x^{n(p-1)} - 1)^{p^{r'}}$ exactly $p^{r'}$ times which implies that

$$R(x)^{p^{r'}+D} \left| \left(\sum_{i=0}^{k-1}(x^{n(p-1)} - 1)^{p^{r'}+i}x^{v_i}\right) A_{r'(x)} \right.$$

and no larger power of $R(x)$ does. As $e_{r'}$ is finite one can always choose $k$ large enough that $\max(D + p^{r'}, e_{r'} + p^{r'}) < p^{r'+k}$ hence $D + p^{r'} = e_{r'} + p^{r'}$ or dividing (B.3.1) by $R(x)^{\min(D+p^{r'}, e_{r'}+p^{r'})}$ will show that $R(x)^{p^{r'+k}}$ cannot divide $\mathbb{T}_{r'+k}(x)$ for such $k$, a contradiction, hence $D = e_{r'}$. Repeating the above argument with $r'$ replaced by $r'+s$,

$s \in \mathbb{N}$, shows that $e_{r'+s} = D$ for all $s \in \mathbb{N}$ or $\{\mathbb{T}_{r,i}\}_{r\in\mathbb{N}}$ is not the trivial $R(x)$-set, thus the exact power of $R(x)$ dividing $\mathbb{T}_{r'+k}(x)$ is $R(x)^{p^{r'}+k}+D$ for all $k \in \mathbb{N}$.

Second stage: Let

$$\gamma_{r'}(x) = \frac{(x^{n(p-1)}-1)^{p^{r'}} A_{r'}(x)}{R(x)^{p^{r'}+D}}$$

so $R(x) \nmid \gamma_{r'}(x)$. Thus $\frac{\mathbb{T}_{r'+1}(x)}{R(x)^{p^{r'}+D}} = \delta_{r'}(x)+\gamma_{r'}(x)$ and $R(x)^{p^{r'}+D-(p^{r'}+D)} = R(x)^{p^{r'}(p-1)}$ is the exact power of $R(x)$ dividing $\delta_{r'}(x)+\gamma_{r'}(x)$. Let

$$\beta_k(x) = \frac{\left(\sum_{i=1}^{k-1}(x^{n(p-1)}-1)^{p^{r'}+i}x^{v_i}\right) A_{r'(x)}}{R(x)^{p^{r'}+D}}$$

then for all $k \geq 2$ the maximum power of $R(x)$ dividing $\beta_k(x)$ is $R(x)^{p^{r'}}$. By (B.3.1) one has

$$\frac{\mathbb{T}_{r'+k}(x)}{R(x)^{p^{r'}+D}} = \delta_{r'}(x)+\gamma_{r'}(x)+\beta_k(x),$$

hence, unless $p^{r'}(p-1) = p^{r'}$ one obtains a contradiction of $R(x)^{p^{r'}+k} | \mathbb{T}_{r'+k}(x)$, but $p^{r'}(p-1) = p^{r'}$ if and only if $p = 2$ and $r' = 0$, in that case just repeat stage two with $r' = 1$. ■

**Proof of lemma 4.2.5**

Clearly $\mathbb{T} \in \frac{\mathbb{F}_{p^q}[x]}{(x^{np^r}-1)\mathbb{F}_{p^q}[x]}$ is a unit if and only if $M_0^r(\mathbb{T}) = \emptyset$. It follows, by a simple counting argument, that

$$|U_{p^q}(n)| = \prod_{i=1}^{m} |U_{P^q}(R_i)| = \prod_{i=1}^{m} |\mathbb{F}^*_{p^{qd_i}}| = \prod_{i=1}^{m}(p^{qd_i}-1).$$

then

$$\begin{aligned}
|U_{p^q}(np^r)| &= \prod_{i=1}^{m} |U_{p^q}(R_i, r)| \\
&= \prod_{i=1}^{m} p^{qd_i(p^r-1)}(p^{qd_i}-1) \quad \text{(by lemma 3.3.3)} \\
&= p^{q(p^r-1)\sum_{i=1}^{m} d_i} \prod_{i=1}^{m}(p^{qd_i}-1) \\
&= p^{qn(p^r-1)} \left|U_{p^q}(n)\right|,
\end{aligned}$$

The number of zero divisors for $r = 0$ then follows because in a finite ring every element is either a unit or a zero divisor. For $r > 0$ one has

$$\begin{aligned} |ZD_{pq}(np^r)| &= p^{qnp^r} - |U_{pq}(np^r)| \\ &= p^{qnp^r} - p^{qn(p^r-1)}\,|U_{pq}(n)| \\ &= p^{qn(p^r-1)}\,(p^{qn} - |U_{pq}(n)|) \\ &= p^{qn(p^r-1)}\,|ZD_{pq}(n)|\,. \quad \blacksquare \end{aligned}$$

**Proof of lemma 4.2.8**

(i) The expression for $\Pi_n(\mathbb{T})$ follows immediately from lemma 3.2.1, (ii). Using theorem 3.3.2 one sees that

$$\begin{aligned} \Pi_{np^r}(\mathbb{T}) &= \mathrm{lcm}_{i\in M\setminus M_0^r(\mathbb{T})}(\Pi(\theta_r^i(\mathbb{T}))) \\ &= \mathrm{lcm}_{i\in M\setminus M_0^r(\mathbb{T})}(L(\mathbb{T}_i)p^{S(\mathbb{T}_i)}) \\ &= p^S\mathrm{lcm}_{i\in M\setminus M_0^r(\mathbb{T})}(O(\pi_{r,0}^i(\theta_r^i(\mathbb{T})))) \\ &= p^S\Pi_n(\Gamma_{r,0}(\mathbb{T})), \end{aligned}$$

noting that $M_0^r(\mathbb{T}) = M_0(\Gamma_{r,0}(\mathbb{T}))$.

(ii) For all $r \in \mathbb{N}$ it is clear that $Att(\mathbb{T}) = \{a : a_i = 0\ \forall\ i \in M_0^0(\mathbb{T})\}$, for $r = 0$ the number of elements of this type is

$$|Att(\mathbb{T})| = \prod_{M\setminus M_0^0(\mathbb{T})} p^{qd_i} = p^{q\sum_{M\setminus M_0^0(\mathbb{T})} d_i}.$$

For $r > 0$ one has

$$|Att(\mathbb{T})| = p^{p^rq\sum_{i\in M\setminus M_0^r(\mathbb{T})} d_i} = p^{p^rq\sum_{i\in M\setminus M_0}(\Gamma_{r,0}(\mathbb{T}))d_i} = |Att(\Gamma_{r,0}(\mathbb{T}))|^{p^r}$$

(iii) For all $r \in \mathbb{N}$, clearly if $a$ is such that $\overline{M}_0^r(a) \not\subseteq M_0^r(\mathbb{T})$ then $a$ will be transient under $\mathbb{T}$ so if $i \in \overline{M}_0^r(a) \cup M_0^r(\mathbb{T})$ then $a_i$ makes no contribution to $(\phi_a)_0$, the result for $r = 0$ follow immediately on reference to lemma 3.2.1. For $r > 0$

$$\begin{aligned} (\phi_a)_0 &= \mathrm{lcm}_{s\in M\setminus(\overline{M}_0^r(a)\cup M_0^r(\mathbb{T}))}((\phi_{a_i})_0) \\ &= \mathrm{lcm}_{s\in M\setminus(\overline{M}_0^r(a)\cup M_0^r(\mathbb{T}))}(L(\mathbb{T}_s)p^{j_s}) \\ &= p^J\mathrm{lcm}_{s\in M\setminus(\overline{M}_0^r(a)\cup M_0^r(\mathbb{T}))}(L(\mathbb{T}_s)) \end{aligned}$$

where $L(\mathbb{T}_s) = L(\theta_s^r(\mathbb{T})) = O(\pi_{r,0}^s(\theta_r^s(\mathbb{T})))$. ■

**Proof of lemma 4.4.2**

In $\frac{\mathbb{F}_{p^q}[x]}{R_i(x)\mathbb{F}_{p^q}[x]}$ there are $\phi(O(\mathbb{T}_i))$ elements with given order $O(\mathbb{T}_i)|p^{qd_i}-1$, see section A.4 in appendix A. Let $a \in \frac{\mathbb{F}_{p^q}[x]}{R_i(x)\mathbb{F}_{p^q}[x]}$, $a \neq 0$ and suppose $O(a) = L$, then in $\frac{\mathbb{F}_{p^q}[x]}{R_i(x)^{p^r}\mathbb{F}_{p^q}[x]}$ the element

$$\hat{a} = a(x)^{p^r} + R_i(x)^{p^r}\mathbb{F}_{p^q}[x]$$

has order $L$ and so does any element of the form $\hat{a}+\eta$ where $\eta \in \text{Ker } \pi_{r,0}$, by lemma 3.3.6, and using lemma 3.3.3 we see that there are $\phi(L)p^{qd_i(p^r-1)}$ units $\mathbb{T}$ in $\frac{\mathbb{F}_{p^q}[x]}{R_i(x)^{p^r}\mathbb{F}_{p^q}[x]}$ with $L(\mathbb{T}_i) = L$. Suppose $\mathbb{T} \in \frac{\mathbb{F}_{p^q}[x]}{R_i(x)^{p^r}\mathbb{F}_{p^q}[x]}$ is such that $L(\mathbb{T}) = L$ and $\mathbb{T} = \hat{a} + \eta$ where $\mathcal{I}_i(\eta) = I$, then

$$\mathbb{T}^L - 1 = \hat{a}^L - 1 + \sum_{j=1}^{L} \binom{L}{j} \hat{a}^{L-j}\eta^j$$

and $\mathcal{I}_i(\sum_{j=1}^{L} \binom{L}{j} \hat{a}^{L-j}\eta^j) = I$. Now suppose that $\mathbb{T}' = \hat{a} + \eta'$ where $\mathcal{I}_i(\eta') = I$ also, we show that if $\mathbb{T}^L - 1 = \mathbb{T}'^L - 1$ then $\mathbb{T} = \mathbb{T}'$, for suppose that $\mathbb{T}^L - 1 = \mathbb{T}'^L - 1$, then $\mathbb{T}^L = \mathbb{T}'^L$ so

$$(\eta - \eta')\hat{a}^{L-1} + \sum_{j=2}^{L} \binom{L}{j} (\eta^{j-1} - \eta'^{j-1})\hat{a}^{L-j} = 0 \qquad \text{(B.3.2)}$$

and either $\eta = \eta'$ or $R^{p^r}(x)$ divides the canonical representative of the left hand side of (B.3.2), but a smaller power of $R$ divides $(\eta-\eta')\hat{a}^{L-1}$ than divides $\sum_{j=2}^{L} \binom{L}{j} (\eta^{j-1} - \eta'^{j-1})\hat{a}^{L-j}$ and thus one cannot have $R^{p^r}(x)$ divides the canonical representative of the left hand side of (B.3.2) and so must have $\eta = \eta'$. Thus for each $n$ with $\mathcal{I}_i(\eta) = I$ there is exactly one unit $\mathbb{T} \in \frac{\mathbb{F}_{p^q}[x]}{R_i(x)^{p^r}\mathbb{F}_{p^q}[x]}$ such that $L(\mathbb{T}) = L$ and $\mathcal{I}_i(\mathbb{T}^L - 1) = I$ and hence there are

$$\phi(L)|\mathcal{D}_R(p^r d_i - 1, I)|$$

such distinct units $\mathbb{T} \in \frac{\mathbb{F}_{p^q}[x]}{R_i(x)^{p^r}\mathbb{F}_{p^q}[x]}$. ■

## B.4 Proofs of results from chapter 5

### Proof of remark 5.1.1

$$\begin{aligned}(a+n)^{p^{k-1}} &= ((a+n)^p)^{p^{k-2}} \\ &= \left(a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} n^i + n^p\right)^{p^{k-2}} \\ &= \left(a^p + p\sum_{i=1}^{p-1} 1/p \binom{p}{i} a^{p-i} n^i + p(n/p)n^{p-1}\right)^{p^{k-2}} \\ &= (a^p + pn_1)^{p^{k-2}} \quad \text{where } p|n_1.\end{aligned}$$

Carrying on in the above manner we see that

$$\begin{aligned}(a+n)^{p^{k-1}} &= a^{p^{k-1}} + p^{k-1}n_{k-1} \quad \text{where } p|n_{k-1} \\ &= a^{p^{k-1}}. \quad \blacksquare\end{aligned}$$

### Proof of lemma 5.1.1

Both $\lambda'_{k,1}$ and $\Lambda_{k,1}$ are surjective and any ring homomorphism maps units to units and nilpotent elements to nilpotent elements. For the converse we prove the second statement, the proof for the first is very similar. Suppose that $\Lambda_{k,1}(a)$ is a unit, then there is an element $\hat{b}$ such that $\Lambda_{k,1}(a)\hat{b} = 1$ and as $\Lambda_{k,1}$ is surjective there is some element $b \in \frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$ such that $\Lambda_{k,1}(b) = \hat{b}$, so $\Lambda_{k,1}(ab) = 1$ and therefore $ab = 1+n$ where $n \in \text{Ker } \Lambda_{k,1}$ so by remark 5.1.1 $(ab)^{p^{k-1}} = 1$ and $a$ is a unit. Suppose that $\Lambda_{k,1}(a)$ is nilpotent so there is some $\mu \in \mathbb{N}$ such that $\Lambda_{k,1}(a)^\mu = 0$ hence $\Lambda_{k,1}(a^\mu) = 0$ hence $a^\mu = n$ where $n \in \text{Ker } \Lambda_{k,1}$ hence $n^k = 0$ hence $a$ is nilpotent. $\blacksquare$

### Proof of lemma 5.1.4

It suffices to prove the result for $j = 1$, the more general case follows by replacing $a$ with $a^{p^{j-1}}$ for $j > 1$. For $p = 2$ we have

$$\begin{aligned}(a-e)^2 &= a^2 + e - 2a = a^2 - e + 2e - 2a \\ \Rightarrow \quad a^2 - e &= (a-e)^2 + 2e(a-e).\end{aligned}$$

For $p > 2$, $p$ is odd so $p-1$ is even and

$$(a-e)^p = a^p + (-e)^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i}(-e)^i,$$

and

$$\sum_{i=1}^{p-1}\binom{p}{i}a^{p-i}(-e)^i = \sum_{i=1}^{\frac{p-1}{2}}\binom{p}{i}(a^{p-i}(-e)^i + a^i(-e)^{p-i})$$

$$= \sum_{i=1}^{\frac{p-1}{2}}\binom{p}{i}a^i(-e)^i(a^{p-2i} - e).$$

Now, for $1 \leq i \leq \frac{p-1}{2}$ one has

$$a^{p-2i} - e = (a-e)(a^{p-2i-1} + a^{p-2i-2} + \ldots + a + e)$$

and as $p\left|\binom{p}{i}\right.$ the first part of the result follows.

For $p = 2$, $\eta_2(a) = e$ for any $a \in R$ and so clearly the last part holds. For $p > 2$ and $b|a - e$ we can write $\eta_p(a)$ as follows:

$$\eta_p(a) = -\sum_{i=1}^{\frac{p-1}{2}} 1/p\binom{p}{i}a^i(-e)^i(a^{p-2i-1} + a^{p-2i-2} + \ldots + e)$$

$$= -\sum_{i=1}^{\frac{p-1}{2}} 1/p\binom{p}{i}a^i(-e)^i((a^{p-2i-1} - e) + (a^{p-2i-2} - e) + \ldots + (p-2i)e)$$

and $a - e|a^{p-2i-j} - e$, $1 \leq j \leq p - 2i - 1$ and $1 \leq i \leq \frac{p-1}{2}$, hence it suffices to show that $b$ does not divide the sum

$$-\sum_{i=1}^{\frac{p-1}{2}} 1/p\binom{p}{i}a^i(-e)^i(p-2i)e = -\sum_{i=1}^{\frac{p-1}{2}} 1/p\binom{p}{i}(a^i - e + e)(-e)^i(p-2i)e$$

$$= -\sum_{i=1}^{\frac{p-1}{2}} 1/p\binom{p}{i}(a^i - e)(-e)^i(p-2i)e$$

$$-\sum_{i=1}^{\frac{p-1}{2}} 1/p\binom{p}{i}(-e)^i(p-2i)e$$

and as $b|a^i - e$ it suffices to show that $b \nmid -\sum_{i=1}^{\frac{p-1}{2}} 1/p\binom{p}{i}(-e)^i(p-2i)e$. We show that $\sum_{i=1}^{\frac{p-1}{2}} 1/p\binom{p}{i}(-1)^i(p-2i) = -1$, then $-\sum_{i=1}^{\frac{p-1}{2}} 1/p\binom{p}{i}(-e)^i(p-2i)e$ is the

image of $-\sum_{i=1}^{\frac{p-1}{2}} 1/p \begin{pmatrix} p \\ i \end{pmatrix} (-1)^i (p-2i)$ under the natural isomorphism from $\frac{\mathbb{Z}}{p^k\mathbb{Z}}$ onto the subring generated by $e$, and hence is $e$, so if $b$ is a non-unit then $b \nmid e$. We examine $\sum_{i=1}^{\frac{p-1}{2}} 1/p \begin{pmatrix} p \\ i \end{pmatrix} (-1)^i (p-2i)$ using a generating function technique: in $\mathbb{Z}[x]$ consider the formal derivative

$$\frac{d}{dx}((x-1)^p) = px + \sum_{j=1}^{p-1} \begin{pmatrix} p \\ j \end{pmatrix} (p-j)x^{p-j-1}(-1)^j,$$

and, as is readily verified by induction,

$$\frac{d}{dx}((x-1)^p) = p(x-1)^{p-1},$$

hence $\frac{d}{dx}((x-1)^p)\big|_{x=1} = 0$ and so

$$\sum_{j=1}^{p-1} \begin{pmatrix} p \\ j \end{pmatrix} (p-j)(-1)^j = -p.$$

One now finds that

$$\sum_{j=1}^{p-1} \begin{pmatrix} p \\ j \end{pmatrix} (p-j)x^{p-j-1}(-1)^j = \sum_{i=1}^{\frac{p-1}{2}} \begin{pmatrix} p \\ i \end{pmatrix} (-1)^i (p-2i) = -p$$

and hence

$$-\sum_{i=1}^{\frac{p-1}{2}} 1/p \begin{pmatrix} p \\ i \end{pmatrix} (-1)^i (p-2i) = 1,$$

which proves the result. ■

**Proof of lemma 5.1.5**

We prove the result for the case $k = 2$ first. Using lemma 5.1.4 one has for all integers $r \geq 1$

$$x^{np^r} - 1 = (x^{np^{r-1}} - 1)^p + p\eta_p(x^{np^{r-1}})(x^{np^{r-1}} - 1).$$

Now, in $\mathbb{Z}_{/p^2}[x]$ we can write $(x^{np^{r-1}} - 1) = \prod_{i=1}^{m} R_i(x)^{p^{r-1}} + pn(x)$ for some $n(x) \notin Ker\ \lambda'_{2,1}$, hence

$$(x^{np^{r-1}} - 1)^p = \prod_{i=1}^{m} R_i(x)^{p^r} \text{ and}$$

$$p(x^{np^{r-1}}-1) \;=\; p\prod_{i=1}^{m} R_i(x)^{p^{r-1}},$$

hence $R_i(x)^{p^{r-1}} | x^{np^r}-1$ for $1 \leq i \leq m$. No greater power of $R_i(x)$ can divide $x^{np^r}-1$, $1 \leq i \leq m$, unless $R_i(x) | \eta_p(x^{np^{r-1}})$ hence it suffices to prove that, in $\mathbb{F}_p[x]$, $R_i(x) \nmid \lambda'_{2,1}(\eta_p(x^{np^{r-1}}))$ ($\eta_p(x^{np^{r-1}}) \notin Ker\ \lambda'_{2,1}$ for $\eta_p(x^{np^{r-1}})$ has degree $np^{r-1}-2$ and the leading coefficient is 1 so $\eta_p(x^{np^{r-1}})$ is not a zero-divisor). Thus it suffices to prove that

$$R_i(x) \nmid \lambda'_{2,1}(\eta_p(x^{np^{r-1}}))$$

$$= \; -\sum_{i=1}^{\frac{p-1}{2}} 1/p \begin{pmatrix} p \\ i \end{pmatrix} x^{np^{r-1}i}(-1)^i((x^{np^{r-1}})^{p-2i-1} + (x^{np^{r-1}})^{p-2i-2} + \ldots + x^{np^{r-1}} + 1)$$

for each $1 \leq i \leq m$. Put $y = x^{np^r}$ then, as in the proof of lemma 5.1.4 we can write

$$\lambda'_{2,1}(\eta_p(x^{np^{r-1}})) \;=\; -\sum_{i=1}^{\frac{p-1}{2}} 1/p \begin{pmatrix} p \\ i \end{pmatrix} y^i(-1)^i((y^{p-2i-1}) + \ldots + (y-1))$$

$$-\sum_{i=1}^{\frac{p-1}{2}} 1/p \begin{pmatrix} p \\ i \end{pmatrix} (y^i-1)(-1)^i(p-2i)$$

$$-\sum_{i=1}^{\frac{p-1}{2}} 1/p \begin{pmatrix} p \\ i \end{pmatrix} (-1)^i(p-2i),$$

hence, as $R_i(x) | y-1$, $1 \leq i \leq m$, $R_i(x)$ divides the first two sums in the above expression but (as in the proof of lemma 5.1.4) $-\sum_{i=1}^{\frac{p-1}{2}} 1/p \begin{pmatrix} p \\ i \end{pmatrix} (-1)^i(p-2i) = 1$ hence $R_i(x) \nmid \lambda'_{2,1}(\eta_p(x^{np^{r-1}}))$, $1 \leq i \leq m$, hence $R_i(x) \nmid \eta_p(x^{np^{r-1}})$, $1 \leq i \leq m$.

For $k > 2$ and $r \geq k-1$ the proof is similar, one uses lemma 5.1.4 $k-1$ times to write $x^{np^r}-1$ as a sum of terms $(x^{np^{r-k+1}}-1)^{p^j}$, $0 \leq j \leq k-1$, multiplied by powers of $p$ and products of the form $\prod_{s=1}^{S} \eta_p(x^{np^{r-s}})$, $1 \leq S \leq k-1$. Examining the terms in this sum will reveal that for each $i$, $1 \leq i \leq m$, $R_i(x)^{p^{r-k+1}}$ divides each term, and a greater power of $R_i(x)$ divides every term except the term (which must occurr)

$$p^{k-1}\left(\prod_{s=1}^{k-1} \eta_p(x^{np^{r-s}})\right)(x^{np^{r-k+1}}-1).$$

Now, exactly as in the $k = 2$ case, one can show that $R_i(x) \nmid \lambda'_{2,1}(\eta_p(x^{np^{r-s}}))$ in $\mathbb{F}_p[x]$ and hence $R_i(x) \nmid \lambda'_{2,1}(\prod_{s=1}^{k-1} \eta_p(x^{np^{r-s}})(x^{np^{r-k+1}} - 1))$ and it follows that

$$R_i(x) \nmid p^{k-1} \prod_{s=1}^{k-1} \eta_p(x^{np^{r-s}}),$$

the result follows immediately. ■

**Proof of remark 5.1.3**

For each$i$, $1 \leq i \leq m$, one has that

$$\hat{e}^r_{i,k} = F^k_{0,r}(e^0_{i,k}) = e^0_{i,k}(x^{p^r}) + (x^{np^r} - 1)\mathbb{Z}_{/p^k}[x] = e^0_{i,1}(x^{p^r})^{p^{k-1}} + (x^{np^r} - 1)\mathbb{Z}_{/p^k}[x],$$

hence

$$\begin{aligned}
\Lambda_{k,1}(\hat{e}^r_{i,k}) &= \lambda'_{k,1}(e^0_{i,1}(x^{p^r})^{p^{k-1}}) + (x^{np^r} - 1)\mathbb{F}_p[x] \\
&= \lambda'_{k,1}(e^0_{i,1}(x^{p^r}))^{p^{k-1}} + (x^{np^r} - 1)\mathbb{F}_p[x] \\
&= e^0_{i,1}(x)^{p^r p^{k-1}} + (x^{np^r} - 1)\mathbb{F}_p[x] \\
&= e^r_{i,1},
\end{aligned}$$

by lemma 4.5.3. ■

**Proof of lemma 5.1.7**

One has that $\Lambda_{k,1}(e) = \Lambda_{k,1}(f) = \hat{e}$ implies that

$$\begin{aligned}
e &= \hat{e}(x) + n_e(x) + (x^N - 1)\mathbb{Z}_{/p^k}[x] \\
f &= \hat{e}(x) + n_f(x) + (x^N - 1)\mathbb{Z}_{/p^k}[x],
\end{aligned}$$

where $n_e(x), n_f(x) \in \text{Ker } \lambda'_{k,1}$ hence by remark 5.1.1 we have

$$e = e^{p^{k-1}} = \hat{e}^{p^{k-1}} = f^{p^{k-1}} = f. \quad \blacksquare$$

**Proof of lemma 5.1.8**

Homomorphisms map idempotents to idempotents so $\Gamma^k_{r,r-1}(e^r_{i,k})$ is idempotent.

Now

$$\begin{aligned}
\Gamma^k_{r,r-1}(e^r_{i,k}) &= e^r_{i,k}(x) + (x^{np^{r-1}} - 1)\mathbb{Z}_{/p^k}[x] \\
\Rightarrow \quad \Lambda_{k,1}(\Gamma^k_{r,r-1}(e^r_{i,k})) &= \lambda'_{k,1}(e^r_{i,k}(x) + (x^{np^{r-1}} - 1)\mathbb{F}_p[x]
\end{aligned}$$

and

$$\begin{aligned} e_{i,k}^r &= e_{i,k}^r(x) + (x^{np^{r-1}} - 1)\mathbb{Z}_{/p^k}[x] \\ &= e_{i,1}^r(x)^{p^{k-1}} + (x^{np^{r-1}} - 1)\mathbb{Z}_{/p^k}[x] \\ &= e_{i,1}^0(x^{p^r})^{p^{k-1}} + (x^{np^{r-1}} - 1)\mathbb{Z}_{/p^k}[x]. \end{aligned}$$

Then

$$\begin{aligned} \Lambda_{k,1}(\Gamma_{r,r-1}^k(e_{i,k}^r)) &= e_{i,1}^0(x^{p^r})^{p^{k-1}} + (x^{np^{r-1}} - 1)\mathbb{F}_p[x] \\ &= e_{i,1}^0(x)^{p^{r+k-1}} + (x^{np^{r-1}} - 1)\mathbb{F}_p[x] \\ &= e_{i,1}^{r-1}, \end{aligned}$$

by lemma 4.5.3, hence

$$\Lambda_{k,1}(\Gamma_{r,r-1}^k(e_{i,k}^r)) = \Lambda_{k,1}(e_{i,k}^{r-1})$$

thus the result follows by lemma 5.1.7. ■

**Proof of lemma 5.1.10**

By definition Im $\Lambda_{k,k-n}^i = e_{i,k-n}\frac{\mathbb{Z}_{/p^{k-n}}[x]}{(x^N-1)\mathbb{Z}_{p^{k-n}}[x]}$ and every $a \in$ Im $\Lambda_{k,k-n}^i$ can be written as

$$a = \left(\sum_{j=0}^{N-1}(a_j + p^{k-n}\mathbb{Z})x^j\right) e_{i,k-n}(x) + (x^N - 1)\mathbb{Z}_{/p^{k-n}}[x],$$

we map Im $\Lambda_{k,k-n}^i$ to $e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{p^k}[x]}$ by

$$a \mapsto a^* = \left(\sum_{j=0}^{N-1}(p^n a_j + p^k\mathbb{Z})x^j\right) e_{i,k}(x) + (x^N - 1)\mathbb{Z}_{/p^k}[x],$$

where $p^n a_j + p^k\mathbb{Z} \neq 0$ unless $a_j = 0$ for if $a_j + p^{k-n}\mathbb{Z} \neq 0$ then $p^{k-n} \nmid a_j$. This map is injective, for if $a^* = b^*$ one has

$$\begin{aligned} &\left(\sum_{j=0}^{N-1}(p^n a_j + p^k\mathbb{Z})x^j\right) e_{i,k}(x) + (x^N - 1)\mathbb{Z}_{/p^k}[x] \\ &= \left(\sum_{j=0}^{N-1}(p^n b_j + p^k\mathbb{Z})x^j\right) e_{i,k}(x) + (x^N - 1)\mathbb{Z}_{/p^k}[x], \end{aligned}$$

thus

$$(p^n + p^k\mathbb{Z})\left(\sum_{j=0}^{N-1}((a_j - b_j) + p^k\mathbb{Z})x^j\right) e_{i,k}(x) + (x^N - 1)\mathbb{Z}_{/p^k}[x] = 0,$$

hence either

$$\left(\sum_{j=0}^{N-1}((a_j - b_j) + p^k\mathbb{Z})x^j\right) e_{i,k}(x) = g(x)(x^N - 1),$$

for some $g(x) \in \mathbb{Z}_{/p^k}[x]$ or $p^{k-n}|a_j - b_j$ for $0 \leq j \leq N-1$. In the first case, applying $\lambda'_{k,k-n}$ one gets

$$\left(\sum_{j=0}^{N-1}((a_j - b_j) + p^{k-n}\mathbb{Z})x^j\right) e_{i,k-n}(x) = \lambda'_{k,k-n}(g(x))(x^N - 1),$$

which implies that $a = b$. In the second case

$$p^{k-n}|a_j - b_j \;\Rightarrow\; a_j - b_j + p^{k-n}\mathbb{Z} = 0 \;\Rightarrow\; a_j + p^{k-n}\mathbb{Z} = b_j + p^{k-n}\mathbb{Z}$$

for $0 \leq j \leq N-1$ so $a = b$.

Let the image of the described bijection be $B_{k,k-n}$, clearly $B_{k,k-n} \subseteq \text{Ker } \Lambda^i_{k,n}$. Let $c \in \text{Ker } \Lambda^i_{k,n}$ so

$$c = \left(\sum_{j=0}^{N-1}(a_j + p^k\mathbb{Z})x^j\right) e_{i,k}(x) + (x^N - 1)\mathbb{Z}_{/p^k}[x]$$

where $p^n|a_j$, $0 \leq j \leq N-1$ hence $a_j = p^n\hat{a}_j$, $0 \leq j \leq N-1$, where $0 \leq \hat{a}_j < p^{k-n}$ and so $c$ is the image of

$$\left(\sum_{j=0}^{N-1}(\hat{a}_j + p^{k-n}\mathbb{Z})x^j\right) e_{i,k-n}(x) + (x^N - 1)\mathbb{Z}_{/p^{k-n}}[x],$$

thus $c \in B_{k,k-n}$ hence $\text{Ker } \Lambda^i_{k,n} \subseteq B_{k,k-n}$ hence $\text{Ker } \Lambda^i_{k,n} = B_{k,k-n}$. ■

**Proof of lemma 5.1.13**

As $C^i_{k,j} = \text{Ker } \Lambda^i_{k,j} \setminus \text{Ker } \Lambda^i_{k,j+1}$ we have

$$\left|C^i_{k,j}\right| = \left|\text{Ker } \Lambda^i_{k,j}\right| - \left|\text{Ker } \Lambda^i_{k,j+1}\right| = p^{(k-j-1)d_ip^r}(p^{d_ip^r} - 1).$$

The $C^i_{k,j}$ are disjoint so

$$\begin{aligned}\left|C^i_{k,k-J} \cup \ldots \cup C^i_{k,k-1}\right| &= p^{(J-1)d_i P^r} - p^{(J-2)d_i p^r} \\ &+ p^{(J-2)d_i P^r} - p^{(J-3)d_i p^r} \\ &\vdots \\ &+ p^{d_i p^r} - 1 \\ &= p^{(J-1)d_i p^r} - 1. \quad \blacksquare\end{aligned}$$

**Proof of lemma 5.1.15**

Suppose first that $r \geq k-1$ and that $e^r_{i,k} R_i^{p^r} = 0$, then

$$e^r_{i,k}(x) R_i(x)^{p^r} = g(x)(x^{np^r} - 1) \tag{B.4.1}$$

for some $g(x) \in \mathbb{Z}_{/p^k}[x]$, further, $g(x) \notin$ Ker $\lambda'_{k,1}$ for if it were one would have $e^r_{i,1}(x) R_i(x)^{p^r} = 0$ in $\mathbb{F}_p[x]$, but $\mathbb{F}_p[x]$ is an integral domain so this cannot happen. By lemma 5.1.5 we have $R_i(x)^{p^r-k+1} | x^{np^r} - 1$ but $R_i(x)^{p^r-k+1+1} \nmid x^{np^r} - 1$ so, as $p \nmid g(x)$, if (B.4.1) is true then we must have $R_i(x) | g(x)$ but $R_i(x) \nmid \lambda'_{k,1}(g(x))$ hence (by remark 5.1.2) $R_i(x) \nmid g(x)$ hence (B.4.1) implies a contradiction as $R_i(x)^{p^r}$ divides the left hand side but not the right hand side. Hence $e^r_{i,k} R_i^{p^r} \neq 0$ for $r \geq k-1$.

For $r < k-1$ we note first that when $k = 2$ the above shows that $e^r_{i,2} R_i^{p^r} \neq 0$ for all $r \in \mathbb{N} \setminus \{0\}$ hence for $k > 2$ and $r < k-1$, if $e^r_{i,k} R_i^{p^r} = 0$ then applying $\Lambda^i_{k,2}$ yields $e^r_{i,2} R_i^{p^r} = 0$, a contradiction, hence the result holds. $\blacksquare$

**Proof of remark 5.1.4**

From lemma 5.1.15 we know that $e^r_{i,2} R_i^{p^r} \neq 0$, hence

$$e^r_{i,2}(x) R_i(x)^{p^r} = p\beta(x) + g(x)(x^{np^r} - 1) \tag{B.4.2}$$

for some $\beta(x), g(x) \in \mathbb{Z}_{/p^2}[x]$ where $g(x) \notin$ Ker $\lambda'_{k,1}$. Using lemma 5.1.5 and a similar argument to that used in the proof of lemma 5.1.15 one must have $R_i(x)^{p^{r-1}} | p\beta(x)$ as $R_i(x)^{p^{r-1}}$ divides the left hand side of (B.4.2) and $R_i(x)^{p^{r-1}} | g(x)(x^{np^r} - 1)$ but no greater power of $R_i(x)$ divides $g(x)(x^{np^r} - 1)$ hence no greater power of $R_i(x)$ divides $p\beta(x)$ hence

$$p\beta(x) = p\hat{\alpha}_r(x) R_i(x)^{p^{r-1}} \;\Rightarrow\; e^r_{i,2} R_i^{p^r} = p\hat{\alpha}_r R_i^{p^{r-1}} = p\hat{\alpha}_r e^r_{i,2} R_i^{p^{r-1}} = p\alpha_r R_i^{p^{r-1}},$$

where $\alpha_r = \hat{\alpha}_r(x)e^r_{i,2}(x) + (x^{np^r} - 1)\mathbb{Z}_{/p^2}[x]$ must be a unit for $R_i(x) \nmid p\hat{\alpha}_r(x)$ and if $p|\alpha_r$ then $e^r_{i,2}R_i^{p^r} = 0$, a contradiction hence $\alpha_r$ is either a unit or of the form $p\gamma + R_i\delta$ for some $\gamma, \delta$ but in that case $p\alpha_r$ is of the form $p\delta R_i$ but we have already shown that this is not the case, thus $\alpha_r$ is a unit. ■

**Proof of lemma 5.1.16**

For given $k > 1$ we fix $r \geq k-1$ and use induction on $K \leq k$. By remark 5.1.4 the result holds for $K = 2$. Suppose the result holds for $K-1$ so that

$$e^r_{i,K-1}R_i^{p^r} = p\alpha_r e^r_{i,K-1}R_i^{p^{r-1}} + \sum_{j=2}^{K-2} p^j\beta_j e^r_{i,K-1}R_i^{p^{r-j}},$$

then $\Lambda^i_{K,K-1}(e^r_{i,K}R_i^{p^r}) = e^r_{i,K-1}R_i^{p^r}$, hence one can write

$$e^r_{i,K}R_i^{p^r} = p\alpha_r e^r_{i,K}R_i^{p^{r-1}} + \sum_{j=2}^{K-2} p^j\beta_j e^r_{i,K}R_i^{p^{r-j}} + p^{K-1}\gamma_K,$$

where $\alpha_r e^r_{i,K}$ and the $\beta_j e^r_{i,K}$, $2 \leq j \leq K-2$, are units because $\alpha_r e^r_{i,K-1}$ and the $\beta_j e^r_{i,K-1}$, $2 \leq j \leq K-2$, are units (this follows from lemma 5.1.1). A very similar argument to that used in the proof of remark 5.1.4 shows that $p^{K-1}\gamma_K = p^{K-1}\beta_{K-1}e^r_{i,K}R_i^{p^{r-K+1}}$ where $\beta_{K-1}e^r_{i,K}$ is a unit, hence the result holds for $K$ if it holds for $K-1$ and so the result holds for all integers $K$ with $1 < K \leq k$. ■

**Proof of lemma 5.1.17**

For $k = 3$ and $r \geq 2$ we know from lemma 5.1.16 that $e^r_{i,3}R_i^{p^r} = p\alpha_r e^r_{i,3}R_i^{p^{r-1}} + p^2\beta_2 e^r_{i,3}R_i^{p^{r-2}}$, multiplying by $e^r_{i,3}R_i^{p^{r-1}(p-1)}$ and using lemma 5.1.16 again gives the required result.

For $k = 4$ and $r \geq 3$, applying $\Lambda^i_{4,3}$ to $e^r_{i,4}R_i^{p^r+p^{r-1}(p-1)}$ shows that one can write

$$e^r_{i,4}R_i^{p^r+p^{r-1}(p-1)} = p^2\alpha_r^2 e^r_{i,4}R_i^{p^{r-1}} + p^2\beta_2 e^r_{i,4}R_i^{p^r+p^{r-2}-p^{r-1}} + p^3\hat{\gamma}_4 e^r_{i,4},$$

moving to $\mathbb{Z}_{/p^4}[x]$ and using lemma 5.1.5 shows that $p^3\hat{\gamma}_4 e^r_{i,4} = p^3\gamma_4 e^r_{i,4}R_i^{p^{r-3}}$ and $\gamma_4 e^r_{i,4} \notin \text{Ker } \Lambda^i_{4,1} \setminus \{0\}$. Multiplying $e^r_{i,4}R_i^{p^r+p^{r-1}(p-1)}$ by $e^r_{i,4}R_i^{p^{r-1}(p-1)}$ and using lemma 5.1.16 gives the result for $k = 4$.

Assume the result holds for $k$ where $r \geq k$, *i.e.*

$$e^r_{i,k}R_i^{p^r+(k-2)p^{r-1}(p-1)} = p^{k-1}\alpha_r^{k-1}e^r_{i,k}R_i^{p^{r-1}} + p^{k-1}\beta_2 e^r_{i,k}\alpha_r^{k-3}R_i^{p^r+p^{r-2}-p^{r-1}}$$

$$+\sum_{j=4}^{k} p^{k-1}\gamma_j e_{i,k}^r \alpha_r^{k-j} R_i^{p^r+p^{r-j+1}-p^{r-1}},$$

then applying $\Lambda_{k+1,k}^i$ to $e_{i,k+1}^r R_i^{p^r+(k-2)p^{r-1}(p-1)}$ and using the above shows that one can write

$$\begin{aligned} e_{i,k+1}^r R_i^{p^r+(k-2)p^{r-1}(p-1)} &= p^{k-1}\alpha_r^{k-1} e_{i,k+1}^r R_i^{p^{r-1}} + p^{k-1}\beta_2 e_{i,k+1}^r \alpha_r^{k-3} R_i^{p^r+p^{r-2}-p^{r-1}} \\ &\quad + \sum_{j=4}^{k} p^{k-1}\gamma_j e_{i,k+1}^r \alpha_r^{k-j} R_i^{p^r+p^{r-j+1}-p^{r-1}} \\ &\quad + p^k \hat{\gamma}_{k+1} e_{i,k+1}^r, \end{aligned} \tag{B.4.3}$$

where the same argument as that for $k = 4$ shows that $p^k\hat{\gamma}_{k+1}e_{i,k+1}^r = p^k\gamma_{k+1}e_{i,k+1}^r R_i^{p^{r-k}}$ and $\gamma_{k+1}e_{i,k+1}^r \notin \text{Ker } \Lambda_{k+1,1}^i \setminus \{0\}$. Multiplying both sides of (B.4.3) by $e_{i,k+1}^r R_i^{p^{r-1}(p-1)}$ and using lemma 5.1.16 after noting that $p^r + p^{r-j} - p^{r-1} + p^{r-1}(p-1) = p^r + p^{r-j} + p^r - 2p^{r-1} \geq p^r$ gives

$$\begin{aligned} e_{i,k+1}^r R_i^{p^r+(k-1)p^{r-1}(p-1)} &= p^k\alpha_r^{k-1} e_{i,k+1}^r R_i^{p^{r-1}} + p^k\beta_2 e_{i,k+1}^r \alpha_r^{k-3} R_i^{p^r+p^{r-2}-p^{r-1}} \\ &\quad + \sum_{j=4}^{k} p^k\gamma_j e_{i,k+1}^r \alpha_r^{k-j} R_i^{p^r+p^{r-j+1}-p^{r-1}} \\ &\quad + p^k\gamma_{k+1} R_i^{p^r+p^{r-k}-p^{r-1}}. \end{aligned}$$

Thus, as the result is true for $k = 4$, the result is true for all $k$. ■

**Proof of corollary 5.1.3**

For $k = 2$ we have for any integer $r \geq 1$ that $e_{i,2}^r R_i^{p^r} = p\alpha_r e_{i,2}^r R_i^{p^{r-1}}$, where $\alpha_r e_{i,2}^r$ a unit, hence multiplying by $e_{i,2}^r R_i^J$, $J < p^{r-1}(p-1)$, gives

$$e_{i,2}^r R_i^{p^r+J} = p\alpha_r e_{i,2}^r R_i^{p^{r-1}+J}$$

which is non-zero as $\Lambda_{2,1}^1(\alpha_r e_{i,2}^r R_i^{p^{r-1}+J}) \neq 0$. However,

$$e_{i,2}^r R_i^{p^r+p^{r-1}(p-1)} = p\alpha_r e_{i,2}^r R_i^{p^r} = 0.$$

For $k > 2$ using lemma 5.1.16 and lemma 5.1.17 in the above manner gives

$$e_{i,k}^r R_i^{p^r+(k-1)p^{r-1}(p-1)} = 0$$

and (where we have included the $k=3$ case in the obvious way)

$$\begin{aligned} e_{i,k}^r R_i^{p^r+(k-1)p^{r-1}(p-1)-1} &= (p^{k-1}\alpha_r^{k-1} e_{i,k}^r R_i^{p^{r-1}} + p^{k-1}\beta_2 e_{i,k}^r \alpha_r^{k-3} R_i^{p^r+p^{r-2}-p^{r-1}} \\ &\quad + \sum_{j=4}^{k} p^{k-1}\gamma_j e_{i,k}^r \alpha_r^{k-j} R_i^{p^r+p^{r-j+1}-p^{r-1}}) R_i^{p^{r-1}(p-1)-1} \end{aligned}$$

and $p^r + p^{r-j+1} - p^{r-1} + p^{r-1}(p-1) - 1 \geq p^r$ for $3 \leq j \leq k$ hence using lemma 5.1.16 gives

$$e_{i,k}^r R_i^{p^r+(k-1)p^{r-1}(p-1)-1} = p^{k-1}\alpha_r^{k-1} e_{i,k}^r R_i^{p^r-1},$$

which is non-zero as $\Lambda_{k,1}^i(\alpha_r^{k-1} e_{i,k}^r R_i^{p^r-1}) \neq 0$. ■

**Proof of theorem 5.1.2**

The result is already proved for $r \geq k-1$. Let $r < k-1$ and let integer $J = k-1-r$, then, for some $e_{i,k}^r V \in e_{i,k}^r \frac{\mathbb{Z}_{/p^k}[x]}{(x^{np^r}-1)\mathbb{Z}_{/p^k}[x]}$

$$\begin{aligned} & F_{r,r+J}^k(e_{i,k}^r R_i^{p^r+(k-1)p^{r-1}(p-1)}) \\ &= e_{i,k}^{r+J}(R_i^{p^J} + pV)^{p^r+(k-1)p^{r-1}(p-1)} \\ &= e_{i,k}^{r+J}(R_i^{p^{r+J}+(k-1)p^{r+J-1}(p-1)} + \\ &\quad \sum_{s=1}^{p^r+(k-1)p^{r-1}(p-1)} \binom{p^r+(k-1)p^{r-1}(p-1)}{s} R_i^{p^{r+J}+(k-1)p^{r+J-1}(p-1)-p^J s}(pV)^s), \end{aligned}$$

the first term of this is zero by the $r = k-1$ case and

$$\begin{aligned} & p^{r+J} + (k-1)p^{r+J-1}(p-1) - p^J s \\ &= p^{J+r} + (k-s-1)p^{r+J-1}(p-1) + sp^{r+J-1}(p-1) - p^J s, \end{aligned}$$

$1 \leq s \leq k-1$, and

$$s(p^{r+J-1}(p-1) - p^J) \geq 0$$

for all $s > 0$ with equality if and only if $p = 2$ and $r = 1$. Hence, from (5.1.7),

$$p^{k-s} | e_{i,k}^{r+J} R_i^{p^{r+J}+(k-1)p^{r+J-1}(p-1)-p^J s}$$

for $1 \leq s \leq k-1$ and clearly all terms for $s \geq k$ vanish, hence one finds that

$$F_{r,r+J}^k(e_{i,k}^r R_i^{p^r+(k-1)p^{r-1}(p-1)}) = 0.$$

Applying $F^k_{r,r+J}$ to $e^r_{i,k}R_i^{p^r+(k-1)p^{r-1}(p-1)-1}$ and performing the same analysis as above shows that, unless $p=2$ and $r=1$, one gets

$$F^k_{r,r+J}(e^r_{i,k}R_i^{p^r+(k-1)p^{r-1}(p-1)}) \quad = \quad e^{r+J}_{i,k}R_i^{p^{r+J}+(k-1)p^{r+J-1}(p-1)-p^J}$$

which is non-zero by the $r=k-1$ case, hence, as $F^k_{r,r+J}$ is a monomorphism, the result is proved. ■

**Proof of remark 5.1.5**

We show that for every $l \geq 1$

$$e^1_{i,2^l}R_i^{2^l} = 2^{2^l-1}e^1_{i,2^l}R_i \neq 0,$$

this is true for $l=1$ by remark 5.1.4. Assume that the result holds for $L \geq 1$ so that

$$e^1_{i,2^{L+1}}R_i^{2^L} = 2^{2^L-1}e^1_{i,2^{L+1}}\alpha_i^{2^L-1}R_i + 2^{2^L}\gamma_{L+1} \tag{B.4.4}$$

for some $\gamma_{L+1}$ and also one must have that

$$e^1_{i,2^{L+1}}R_i^2 = 2\alpha_1 e^1_{i,2^{L+1}}R_i + 4\delta_{L+1} \tag{B.4.5}$$

for some $\delta_{L+1}$. Squaring (B.4.4) gives

$$e^1_{i,2^{L+1}}R_i^{2^{L+1}} = 2^{2^{L+1}-2}e^1_{i,2^{L+1}}\alpha_i^{2^{L+1}-2}R_i^2$$

and using (B.4.5) gives

$$e^1_{i,2^{L+1}}R_i^{2^{L+1}} = 2^{2^{L+1}-1}e^1_{i,2^{L+1}}\alpha_i^{2^{L+1}-1}R_i,$$

which is non-zero for if it were applying $\Lambda^i_{2^{L+1},2^L}$ would give a contradiction of the inductive hypothesis. Thus as the result holds for $l=1$ it holds for all $l \geq 1$. ■

**Proof of lemma 5.2.1**

We have $\mathbb{T}^{\Pi_N}_{s^*} = e_{i,s^*} + g$ but $\mathbb{T}^{\Pi_N}_{s^*-1} = e_{i,s^*-1}$ so $\Lambda^i_{s^*,s^*-1}(g) = 0$ and $p^{s^*-1}|g$, thus $\mathbb{T}^{p\Pi_N}_{s^*} = (e_{i,s^*}+g)^p = e_{i,s^*}$, hence $\Pi_N(\mathbb{T}_{s^*})|p\Pi_N$. Clearly $\Pi_N|\Pi_N(\mathbb{T}_{s^*})$ and it follows that $\Pi_N(\mathbb{T}_{s^*}) = p\Pi_N$. The rest of the proof consists of two stages of induction.

First inductive stage: We show that $\mathbb{T}^{p^j\Pi_N}_{s^*+j} = e_{i,s^*+j} + g_j$ with $g_j \neq 0$ implies that $\mathbb{T}^{p^{j+1}\Pi_N}_{s^*+j+1} = e_{i,s^*+j+1} + g_{j+1}$ with $g_{j+1} \neq 0$. Now $\mathbb{T}^{p^j\Pi_N}_{s^*+j} = \Lambda^i_{s^*+j+1,s^*+j}(\mathbb{T}^{p^j\Pi_N}_{s^*+j+1})$ so

$$\mathbb{T}^{p^j\Pi_N}_{s^*+j+1} = e_{i,s^*+j+1} + e_{i,s^*+j+1}g_j + \hat{g}_{j+1}$$

where either $\hat{g}_{j+1} = 0$ or $p^{s^*+j} | \hat{g}_{j+1}$, thus

$$\begin{aligned} \mathbb{T}^{p^{j+1}\Pi_N}_{s^*+j+1} &= e_{i,s^*+j+1} + \sum_{s=1}^{p} \binom{p}{s} (e_{i,s^*+j+1} g_j + \hat{g}_{j+1})^s \\ &= e_{i,s^*+j+1} + \sum_{s=1}^{p} \binom{p}{s} e_{i,s^*+j+1} g_j^s, \end{aligned}$$

as $p\hat{g}_{j+1} = 0$. If $\sum_{s=1}^{p} \binom{p}{s} e_{i,s^*+j+1} g_j^s = 0$ then

$$\begin{aligned} p e_{i,s^*+j+1} g_j \sum_{s=1}^{p} 1/p \binom{p}{s} e_{i,s^*+j+1} g_j^{s-1} &= 0 \\ \Rightarrow \quad p e_{i,s^*+j+1} g_j \left( e_{i,s^*+j+1} + \sum_{s=2}^{p} 1/p \binom{p}{s} e_{i,s^*+j+1} g_j^{s-1} \right) &= 0, \end{aligned}$$

Now $p e_{i,s^*+j+1} g_j \neq 0$ hence $e_{i,s^*+j+1} + \sum_{s=2}^{p} 1/p \binom{p}{s} e_{i,s^*+j+1} g_j^{s-1}$ must be a zero-divisor and hence nilpotent, but an element of the form $e_{i,s^*+j+1} + n$, $n$ nilpotent, cannot be nilpotent, thus $\sum_{s=1}^{p} \binom{p}{s} e_{i,s^*+j+1} g_j^s \neq 0$. Hence

$$g_{j+1} = \sum_{s=1}^{p} \binom{p}{s} e_{i,s^*+j+1} g_j^s,$$

moreover, we know that the inductive hypothesis holds for $j = 0$, thus $\mathbb{T}^{p^s\Pi_N}_{s^*+j+1} \neq e_{i,s^*+j+1}$ for $j \in \mathbb{N}$ and any integer $s$, $0 \leq s \leq j+1$.

Second inductive stage: We show that $\Pi_N(\mathbb{T}_{s^*+j}) = p^{j+1}\Pi_N$ implies that $\Pi_N(\mathbb{T}_{s^*+j+1}) = p^{j+2}\Pi_N$. From the first inductive stage we know that $\mathbb{T}^{p^{j+1}\Pi_N}_{s^*+j+1} = e_{i,s^*+j+1} + g_{j+1}$ where $g_{j+1} \neq 0$, $g_{j+1} = \sum_{s=1}^{p} \binom{p}{s} e_{i,s^*+j+1} g_j^s$ and $p^{s^*-1} | g_0$ so an easy induction shows that $p^{s^*+j} | g_{j+1}$, therefore $\mathbb{T}^{p^{j+2}\Pi_N}_{s^*+j+1} = e_{i,s^*+j+1}$ and hence $\Pi_N(\mathbb{T}_{s^*+j+1}) | p^{j+2}\Pi_N$ and by the inductive hypothesis we must have

$$\Pi_N(\mathbb{T}_{s^*+j}) = p^{j+1}\Pi_N | \Pi_N(\mathbb{T}_{s^*+j+1}),$$

hence $\Pi_N(\mathbb{T}_{s^*+j+1}) = p^{j+2}\Pi_N$. We have shown that the inductive hypothesis holds for $j = 0$ hence we have

$$\Pi_N(\mathbb{T}_{s^*+j}) = p^{j+1}\Pi_N$$

for all $j \in \mathbf{N}$, the result now follows on putting $j = k - s^*$. ■

**Proof of lemma 5.2.2**

For $k < s^*$ or all integers $k > 0$ if $s^*$ does not exist, one has $\mathbb{T}_k^{\Pi_N} = e_{i,k}$, hence all elements of $e_{i,k}\frac{\mathbb{Z}_{/p^k}[x]}{(x^N-1)\mathbb{Z}_{/p^k}[x]}$ are on orbits of length dividing $\Pi_N$. If $s^*$ exists then one must have $\mathbb{T}_{s^*-1}^{\Pi_N} = e_{i,s^*-1}$ hence $\mathbb{T}_{s^*}^{\Pi_N} = e_{i,s^*} + g$ where $\Lambda_{s^*,s^*-1}^i(g) = 0$ hence $p^{s^*-1}|g$ and, by lemma 5.2.1, $\Pi_N(\mathbb{T}_{s^*}) = p\Pi_N$ and, for all $k > s^*$, $\Pi_N(\mathbb{T}_k) = p^{k-s^*+1}\Pi_N$. For $k = s^*$, if $a \in \text{Ker } \Lambda_{s^*,s^*-1}$, then

$$\mathbb{T}_{s^*}^{\Pi_N} a = e_{i,s^*}a + ga = e_{i,s^*}a = a,$$

so the elements of Ker $\Lambda_{s^*,s^*-1}$ have prime periods dividing $\Pi_N$. For $k > s^*$, if j is an integer such that $0 \leq j \leq k - s^*$ then $\mathbb{T}_k^{p^j\Pi_N} = e_{i,k} + g_j$, where $\Lambda_{k,s^*+j-1}^i(\mathbb{T}_k^{p^j\Pi_N})$ $= \mathbb{T}_{s^*+j-1}^{p^j\Pi_N} = e_{i,s^*+j-1}$ so $p^{s^*-1+j}|g_j$ but $p^{s^*+j} \nmid g_j$ (see the proof of lemma 5.2.1). For $j = 0$, $\mathbb{T}_k^{\Pi_N} = e_{i,k} + g_0$ where $p^{S^*-1}|g_0$ but $p^{s^*} \nmid g_0$, hence $g_0$ annihilates any $a \in \text{Ker } \Lambda_{k,1}^i$ such that $p^{k-s^*+1}|a$, such $a$ are exactly the elements of

$$C_{k,k-s^*+1}^i \cup C_{k,k-s^*+2}^i \cup \ldots \cup C_{k,k-1}^i \cup \{0\}.$$

For $j > 0$ one has $p^{s^*+j-1}|g_j$ so we are interested in those $a \in \text{Ker } \Lambda_{k,1}^i$ which are annihilated by $p^{s^*+j-1}$ but not by $p^{s^*+j-2}$, these are exactly the elements of $C_{k,k-s^*+1-j}^i$ and thus such elements have prime periods dividing $p^j\Pi_N$ under $\mathbb{T}_k$. ■

## B.5 Proofs of results from chapter 6

**Proof of lemma 6.1.2**

For $U(t)$ periodic we have

$$\begin{aligned}
\mathbb{T}_{U(t)}^{nP_{U(t)}}(a) &= \mathbb{T}^{nP_{U(t)}}a + \sum_{i=1} \mathbb{T}^{nP_{U(t)}-i}U(i) \\
&\mathbb{T}^{nP_{U(t)}}a + \mathbb{T}^{nP_{U(t)}-1}U(1) + \ldots + \mathbb{T}^{(n-1)P_{U(t)}}U(P_{U(t)}) \\
&+ \mathbb{T}^{(n-1)P_{U(t)}-1}U(P_{U(t)}+1) + \ldots + \mathbb{T}^{(n-2)P_{U(t)}}U(2P_{U(t)}) \\
&= \qquad \vdots \\
&+ \mathbb{T}^{P_{U(t)}-1}U((n-1)P_{U(t)}+1) + \ldots + U(nP_{U(t)})
\end{aligned}$$

hence

$$\begin{aligned}
\mathbb{T}_{U(t)}^{nP_{U(t)}}(a) &= \mathbb{T}^{nP_{U(t)}}a + \mathbb{T}^{(n-1)P_{U(t)}}\left(\mathbb{T}^{P_{U(t)-1}}U(1) + \ldots + U(P_{U(t)})\right) \\
&+ \mathbb{T}^{(n-2)P_{U(t)}}\left(\mathbb{T}^{P_{U(t)-1}}U(1) + \ldots + U(P_{U(t)})\right) \\
&\vdots \\
&+ \left(\mathbb{T}^{P_{U(t)-1}}U(1) + \ldots + U(P_{U(t)})\right) \\
&= \mathbb{T}^{nP_{U(t)}}a + \left(\mathbb{T}^{(n-1)P_{U(t)}} + \ldots + 1\right)W(U),
\end{aligned}$$

hence

$$\mathbb{T}_{U(t)}^{nP_{U(t)}}(a) = (\mathbb{T}^{P_{U(t)}})_{W(U)}^{n}(a).$$

For $U(t)$ eventually periodic we have

$$\mathbb{T}_{U(t)}^{T_{U(t)}}(a) = \mathbb{T}^{T_{U(t)}}a + \sum_{i=1}^{T_{U(t)}} \mathbb{T}^{T_{U(t)}-i}U(i) = \mathbb{T}^{T_{U(t)}}a + S(U)$$

and the rest of the proof follows very similar lines to the $U(t)$ periodic case. ■

**Proof of lemma 6.1.3**

It is sufficient to prove that there is some positive integer $K$ such that

$$\mathbb{T}_{U(t)}^{T_{U(t)}+KP_{U(t)}}(R_N) = Att((\mathbb{T}^{P_{U(t)}})_{W(U)}),$$

for then all primary periodic points will be in $Att((\mathbb{T}^{P_{U(t)}})_{W(U)})$

We note first that $Att(\mathbb{T}^L) = Att(\mathbb{T})$ for any $L > 0$ and that

$$Att((\mathbb{T}^{T_{U(t)}})_{S(U)}) \subseteq (\mathbb{T}^{T_{U(t)}})_{S(U)}(R_N) = \mathbb{T}_{U(t)}^{T_{U(t)}}(R_N) \qquad \text{(B.5.1)}$$

Set $K = T(\mathbb{T})$, the maximum tree height that occurs under $\mathbb{T}$. Let $a \in R_N$, then

$$\mathbb{T}_{U(t)}^{T_{U(t)}}(a) = b \in Att((\mathbb{T}^{T_{U(t)}})_{S(U)}),$$

and by (B.5.1) every element of $Att((\mathbb{T}^{T_{U(t)}})_{S(U)})$ is $\mathbb{T}_{U(t)}^{T_{U(t)}}(a)$ for some $a \in R_N$. Then by theorem 2.2.2 $b = b' + c$ where $c \in Att(\mathbb{T}^{T_{U(t)}}) = Att(\mathbb{T})$ and $b' \in Att((\mathbb{T}^{T_{U(t)}})_{S(U)})$ (and, as $c$ ranges over $Att(\mathbb{T})$, $b$ ranges over $Att((\mathbb{T}^{T_{U(t)}})_{S(U)})$). Then

$$\begin{aligned}
\mathbb{T}_{U(t)}^{T_{U(t)}+KP_{U(t)}}(a) &= (\mathbb{T}^{P_{U(t)}})_{W(U)}^{K}(b) \\
&= (\mathbb{T}^{P_{U(t)}})^{K}b' + (\mathbb{T}^{P_{U(t)}})^{K}c + (\mathbb{T}^{P_{U(t)}})_{W(U)}^{K}(0).
\end{aligned}$$

Now, $(\mathbb{T}^{P_{U(t)}})^K c \in Att(\mathbb{T}) = Att(\mathbb{T}^{P_{U(t)}})$ and by choice of $K$

$$(\mathbb{T}^{P_{U(t)}})^K b' + (\mathbb{T}^{P_{U(t)}})^K_{W(U)}(0) \in Att((\mathbb{T}^{P_{U(t)}})_{W(U)}).$$

Hence by theorem 2.2.2

$$\mathbb{T}^{T_{U(t)}+KP_{U(t)}}_{U(t)}(a) \in Att((\mathbb{T}^{P_{U(t)}})_{W(U)}),$$

further, as $c$ ranges over $Att(\mathbb{T})$, $(\mathbb{T}^{P_{U(t)}})^K c$ ranges over $Att(\mathbb{T})$ ($c \mapsto (\mathbb{T}^{P_{U(t)}})^K c$ is a bijection on $Att(\mathbb{T})$), thus every element of $Att((\mathbb{T}^{P_{U(t)}})_{W(U)})$ is obtained in this manner, hence

$$Att((\mathbb{T}^{P_{U(t)}})_{W(U)}) \subseteq \mathbb{T}^{T_{U(t)}+KP_{U(t)}}_{U(t)}(R_N).$$

It remains to consider those elements $a \in R_N$ such that

$$\mathbb{T}^{T_{U(t)}}_{U(t)}(a) = \mathbb{T}^{T_{U(t)}}a + S(U) = b \in (\mathbb{T}^{T_{U(t)}})_{S(U)}(R_N) \setminus Att((\mathbb{T}^{T_{U(t)}})_{S(U)})$$

then as $KP_{U(t)} \geq T(\mathbb{T})$

$$\mathbb{T}^{T_{U(t)}+KP_{U(t)}}_{U(t)}(a) = (\mathbb{T}^{P_{U(t)}})^K_{W(U)}(b) \in Att((\mathbb{T}^{P_{U(t)}})_{W(U)}).$$

Hence

$$Att((\mathbb{T}^{P_{U(t)}})_{W(U)}) = \mathbb{T}^{T_{U(t)}+KP_{U(t)}}_{U(t)}(R_N). \quad \blacksquare$$

**Proof of lemma 6.2.1**

Consider the bilinear map

$$\beta : \frac{\mathbb{F}_{p^q}[x_1]}{(x^{N_1}-1)\mathbb{F}_{p^q}[x_1]} \times \frac{\mathbb{F}_{p^q}[x_2]}{(x^{N_2}-1)\mathbb{F}_{p^q}[x_2]} \longrightarrow \frac{\mathbb{F}_{p^q}[x_1,x_2]}{(x_1^{N_1}-1, x_2^{N_2}-1)\mathbb{F}_{p^q}[x_1,x_2]}$$

given by

$$(a(x_1) + (x^{N_1}-1)\mathbb{F}_{p^q}[x_1], b(x_2) + (x^{N_2}-1)\mathbb{F}_{p^q}[x_2])) \quad \mapsto$$

$$a(x_1)b(x_2) + (x_1^{N_1}-1, x_2^{N_2}-1)\mathbb{F}_{p^q}[x_1,x_2].$$

We must first check that $\beta$ is well defined, let $a(x_1)$ and $\hat{a}(x_1)$ be two representatives of $a$ and $b(x_2)$ and $\hat{b}(x_2)$ two representatives of $b$, so that

$$\begin{aligned} a(x_1) - \hat{a}(x_1) &= A(x_1)(x^{N_1}-1) \\ b(x_2) - \hat{b}(x_2) &= B(x_2)(x^{N_2}-1), \end{aligned}$$

where $A(x_1) \in \mathbb{F}_{p^q}[x_1]$ and $B(x_2) \in \mathbb{F}_{p^q}[x_2]$. Then applying $\beta$ to the different representations and examining the difference of their images one sees that

$$\begin{aligned} & a(x_1)b(x_2) - \hat{a}(x_1)\hat{b}(x_2) + (x_1^{N_1} - 1, x_2^{N_2} - 1)\mathbb{F}_{p^q}[x_1, x_2] \\ &= a(x_1)b(x_2) - a(x_1)\hat{b}(x_2) + a(x_1)\hat{b}(x_2) - \hat{a}(x_1)\hat{b}(x_2) + (x_1^{N_1} - 1, x_2^{N_2} - 1)\mathbb{F}_{p^q}[x_1, x_2] \\ &= a(x_1)(b(x_2) - \hat{b}(x_2)) + (a(x_1) - \hat{a}(x_1))\hat{b}(x_2) + (x_1^{N_1} - 1, x_2^{N_2} - 1)\mathbb{F}_{p^q}[x_1, x_2] \\ &= 0 + (x_1^{N_1} - 1, x_2^{N_2} - 1)\mathbb{F}_{p^q}[x_1, x_2]. \end{aligned}$$

Thus $\beta$ is well defined, and hence induces a $\mathbb{F}_{p^q}$–homomorphism

$$\begin{aligned} f : \frac{\mathbb{F}_{p^q}[x_1]}{(x^{N_1} - 1)\mathbb{F}_{p^q}[x_1]} \otimes \frac{\mathbb{F}_{p^q}[x_2]}{(x^{N_2} - 1)\mathbb{F}_{p^q}[x_2]} &\longrightarrow \frac{\mathbb{F}_{p^q}[x_1, x_2]}{(x_1^{N_1} - 1, x_2^{N_2} - 1)\mathbb{F}_{p^q}[x_1, x_2]} \\ a \otimes b &\mapsto ab. \end{aligned}$$

Now,

$$\begin{aligned} & f((x_1^i + (x^{N_1} - 1)\mathbb{F}_{p^q}[x_1]) \otimes (x_2^j + (x^{N_2} - 1)\mathbb{F}_{p^q}[x_2])) \\ &= x_1^i x_2^j + (x_1^{N_1} - 1, x_2^{N_2} - 1)\mathbb{F}_{p^q}[x_1, x_2] \end{aligned}$$

hence $f$ maps distinct basis elements to distinct basis elements and thus is surjective and hence injective, hence an $\mathbb{F}_{p^q}$–isomorphism. Clearly

$$f(a_1 \otimes b_1)f(a_2 \otimes b_2) = f(a_1a_2 \otimes b_1b_2)$$

hence $f$ is a ring isomorphism. ■

# Bibliography


[1] E. Jen. Exact solvability and quasiperiodicity of one-dimensional cellular automata. *Nonlinearity*, 4:251–276, 1991.

[2] R. Bartlett and M. Garzon. Monomial cellular automata. *Complex Sytems*, 7:367–388, 1993.

[3] O. Martin, A.M. Odlyzko and S. Wolfram. Algebraic properties of cellular automata. *Commun. Math. Phys.*, 93:219–258, 1984.

[4] A. Compagner and A. Hoogland. Maximum-length sequences, cellular automata and random numbers. *J. Comp. Phys.*, 71:391–428, 1987.

[5] P.D. Hortensius, R.D. MacLeod, W. Pries, D.M. Miller and H.C. Card. *IEEE Transactions on Computer Aided Design*, 8(8):842–858, 1989.

[6] W. Preis, A. Thanailakis and H.C. Card. Group properties of cellular automata and vlsi applications. *IEEE Transactions on Computers*, c-35(12):1013–1024, 1986.

[7] T. Toffoli and N.H. Margolus. Invertible cellular automata: A review. *Physica D*, (45):229–253, 1990.

[8] S. Wolfram. Statistical mechanics of cellular automata. *Rev. Mod. Phys*, 53(3):601–643, 1983.

[9] S. Tadakis. Orbits in one-dimensional cellular automata. *Physical Reviews E*, 49(2):1168–1173, 1994.

[10] S. Tadakis and S.Matsufuji. Periodicity in one-dimensional finite linear cellular automata. *Prog. Theor. Phys*, 89:325–331, 1993.

[11] S. Tadakis. Periodicity of linear cellular automata. *Preprint*, 1994.

[12] J.G. Stevens, R.E. Rosensweig and A.E. Cerkanowicz. Transient and cyclic behaviour of cellular automata with null boundary configurations. *J. Stat. Phys*, 73(1/2):159–174, 1993.

[13] E. Moore. Machine models of self reproduction. *Proc. Symp. Appl. Math*, 14:17–33, 1962.

[14] D. Richardson. Tessellation with local transformations. *J.Comp.Syst.Sci.*, 6:373–388, 1972.

[15] K. Culik II, L.P. Hurd and S. Yu. Computation theoretic aspects of cellular automata. *Physica D*, 45:357–378, 1990.

[16] A. Gill. Linear modular systems. In L.A. Zadeh and E. Polak, editors, *System Theory*. McGraw-Hill:Inter-University Electronic Series, 1969.

[17] S. Wolfram. *Theory and Applications of Cellular Automata*, volume 1 of *Advanced series on complex Systems*. World Scientific, 1986.

[18] H. Gutowitz. *Cellular Automata*. MIT Press, 1991.

[19] E. Jen. Linear cellular automata and recurring sequences in finite fields. *Commun. Math. Phys.*, 119:13–28, 1988.

[20] M. Nohmi. on a polynomial representation of finite linear cellular automata. *Bulletin of Informatics and Cybernetics*, 24(3-4), 1991.

[21] Y. Kawahara, S. Kumamoto, Y. Mizoguchi, M. Nohmi, H. Ohtsuka and T. Shoudai. Period lengths of cellular automata on square lattices with rule 90. *J. Math. Phys.*, 36(3):1435–1456, 1995.

[22] Y. Kawahara and H. Y. Lee. Period lengths of cellular automata *cam* - 90 with memory. *Preprint*, 1995.

[23] B. Voorhees. A note on injectivity of additive cellular automata. *Complex Systems*, 8:151–159, 1994.

[24] F. Vivaldi. Cellular automata and finite fields. *Physica D*, (79):115–131, 1994.

[25] P.M. Cohn. *Algebra*, volume Two. John Wiley and Sons, 1989.

[26] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and their applications*. Cambridge University Press, 1986.

[27] P. Guan and Y. He. Exact results for deterministic cellular automata with additive rules. *J. Stat. Phys.*, 43, 1986.

[28] S. Lang. *Algebra.* Addison-Wesley, third edition, 1993.

[29] J.H. Davenport, Y. Siret and E. Tournier. *Computer Algebra.* Academic Press, 1988.

[30] T.W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics.* Springer-Verlag, 1974.

[31] P.M. Cohn. *Algebra*, volume 0ne. John Wiley and Sons, 1982.

[32] L. Rowen. *Ring Theory*, volume One. Academic Press, 1988.

[33] D. S. Passman. *The Algebraic Structure of Group Rings.* John Wiley and Sons, 1977.