May, 1973 Report ESL-R-497

LINEAR SYSTEMS OVER VARIOUS RINGS

by-

Robert deB. Johnston

This report is based on the unaltered thesis of Robert Johnston submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at the Massachusetts Institute of Technology in May, 1973. The research was done in the Decision and Control Sciences Group at the Electronic Systems Laboratory.

Electronic Systems Laboratory
Department of Electrical Engineering
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

LINEAR SYSTEMS OVER VARIOUS RINGS

by

Robert deBeauchesne Johnston

B. Eng., McGill University
(1968)

M. Eng., McGill University
(1971)

SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY
at the
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

May, 1973

Signature of Author........Robert deB. Johnston..............
Department of Electrical Engineering, May 4, 1973

Certified by...
Thesis Supervisor

Accepted by..
Chairman, Departmental Committee on Graduate Students

LINEAR SYSTEMS OVER VARIOUS RINGS

BY

Robert deBeauchesne Johnston

Submitted to the Department of Electrical Engineering
on May 4, 1973 in partial fulfillment of
the requirements for the Degree of Doctor of Philosophy

ABSTRACT

This thesis first presents a general formulation for (discrete-time, time-invariant) linear systems over an arbitrary ring with identity.

Secondly, the ascending chain condition (A.C.C.) is imposed on the various rings and modules involved. The result is a network of familiar relations connecting reachability, controllability, distinguishability, realizability, and transfer functions. In general, commutativity is not required of the underlying ring at this stage. The results are later specialized to the case where the ring is a Noetherian domain to obtain a useful realizability criterion.

The development is further specialized to the case where the state is a finitely-generated torsion module over a principal ideal domain, e.g., a finite abelian group. This section is motivated by an extension to the B.C.H. coding scheme.

Fourthly, a series of decomposition results is presented under three different levels of structure on the state module. Finally, some applications and examples are discussed, followed by suggestions for further work and a summary.

THESIS SUPERVISOR: Sanjoy K. Mitter

TITLE: Professor of Electrical Engineering

ACKNOWLEDGEMENTS

The author first wishes to express grateful thanks to his supervisor, Professor S. K. Mitter of the Department of Electrical Engineering, M.I.T.. His guidance, comments, encouragement and patience were all greatly appreciated.

The author also wishes to thank Professor A. S. Willsky (Department of Electrical Engineering, M.I.T.), Dr. D. Forney (Codex Corporation, Waltham, Massachusetts) and A. Desalu (Department of Electrical Engineering, M.I.T.) for their suggestions and comments and for the illuminating discussions held with them. A particular word of thanks is due Professor Burton J. Smith (now with the Department of Electrical Engineering, University of Colorado, Denver) for his unceasing interest in and encouragement for this work; much of this thesis derives from lengthy discussions held with him.

In addition, special thanks go to Ms. Marsha Baker and Ms. Barbara Kohl for transforming the handwritten originals into legible typewritten text. Their speed and accuracy are without equal.

Perhaps the greatest debt is to the author's wife, Celeste, and daughter, Elise for their unflagging support and encouragement during the entire period that this work was being done.

Finally, the author greatefully acknowledges the financial support from Project MAC and from a Sloane Foundation Traineeship.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 System-Theoretic Position

Throughout this work, discussion is restricted to the class of discrete-time sequential systems. A system in this class can be described by equations of the form

$$x_{t+1} = f(x_t, u_t)$$

and

$$y_t = h(x_t)$$

where u_t($\in U$ = some set of inputs), x_t($\in X$ = a set of states), and y_t($\in Y$ = some set of outputs) denote the inputs, state, and output at time t; $x_{t+1} \in X$ denotes the state at time t+1, and $f: X \times U \to X$, $h: X \to Y$ are functions.

Specifically, this class excludes systems operating in continuous time, such as those described by differential equations. It also excludes systems where concurrent activities may take arbitrary finite times to complete, such as those described by Petri nets.

There is a qualitative division of the class of discrete-time sequential systems (D.T.S.S.) according to the amount of algebraic structure afforded the system. At one extreme is the theory of finite-automata as described by J. Hartmanis and R. E. Stearns [1], H. P. Zeiger [2], and by K. Krohn and J. Rhodes [3]. Here there is no algebraic structure placed on the input and output sets; the only assumption is that these sets (and the state set) are finite.

At the other extreme is the theory of finite-dimensional linear systems over a field F, where F may be finite or infinite. Here the input, output and state sets are finite-dimensional vector spaces over F, and all associated maps are linear (i.e., are vector space homomorphisms).

What lies between these extremes is of considerable interest. One research effort has imposed a certain amount of structure on the input, output, and state sets and has required that the associated maps be "compatible" with that structure in an algebraic sense. This point of view is illustrated by the work of R. Brockett and A. Willsky [4] and of M. Arbib [5] on group homomorphic machines. Here the input, output, and state sets are required to be groups, and the associated maps are all group homomorphisms.

Another line of research has relaxed the requirement that a linear system be constructed of elements chosen from fields and vector spaces. The result is the study of linear dynamic systems over a ring R; appropriate references are Y. Rouchaleau [6], and Y. Rouchaleau, R. E. Kalman, B. F. Wyman [7]. Here the input, output, and state sets are finitely-generated unitary modules over a ring R, and the associated maps are homomorphisms of R-modules. Specifically, the dynamic equations take the form

$$x_{t+1} = \varphi(x_t) + \psi(u_t)$$

and

$$y_t = \eta(x_t),$$

where x_t, $x_{t+1} \in X$ = state module, $u_t \in U$ = input module, $y_t \in Y$ = output module, and $\varphi: X \to X$, $\psi: U \to X$, $\eta: X \to Y$ are all R-homomorphisms.

It is proposed here to extend the study of (discrete-time) linear dynamic systems over various rings. There are two major parts of this work.

The first examines the effects various assumptions on the underlying ring have on important properties such as controllability, observability, decomposability, and realizability.

The second major part attempts to illustrate the usefulness of this extended linear system theory, from both practical and theoretical viewpoints. A great emphasis is placed on formulating a wide variety of interesting problems in terms of a linear system over some ring R.

1.2 Brief Historical Summary

The work of Rouchaleau, Kalman, and Wyman is eminent in extending conventional linear system theory to the theory of linear dynamic systems over various rings. Their emphasis, however, has been on systems whose input and output sets are finitely-generated free modules over integral domains. In his doctoral dissertation, Rouchaleau studied the problem of realizing linear systems over Noetherian domains, integrally closed and unique factorization domains, and principal ideal domains. This problem is briefly outlined below.

A linear system is completely specified by its impulse response, that is, by the m output sequences resulting from a 1 applied to each of its m input "ports". If there are p output "ports", these m semi-infinite sequences can be combined into a semi-infinite sequence of p × m matrices; this sequence can be called the Hankel sequence of the system.

The realization problem is this: given a semi-infinite sequence of p × m matrices, find a linear system for which this is the Hankel sequence. Such a system is said to be a realization of the sequence. It is usually required to find a "simple" or the "simplest" (in some sense) realization; it is always required that the state module be finitely generated.

One major result of Rouchaleau, Kalman, and Wyman is that a sequence of $p \times m$ matrices over a Noetherian domain R is realizable if, and only if, it is realizable over R's field of quotients, K.

Another major result, one appearing in Rouchaleau's dissertation, is an algorithm for computing minimal, canonical, free, realizations over a principal ideal domain. This is a system-theoretic application of an algebraic procedure for constructing a free set of generators for a module over a principal ideal domain, given an arbitrary set of generators.

Since the idea of considering linear dynamic systems over rings that are not fields is relatively new, the literature in the area is sparse. It is probably safe to say that the work of Kalman, Rouchaleau, and Wyman accounts for a large fraction of it.

1.3 Motivation

Why extend linear system theory to cases where the underlying ring is not a field? One way to answer this question is to exhibit linear systems of practical or theoretical interest that fall into this class. Another way to answer this question is to point to the success of others in the area, and discuss questions raised by their work.

The next few paragraphs will present examples of linear dynamic systems over certain rings that are not fields. These examples were chosen to be as interesting and varied as possible; hopefully, they will at least demonstrate the subject's versatility. (These and other examples are developed in much greater deatil later).

1.3.1 Encoders and Decoders for Certain Group Codes

The general idea of coding is to append some number r of check digits to a message of k information digits thus forming a composite which is hopefully "insensitive" to alteration by noise encountered in transmission. The check digits are chosen tŏ provide a certain amount of redundancy in the transmitted sequence, so that even if a few errors occur during transmission, the original message can still be recovered.

It is customary to view the digits as belonging to some finite field F. A message of k information digits can then be viewed as an element $\underline{u}$ of a k-dimensional vector space over F, and the r check digits can be viewed as an element $\underline{c}$ of an r-dimensional vector space over F.

As explained by Berlekamp [8] or Gallager [9], it is convenient to generate the r check digits by applying the k information digits in sequence to a linear dynamic system over F. The dimension of the state space is taken to be r, and the system is originally in the zero state. After all the information digits have been applied, the system is in some state $\underline{x}_k$, and the r components of this state are taken to be the check digits. If the state is represented by the contents of a shift register, it is then easy to shift these digits one by one into the transmission channel.

It is clear that this general technique of implementation does not depend on the vector space structure. Hence we may ask whether there are interesting codes whose implementation requires a more general type of linear dynamic system. A major part of research reported in this thesis deals with the construction of error-correcting codes whose implementation requires linear dynamic systems whose state sets are finite abelian groups. Such machines can be viewed as linear dynamic systems whose state, input, and output sets are all *torsion* modules (over Z), and hence are called *torsion linear machines* (or *systems*). These machines can also be viewed as finite *abelian group homomorphic machines*. A subclass of the codes discussed reduces to the Bose-Chaudhuri-Hocquenghem (B.C.H.) codes when the digits are viewed as elements of a finite field.

1.3.2 Certain Partial Difference Equations and Systems

Consider the heat flow equation along a one-dimensional bar

$$\frac{\partial^2 T}{\partial x^2} - \frac{1}{\alpha^2}\,\frac{\partial T}{\partial t} = s(x,t)$$

where T denotes temperature, x denotes spatial extent, t denotes time, and s(x,t) denotes the distribution of heat sources (in space and time) along the bar. Assume that the bar is at temperature zero everywhere at time zero. We can construct a discrete approximation to this system by letting T(i,j) denote the temperature at integral positions i along the bar at integral instants of time j. Although more complex approximations exist, for illustrative purposes we can approximate $\frac{\partial T}{\partial t}$ by T(i,j) - T(i,j-1) and $\frac{\partial^2 T}{\partial x^2}$ by T(i,j) - 2 T(i-1,j) + T(i-2,j). The approximate equation becomes:

$$[T(i,j) - 2\,T(i-1,j) + T(i-2,j)] - \frac{1}{\alpha^2}\,[T(i,j) - T(i,j-1)] = s(i,j).$$

Let y denote the shift operator y: T(i,j) → T(i-1,j), and let z denote the shift operator z: T(i,j) → T(i,j-1). Then the approximate equation can be written as

$$[(1-y)^2 - \frac{1}{\alpha^2}\ (1-z)] \cdot T(i,j) = s(i,j), \quad \forall i,j,$$

or

$$[z-1 + \alpha^2(1-y)^2] \cdot T(i,j) = \alpha^2 s(i,j), \quad \forall i,j.$$

To make contact with linear system theory over rings, let $R^*[y]$ denote the quotient ring of $R[x,y]$ modulo the principal ideal generated by $(xy-1)$, where R is the real field. Clearly, y (i.e., class of y) is a unit of $R^*[y]$, with inverse equal to x (i.e., class of x). We can represent the temperature distribution along the bar at any instant of time by an element of $R^*[y]$. We will also represent the source distribution along the bar at any instant of time by an element of $R^*[y]$. It follows that the above approximate equation represents a linear difference equation over the ring $R^*[y]$; from another point of view, the above approximate equation states that the polynomial $[z-1 + \alpha^2(1-y)^2] \in (R^*[y])\ [z]$ annihilates the state module of a discrete, one-dimensional, diffusion system viewed as a quotient module of $(R^*[y])\ [z]$.

Several points should be mentioned. First of all, any linear, constant-coefficient partial differential equation may be approximated in this fashion, and any linear, constant-coefficient, partial difference equation may be put in this form, provided that the boundary conditions are simple enough. Secondly, the ring $R^*[y]$ is a principal ideal domain, thus we can expect fairly detailed results. Finally, the step of forming $R^*[y]$ may be avoidable; it may be possible to split the spatial effects into "causal" and "anti-causal" parts, in which case we would deal with $R[y]$ instead.

This last remark is purely speculative. In any case it should still be clear that certain partial difference systems can be viewed as linear dynamic systems over a ring R.

1.3.3 Group Homomorphic Machines

As mentioned above, group homomorphic machines (G.H.M.'s) have been studied by Brockett and Willsky and by Arbib. In general, a G.H.M. is described by the dynamic equations

$$x_{t+1} = \varphi(x_t) \cdot \psi(u_t)$$

and

$$y_t = \eta(x_t),$$

where $u_t \in U$ = the input group; x_t, $x_{t+1} \in X$ = the state group, and $y_t \in Y$ = the output group; $\varphi: X \to X$, $\psi: U \to X$, and $\eta: X \to Y$ are all group homomorphisms. For our purposes, all groups will be finite.

The study of linear systems can be helpful here in several ways. The first is applicable when the groups are abelian. Such machines were mentioned earlier in the context of coding. Here they can be viewed as special cases of group homomorphic machines. In this sense, linear system theory is directly applicable to a subclass of G.H.M.s.

Another way is via the theory of groups with operators, which applies not only to modules over a ring, but to groups equipped with an endomorphism. At least on an intuitive level, it seems reasonable to expect that certain techniques are common to the linear case and the group case, since both involve groups with operators. The major difference is that in the linear case, the group (i.e. the module) is abelian.

A third way is applicable if the input to the G.H.M. were to be ignored (or set to the identity) and only the free response were of interest. In this case, one could ignore the group multiplication that takes place between $\varphi(x_t)$ and $\psi(u_t)$.

Under these circumstances, one could embed X and Y in the group algebras k[X] and k[Y], respectively, where k is some field such as the complex numbers. One would then extend φ and η to k-algebra homomorphisms. Then, as a result of a cascade decomposition theory mentioned below, one obtains immediately that k[x] is the direct product of two (left) ideals, where the restriction of φ to one is automorphic, and the restriction of φ to the other is nilpotent This result provides a preliminary decomposition of k[X]. Further decomposition can be obtained by exploiting the semisimplicity of k[x].

Naturally, this decomposition holds whether or not U is ignored, since it involves only φ and X. However, ignoring U allows the group algebra system to be treated as a linear inforced system.

1.3.4 Some Theoretical Questions

The above examples were chosen from areas not immediately related to the development of linear system theory over rings per se. The work of Rouchaleau, Kalman, and Wyman, however, does pose several questions and problems that are immediately related to the theory's development. Some of these points are brought up below.

The first concerns decomposition; in particular it concerns the lack of a decomposition theory even in the cases considered by Rouchleau, Kalman, and Wyman, where the input and output modules are free modules over some Noetherian domain. Since decomposition is an important system-theoretic topic, it seems reasonable to pursue the goal of a decomposition theory for linear systems over such important classes of rings as unique factorization domains and principal ideal domains. Of course it is also reasonable to expect that decompositions in these situations are not as readily forthcoming as in the vector space case. Nevertheless one might like to investigate Rouchaleau's technique of comparing a realization over a domain with a realization over that domain's field of quotients as a possible tool in developing decomposition theories for these more general systems.

Another question concerns the preoccupation with finding canonical (i.e., reachable and observable) realizations of Hankel sequences. It seems that, in general, a canonical realization may have a state set which is not a free module over the underlying ring. On the assumption that this could be a serious problem, it becomes reasonable to ask "when is there a free canonical realization?" and if no free canonical realization exists, "what is a 'good' free realization?" even though it may not be canonical.

A final question deals with alternate methods of specifying linear systems. Rouchaleau emphasizes Hankel sequences. One would like to have more information about specifying systems by difference equations and transfer functions or matrices.

1.4 Outline of Thesis

This thesis first develops the concept of a linear system over an arbitrary ring and then proceeds by adding more and more structure on the ring to obtain more comprehensive results. An outline of this process is as follows.

Chapter 2 develops the general concept of a discrete-time, linear, time-invariant (D.L.T.I.) system over an arbitrary ring R. The notion of a linear input-output map over a ring R is developed alongside. The treatment is very brief, and tends to follows that in Kalman, Falb, and Arbib [10].

Chapter 3 investigates the implications of the assumption that R satisfy the ascending chain condition on ideals, at first without commutativity. A web of relationships between reachability, controllability, finite-dimensionality, and monic annihilators in R[z] of the state module, is the result. It will appear that a linear system over R may be quite intractible unless R satisfies the ascending chain condition (A.C.C.). The second part of this chapter requires commutativity as well. In other words, the rings discussed are Noetherian. Fundamental realizability criteria are presented; from these, some of Rouchaleau, Kalman, and Wyman's results can be derived immediately.

Chapter 4 requires that the underlying ring R be a principal ideal domain (P.I.D.) and that the state module be a torsion module over R. (The case where the state module is free is covered to some extent by Rouchaleau in his dissertation and by Chapter 6 of this thesis). Such systems are called torsion linear machines (or systems) over a P.I.D.. The first part of this chapter develops an extensive class of error-correcting codes which are implemented using these systems. The second part proceeds with the general analysis of torsion linear machines.

Chapter 5 continues to exploit A.C.C. and provides a cascade decomposition for any linear system over a ring satisfying this condition. The decomposition is not thoroughly satisfying, however, since the state set is expressed as a subdirect product of certain modules. The effects of imposing the descending chain condition (on ideals or submodules) are then investigated. In this case, a certain uniqueness can be proved for a "complete" parallel decomposition of the original machine. Again, commutativity is not required. Finally, a decomposition and representation is provided for systems whose state sets are semisimple modules. This last decomposition is considerably more detailed and precise than others appearing here (except possibly for single input systems over a unique factorization domain).

Chapter 6 presents an assortment of applications and examples, and finally, Chapter 7 summarizes this thesis and suggests areas for further work.

2. GENERAL FORMULATION

This chapter reviews the concepts associated with linear dynamic systems. The treatment is a minor extension of that in chapter ten of Kalman, Falb, and Arbib [10]. All modules are assumed to be unitary left-modules, that is, the rings always will have a 1, which acts as an identity operator on the module, and the ring acts on module elements from the left.

2.1 The Linear Dynamical System Σ

Definition 2.1. A discrete-time, linear, time-invariant (D.L.T.I.) system Σ over a ring R is a triple of R-module homomorphisms, $\Sigma = (\varphi: X \to X, \psi: U \to X, \eta: X \to Y)$, where U (the input module) and Y (the output module) are finitely generated R-modules. X is the state module.

The interpretation of this definition is that the triple Σ defines the dynamic equations

$$x_{t+1} = \varphi(x_t) + \psi(u_t) \qquad 2.1$$

and

$$y_t = \eta(x_t), \qquad 2.2$$

where $u_t \in U$ denotes the input applied at time t; x_t, $x_{t+1} \in X$ denotes the states at times t and t+1 respectively, and $y_t \in Y$ denotes the output at time t. Note that in this formulation, an input u_t applied at time t has no effect on the output y_t at time t, although it does affect the output at time t+1. In other words, there is no "feed-through."

Secondly, each generator of U can be thought of as an input "port." If U has m generators over R, an input u_t can be specified by m elements of

R, and so Σ can be pictured as having m input "ports." Similarly, each generator of Y can be thought of as an output port. This interpretation is strengthened if U and Y are free modules, i.e., of the form R^m.

When no confusion can arise, the dynamical system Σ will simply be denoted by the triple (φ, ψ, η). Similarly, the above dynamic equations will sometimes be written

$$x_{t+1} = \varphi \cdot x_t + \psi \cdot u_t \qquad 2.3$$

and

$$y_t = \eta \cdot x_t \qquad 2.4$$

There are several important maps that can be derived from $\Sigma = (\varphi, \psi, \eta)$. Equation 2.3 describes the operation of Σ under the application of an input at a single instant of time, and can be viewed as a map : $X \times U \to X$. This map can be extended to sequences of inputs of arbitrary but finite length:

Definition 2.2. Let U^* denote the set of all finite length sequences of elements from U. That is,

$$U^* = \{(u_0, u_1, \dots, u_n) \mid u_i \in U;\ n \text{ arbitrary}\}$$

We will represent U^* by the finitely generated R[z] module Ω, where

$$\Omega = U[z] = \{\text{all polynomials in } z \text{ with coefficients from } U\}. \qquad 2.5$$

Given an element $\omega \in \Omega$, we will interpret the coefficient of z^i as the input applied i instants of time before the present. Thus $z\omega$ will denote the input sequence ω followed by a zero input; the inputs are pictured as being applied up to and including time = 0, and the output resulting from this sequence of inputs appears at time = 1.

<u>Definition 2.3.</u> Let $\Sigma = (\varphi, \psi, \eta)$ be D.L.T.I. system over R. If $\omega = \sum_{i=0}^{n-1} u_i z^{n-1-i} \in \Omega$, the map $G^*: X \times \Omega \to X$ is defined by

$$G^*: (x_o, \omega) \mapsto \varphi^n \cdot x_o + \sum_{i=0}^{n-1} \varphi^{n-1-i} \cdot \psi \cdot u_i \qquad 2.6$$

$G^*(x_o, \omega)$ is the state reached by starting Σ in state x_o, and applying the sequence of the n inputs represented by ω.

<u>Definition 2.4.</u> $\bar{G}_\Sigma : \Omega \to X$, the extended 0-state transition map of Σ, is defined by

$$\bar{G}_\Sigma : \omega \mapsto G^*(0, \omega). \qquad 2.7$$

<u>Definition 2.5.</u> Let $\Sigma = (\varphi: X \to X, \psi: U \to X, \eta: X \to Y)$ be a D.L.T.I. system over R, and let $\bar{G}_\Sigma : \Omega \to X$ be its extended 0-state transition map.

Then X_r, the reachable set of X, is defined by

$$X_r = \text{im } \bar{G}_\Sigma$$
$$= \bar{G}_\Sigma(\Omega). \qquad 2.8.$$

Another map of interest derivable from 2.3 and 2.4 is the free response map which describes the output of Σ started in some state x and supplied with an all-zero input sequence. In general, this output sequence is semi-infinite.

<u>Definition 2.6</u> Let Y^{**} denote the set of all semi-infinite sequences of

elements drawn from the R-module Y. We will identify Y^{**} with the R[z]-module Γ where

$$\Gamma = Y[[z^{-1}]] \\ = \left\{\sum_{i=1}^{\infty} y_i z^{-i} \mid y_i \in Y\right\}. \qquad 2.9$$

Γ is an R[z]-module under the following action of z: ordinary multiplication by z followed by discarding non-negative powers of z.

<u>Definition 2.7.</u> Let $\Sigma = (\varphi: \ X \to X, \ \psi; \ U \to X, \ \eta: \ X \to Y)$ be a D.L.T.I. system over R. Then $\bar{H}_\Sigma: \ X \to \Gamma$, the free response map of Σ, is defined by

$$\bar{H}_\Sigma: \ x \mapsto \sum_{i=1}^{\infty} (\eta\varphi^{i-1}x) \ z^{-i} \qquad 2.10$$

Thus, $\bar{H}_\Sigma(x)$ represents the sequence $\{\eta(x), \eta\varphi(x), \ldots, \eta\varphi^{i}(x), \ldots\}$.

<u>Definition 2.8.</u> Let $\Sigma = (\varphi, \psi, \eta)$ be a D.L.T.I. system over R and let $\bar{G}_\Sigma : \Omega \to X$, $\bar{H}_\Sigma : X \to \Gamma$ be the extended 0-state transition map and free response map respectively.

Then $f_\Sigma: \ \Omega \to \Gamma$, the input/output map of Σ, is defined by

$$f_\Sigma = \bar{H}_\Sigma \cdot \bar{G}_\Sigma \qquad 2.11$$

<u>Proposition 2.1.</u> $\Omega = U[z]$ and $\Gamma = Y[[z^{-1}]]$ are both R[z]-modules, as discussed above. X is also an R[z]-module with the action of z defined by

$$\forall x \in X, \quad z\cdot x = \varphi(x). \qquad 2.12$$

With this structure, $\bar{G}_\Sigma : \Omega \to X$ and $\bar{H}_\Sigma : X \to \Gamma$ are both R[z]-homomorphisms, and hence so is $f_{\Sigma} : \Omega \to \Gamma$.

Proof. See Chapter 10 of Kalman, Falb, Arbib [10].

Thus, a D.L.T.I. system $\Sigma = (\varphi: X \to X, \psi: U \to X, \eta: X \to Y)$ over R induces an R[z]-homomorphism $f_{\Sigma}: U[z] \to Y[[z^{-1}]]$. The converse is also true, as outlined next.

2.2 Linear, Zero-state, Input/Output Maps

Definition 2.9. Let U, Y be finitely-generated (F.G.) R-modules, and let Ω, Γ denote the R[z]-modules U[z], $Y[[z^{-1}]]$ as above. A linear, zero-state, input/output map f over R is simply an R[z]-homomorphism $f: \Omega \to \Gamma$.

Proposition 2.2. Let $f : \Omega \to \Gamma$ be linear, zero-state, input/put map over R. Then f induces a D.L.T.I. system $\Sigma_f = (\varphi: X \to X, \psi : U \to \bar{X}, \eta: X \to Y)$.

Proof. Take $X = \Omega/\ker f$. Let $G_f : \Omega \to X$ be the canonical surjection and let $\bar{H}_f : X \to \Gamma$ be the canonical injection induced by f. The action of φ on X is taken to be the action of z on X, viewed as an R-module. ψ is defined by letting finding the images under $\bar{G}_f$ of U's generators and extending this map by R-linearity. η is defined by finding the images in Γ of X's generators an R-module, retaining only the coefficients of z^{-1}, and extending this map by R-linearity. (For more details, see chapter 10 of Kalman, Falb, and Arbib [10]).

Definition 2.10. . Σ_f, the D.L.T.I. system induced by a linear input/output map $f: \Omega \to \Gamma$, will be called the canonical system induced by f.

Notice that $\bar{G}_f$ and $\bar{H}_f$ are precisely the extended 0-state transition map and free response map of Σ_f. The facts that these maps are surjective and injective respectively have several interesting interpretations and ramifications.

2.3. Reachability, Observability, and Realizability

<u>Definition 2.11.</u> Let X be the state module of a D.L.T.I. system Σ. Σ is said to be completely reachable iff $X_r = X$, where $X_r = \operatorname{im} \bar{G}_\Sigma$ = the set of reachable states.

<u>Proposition 2.3</u> The canonical system Σ_f induced by a linear input/put map is completely reachable. The proof follows from the fact that $\bar{G}_f$: $\Omega \to X = \Omega/\ker f$ is surjective.

<u>Definition 2.12.</u> Let X be the state module of a D.L.T.I. system Σ. A state $x \in X$ is said to be indistinguishable from 0 iff $\bar{H}_\Sigma(x) = 0 \in \Gamma$. The set of all indistinguishable states is denoted X_i. A D.L.T.I. system is said to be conpletely distinguishable iff $X_i = (0)$.

<u>Proposition 2.4.</u> The set X_i of indistinguishable states in a D.L.T.I. system Σ is equal to the R[z]-submodule $\ker \bar{H}_\Sigma$. The canonical system induced by a linear input/output map is completely distinguishable (since $\bar{H}_f$ is injective and so $X_i = \ker \bar{H}_f = (0)$).

<u>Definition 2.14.</u> A D.L.T.I. system $\Sigma = (\varphi: X \to X,\ \psi: U \to X,\ \eta: X \to Y)$ over R will be called a finite D.L.T.I. system iff X is a finitely generated R-module. (This will be the usual case and the adjective "finite" will be

dropped if there is no cause for confusion).

Definition 2.15. Let $f: \Omega \to \Gamma$ be a linear input/output map over R. f is said to be realizable iff there exists a finite D.L.T.I. system Σ such that f_Σ (the input/output map of Σ) equals f. In this case, Σ is said to realize, or be a realization of, $f: \Omega \to \Gamma$. Note that if Σ_f, the canonic system induced by f, is a finite D.L.T.I. system, then f is realizable. In other words, if $X = \Omega/\ker f$ is F.G. (finitely-generated) over R, then f is realizable, and furthermore, Σ_f is a canonical realization of f.

This completes the basic formulation of D.L.T.I. systems of a ring R. The treatment in Chapter 10 of Kalman, Falb, and Arbib, although developed for the case where R is a field, is similar but more detailed.

3. THE ASCENDING CHAIN CONDITION: REACHABILITY, CONTROLLABILITY, AND REALIZABILITY

3.1 Introduction

The purpose of this chapter is to impose one of the mildest possible conditions on the ring R underlying a D.L.T.I. system Σ. Immediately, some of the more familiar properties of D.L.T.I. systems over a field reappear in this more general context. For example, a linear input/output map over a ring R satisfying the ascending chain condition is realizable if and only if it has a description in terms of transfer functions. This holds even when R is noncommutative.

Throughout much of this chapter, the ring R is not required to be commutative, although it must satisfy A.C.C. (the ascending chain condition). It will be shown, however, that if R is commutative, many of the results hold without requiring A.C.C.

3.2 Properties of A.C.C.

(Recall: all rings have a 1, and all modules are unitary).

Definition 3.1 An R-module M is said to satisfy the ascending chain condition iff every properly ascending chain of submodules is finite. That is, given any sequence of submodules

$$M_0 \subseteq M_1 \subseteq M_2 \subseteq \dots \subseteq M_k \subseteq \dots,$$

where $\subseteq$ denotes inclusion, there exists a k such that $M_k = M_{k+1} = \dots$.

Definition 3.2. A ring R is said to satisfy A.C.C. iff R satisfies A.C.C. as a (left) module over itself, i.e., iff every properly ascending sequence of left ideals is finite.

These definitions lead to the follwoing important properties (for proofs, see Jacobson, N. [11]):

Proposition 3.1. (i) An R-module M satisfies A.C.C. iff every submodule of M is F.G. (finitely generated). In particular, R satisfies A.C.C. iff every left ideal is F.G.

(ii) (Principle of Divisor Induction). Assume that the R-module M satisfies A.C.C. and that P(X) is a proposition about submodules X of M. Suppose the following is true (where X, Y range over submodules of M):

$$[(\forall X)\ (X \supset Y \ \Rightarrow\ P(X))]\ \Rightarrow P(Y).$$

Then P is true of all submodules X of M.

(iii) If R satisfies A.C.C. and M is an F.G. R-module, then M satisfies A.C.C..

(iv) If the R-module M satisfies A.C.C., then all submodules and homomorphic images of M also satisfy A.C.C..

(v) (Hilbert Basis Theorem). If the ring R satisfies A.C.C., then so does R[z], the ring of polynomials in one indeterminate with coefficients from R.

Definition 3.3. A commutative ring satisfying A.C.C. is called Noetherian.

The class of rings and modules satisfying A.C.C. is quite broad. It includes:

(i) all finite systems,

(ii) fields and vector spaces,

(iii) principal ideal domains and their F.G. modules,

(iv) all polynomial extensions of the above systems,

(v) rings and matrices and endomorphisms over the above rings, their F.G. modules and polynomial extensions.

3.3. Annihilators and Dimensionality

The main result of this section is to establish the connection between the realizability of an input/output map $f: \Omega \to \Gamma$ over a ring R and the existence of monic annihilators $\in R[z]$ for each generator of $X_f = \Omega/\ker f$. These two features are shown to be equivälent if R satisfies A.C.C. or if R is commutative. In either case, f is realizable if, and only if, for each generator g_i of X_f over R[z] there exists a monic polynomial $g_i(z) \in R[z]$ such that $g_i(z) \cdot g_i = 0$. These realizability criteria are now proved.

Definition 3.4. Let S be a subset of the R-module M. Then A(S), the annihilating ideal of S, is defined by

$$A(S) = \{r \in R \mid rs = 0, \forall s \in S\};$$

an element of A(S) is called an annihilator of S.

Proposition 3.2. A(S) is in general a left ideal of R. If S is a submodule of M, A(S) is a two-sided ideal of R.

Proof: clear

Proposition 3.3. Let g be a generator of the cyclic R-module M. Then $M \simeq R/A(g)$.

Proof: define $f: M \to R/A(g)$ by

$$f: rg \mapsto [r],$$

where [r] denotes the residue class of r modulo A(g). Note that A(g), being a left ideal of R, is viewed as an R-submodule of R.

f is well-defined, for if $r_1\ g = r_2 g$, then $(r_1 - r_2)g = 0$, so that $(r_1 - r_2) \in A(g)$; hence $[r_1] = [r_2]$, and so $f(r_1 g) = f(r_2 g)$. f is clearly onto. f is injective, for if $[r_1] = [r_2]$, then $r_1 - r_2 \in A(g)$ and so $r_1 g = r_2 g$. It is easily verified that f is a homomorphism (of R-modules), and the claim is proved.

Definition 3.5. Let R be a ring with a 1. A monic polynomial in R[z] is one whose leading coefficient..is 1.

Proposition 3.4. Let X be a cyclic R[z]-module with generator g. If A(g) contains a moni polynomial, then X is a F.G. R-module.

Proof: Let $q(z) \in A(g)$ be a monic polynomial of degree n, and let $f(z) \cdot g$ be an arbitrary element of X. Since q(z) is monic, we can write f(z) uniquely as (see Jacobson, N. [11]).

$$f(z) = m(z)\ q(z) + r(z)$$

where $\partial^o r < \partial^o q = n$.

$$\begin{aligned} \text{Thus } f(z) \cdot g &= m(z) q(z) . g + r(z) \cdot g \\ &= r(z) \cdot g, \end{aligned}$$

since $q(z) \in A(g)$. But $r(z) \cdot g$ is always a finite R-linear combination of g, $z \cdot g, \ldots, z^{n-1} \cdot g$. Since every element of X can be so expressed, X is an F.G. R-module with a set of generators given by $\{g, z \cdot g, \ldots, x^{n-1} \cdot g\}$.

Corollary 3.4.1. Let X be an F.G. R[z]-module generated by $\{g_1, \ldots, g_k\}$. If for all $i = 1, \ldots, k$, $A(g_i)$ contains a monic polynomial, then X is F.G. over R.

Proof: Since X is generated over R[z] by $\{g_1, \ldots, g_k\}$, X is the sum of the cyclic R[z]-modules $<g_i>$, $i=1, \ldots k$; since $A(g_i)$ contains a monic polynomial for $i = 1, \ldots, k$, the above proposition states that each $<g_i>$ is F.G. over R. Since X is a finite sum of the $<g_i>$, X is also F.G. over R.

Corollary 3.4.2. Let $U = <g>$ be a cyclic R-module, and let Y be any F.G. R-module. Let $f: U[z] \to Y[[z^{-1}]]$ be a linear input-output map (i.e., an R[z] homomorphism), and let $\bar{G}_f: U[z] \to X_f = U[z]/\ker f$ be the canonical surjection.

If $A(\bar{G}_f(g)) \subseteq R[z]$ contains a monic polynomial, then f is realizable, and furthermore $X_f \simeq R[z] \,/\, A(\bar{G}_f(g))$.

Proof: Since U is a cyclic R-module, U[z] is a cyclic R[z]-module, also generated by g, and hence $\bar{G}_f(U[z]) = X_f$ is a cyclic R[z]-module. X_f is generated over R[z] by $\bar{G}_f(g)$.

If $A(\bar{G}_f(g)) \subseteq R[z]$, contains a monic polynomial, then the above proposition tells us that X_f is F.G. over R. Hence f is realizable. The isomorphism result follows from Proposition 3.3.

Corollary 3.4.3. Let f: $\Omega \to \Gamma$ be a linear input/output map over R, and let $\bar{G}_f$: $\Omega \to X_f = \Omega/\ker f$ be the canonical surjection. If each generator of X_f over R[z] has a monic annihilator $\in$ R[z], then f is realizable.

Proof: clear.

The above proposition establishes that the existence of monic annihilators for X_f's generators is sufficient to guarantee the realizability of f. The importance of monic annihilators is extended by the next few propositions which show the necessity of their existence when f is realizable.

Proposition 3.5. Let X be an F.G. R[z]-module generated by $\{g_1,\dots,g_k\}$ where R satisfies A.C.C..

If X is F.G. over R, then $A(g_i)$ contains a monic polynomial for $i = 1,\dots,k$.

Proof: Let g_1 be a generator of X over R[z]. Let $<x_1, x_2,\dots,x_n>$ denote the R-submodule of X generated by $\{x_1, x_2, \dots, x_n\}$. Consider the following ascending chain of R-submodules:

$$<g_1> \subset <g_1, z\cdot g_1> \subset <g_1, z\cdot g_1, z^2\cdot g_1> \subset \dots$$

Since R satisfies A.C.C. and X is F.G. over R, X also satisfies A.C.C..
Hence there exists an integer $n \geq 0$ such that

$$<g_1, z\cdot g_1\dots,z^{n-1}\cdot g_1> = <g_1, z\cdot g_1,\dots,z^{n-1}\cdot g_1, z^n\cdot g_1>.$$

Thus, $z^n\cdot g_1 \in <g_1, z\cdot g_1,\dots,z^{n-1}\cdot g_1>$, and we can write

$$z^n\cdot g_1 = \sum_{i=0}^{n-1} r_{ij}\, z^i\cdot g_1, \quad \text{some } r_{ij} \in R.$$

Hence, $(z^n - \sum_{i=0}^{n-1} r_{ij}\ z^i)\cdot g_1 = 0$.

In other words, g_1 possesses a monic annihilator $\in R[z]$. By repeating this process on each of the k generators, the proposition that each g_i has a monic annihilator $q_i(z) \in R[z]$ is established.

Corrollary 3.5.1. Let R satisfy A.C.C. and let f: $\Omega \rightarrow \Gamma$ be a linear input/output map over R. Let $X_f = \Omega/\ker f$. Then f is realizable if and only if each generator of X_f (over R[z]) has a monic annihilator $\in R[z]$.

Proof: by corollary 3.4.3.

$\Rightarrow$: X_f is an F.G. R[z]-module because U is F.G. over R and hence $\Omega = U[z]$ is F.G. over R[z]; X_f is the image of U[z] under the R[z]-homomorphism f, so X_f is indeed an F.G. R[z]-module. X_f is also F.G. over R by the realizability assumption. Proposition 3.5 then gives the result.

If R is commutative, the same result can be obtained without requiring R to satisfy A.C.C..

Proposition 3.6. Let R be a commutative ring, and let f: $\Omega \rightarrow \Gamma$ be a linear input/output map over R. Let $X_f = \Omega/\ker f$. Then, f is realizable if and only if each generator of X_f (over R[z]) has a monic annihilator $\in R[z]$ (in which case $A(X_f)$ contains a monic polynomial).

Proof: by corollary 3.4.3.

$\Rightarrow$: if f is realizable, X_f is F.G. over R. Suppose then that X_f is generated over R by $\{g_1,\ldots,g_k\}$. Now, the action of Z on X_f is an R-endomorphism and is determined by its action on each of the generators. We can thus write for all $i = 1,\ldots,k$

$$z\cdot g_i = \sum_{j=1}^{k} r_{ji}\, g_j, \quad \text{some } r_{ji} \in R.$$

We can then construct the matrix $\varphi \in \mathrm{Mat}_k(R)$:

$$\varphi = [r_{ji}]$$

By the Cayley-Hamilton theorem, φ satisfies its characteristic polynomial $q(z) \in R[z]$ (see Lang, S. [12], ch. 8) which is always monic. Hence, it is easy to argue the $q(z)$ is a monic annihilator of X_f. Consequently, each generator of X_f has a monic annihilator $\in R[z]$. Q.E.D.

Corollary 3.6.1. Let R be a commutative ring, and let $f\colon \Omega \to \Gamma$ be a linear input/output map over R. Let $X_f = \Omega/\ker f$. Then,

f is realizable iff $A(X_f)$ contains a monic polynomial.

Proof: clear.

It can be shown that even in some cases where R is noncommutative, f realizable implied $A(X_f)$ contains a monic polynomial. One such case occurs when R is a finitely-generated algebra over a commutative ring T; for example, if R is a matrix algebra over a commutative ring. Then f realizable implies that X_f is F.G. over R; since R is F.G. over T, X_f is F.G. over T as well. X_f can be shown to be a T[z]-module, and by the Cayley-Hamilton theorem, there exists a monic annihilator of X_f in T[z]. It will follow that there exists a monic annihilator if X_f in R[z] as well. This result is merely outlined here since it is not in the mainstream of the development.

The important thing is that if R satisfies A.C.C., or if R is commutative, f: $\Omega \to \Gamma$ is realizable over R if and only if every generator of $X_f = \Omega/\ker f$ over R[z] has a monic annihilator in R[z].

3.4 Reachability and A.C.C.

Here the object is to show that if R satisfies A.C.C. or if R is commutative, and if f: $\Omega \to \Gamma$ is a linear input/output map over R, then: every state of f's canonic system can be reached in a maximum of N steps (where N is some fixed positive integer) if and only if f is realizable.

Definition 3.6. Let X be the state module of a completely reachable D.L.T.I. system $\Sigma = (\varphi: X \to X,\ \psi: U \to X,\ \eta: X \to Y)$, and let $\bar{G}_\Sigma: \Omega \to X$ be the extended 0-state transition map. Σ is said to be reachable in bounded time iff there exists an integer $N \geq 0$ with the property that $\forall x \in X$, $\exists \omega \in \Omega$ such that

$$\bar{G}_\Sigma(\omega) = x$$

and the degree of ω is $\leq N$. (The degree of $\omega \in \Omega = U[z]$ is the highest power of z occuring in ω). In other words, Σ is reachable in bounded time iff every state of X can be reached in $\leq N+1$ instants of time.

Proposition 3.7. Let Σ be a D.L.T.I. system over R with state module X. If Σ is reachable in bounded time, then X is F.G. over R.

Proof: Let $\Sigma = (\varphi: X \to X,\ \psi: U \to X,\ \eta: X \to Y)$. Let $\Omega = U[z]$ and $\Gamma = Y[[z^{-1}]]$ as usual. We will view X as an R[z]-module, and let $\bar{G}_\Sigma: \Omega \to X$ be the extended

0-state transition map; $\bar{G}_\Sigma$ is an R[z] homomorphism.

If U is generated over R by $\{e_1,\ldots,e_m\}$, then $\Omega = U[z]$ is generated over R[z] by $\{e_1,\ldots,e_m\}$.

Let $g_k = \bar{G}_\Sigma(e_k)$, $k = 1,\ldots,m$. Then $\bar{G}_\Sigma(\Omega)$ is generated over R[z] by $\{g_1,\ldots,g_m\}$. Since X is completely reachable, $\bar{G}_\Sigma$ is surjective, and so X is generated over R[z] by $\{g_1,\ldots,g_m\}$.

Since Σ is reachable in bounded time, there exists an integer $N \geq 0$ where $\forall x \in X$, $\exists \omega \in \Omega$ such that

$$\bar{G}_\Sigma(\omega) = x \quad \text{and } \partial^o \omega \leq N$$

Hence, $\forall x \in X$, $\exists \omega \in \Omega$ where

$$\omega = \sum_{i=1}^{m} r_i(z)\, e_i, \quad \partial^o r_i(z) \leq N,$$

such that

$$\bar{G}_\Sigma(\omega) = x.$$

Hence, every $x \in X$ can be expressed in the form

$$x = \sum_{i=1}^{m} r_i(z)\, g_i, \quad \partial^o r_i(z) \leq N.$$

But this is precisely the same as saying that every $x \in X$ is an R-linear combination of

$$\{g_1,\ z\cdot g_1,\ldots,z^n\cdot g_1;\ldots;\ g_m,\ z\cdot g_m,\ldots,x^n\cdot g_m\}.$$

Thus X is F.G. over R. Q.E.D.

Proposition 3.8. Let Σ be a D.L.T.I. system over R with state module X. Assume Σ is completely reachable and that X, viewed as an R[z]-module is generated by $\{g_1,\ldots,g_m\}$, where U is generated over R by $\{e_1,\ldots,e_m\}$ and $g_i = \bar{G}_\Sigma(e_i)$, $i = 1,\ldots,m$.

If $A(g_i)$ contains a monic polynomial, $i = 1,\ldots,m$, then Σ is reachable in bounded time.

Proof: Since Σ is completely reachable, every $x \in X$ can be expressed

$$x = \sum_{i=1}^{m} f_i(z)\cdot g_i, \quad f_i(z) \in R[z]$$

Let $A(g_i)$ contain the monic polynomial $q_i(z)$, $i = 1,\ldots,m$. We can write, for $i = 1,\ldots,m$.

$$f_i(z) = m_i(z)\, q_i(z) + r_i(z), \quad \partial^o r_i < \partial^o q_i$$

Then, since $q_i(z) \in A(g_i)$, we can write

$$x = \sum_{i=1}^{m} r_i(z)\cdot g_i, \quad \partial^o r_i < \partial^o q_i$$

Let $N = \max\{\partial^o q_i\}$, so that each $r_i(z)$ is a polynomial of degree $\leq N$. Thus if we let

$$\omega = \sum_{i=1}^{m} r_i(z)\cdot e_i.$$

we see that $\partial^o \omega \leq N$ and $\bar{G}_\Sigma(\omega) = x$.

Hence, every $x \in X$ is reachable in $\leq N$ steps, and so Σ is reachable in bounded time. Q.E.D.

Corollary 3.8.1. Let R satisfy A. C.C., and let Σ be a completely reachable D.L.T.I. system over R with state module X.

Then Σ is reachable in bounded time if and only if X is F.G. over R.

Proof: $\Rightarrow$: is Σ is reachable in bounded time, X is F.G. over R by proposition 3.7.

$\Leftarrow$: if X is F.G. over R and R satisfies A.C.C., proposition 3.5 yields that $A(g_i)$ contains a monic polynomial for each generator g_i of X over R[z], $i = 1,\ldots,m$. By proposition 3.8, Σ is reachable in bounded time.

Corollary 3.8.2. Let R be a commutative ring, and let Σ be a completely reachable D.L.T.I. system over R with state module X.

Then Σ is reachable in bounded time if and only if X is F.G. over R.

Proof: $\Rightarrow$: by proposition 3.7.

$\Leftarrow$: If X is F.G. over R and R is commutative, then the Cayley-Hamilton theorem guarantees the existence of a monic annihilator of X in R[z]. Hence each generator of X has a monic annihilator in R[z], and the result follows from proposition 3.8.

The above results establish a fundamental connection between realizability, reachability in bounded time, and the existence of monic annihilators in R[z] for the state module's generators.

3.5 Controllability and A.C.C.

Results similar to the above can be obtained in terms of controllability. Specifically, we have the result that if Σ is a completely reachable linear system over a ring R satisfying A.C.C. whose state module is F.G., then Σ is completely controllable and in fact there is a bounded $N \geq 0$ on the number of steps required to drive any state to 0. In other words, realizability implies that every reachable state can be driven to 0 in a bounded number of states, when R satisfies A.C.C.. This is explained in corollary 3.9.2. The result is also true when R is commutative.

A converse to this theorem holds when R is commutative; this is proved in proposition 3.10.

Definition 3.7. Let $\Sigma = (\varphi, \psi, \eta)$ be a D.L.T.I. system over R, with the state module X viewed as an R[z]-module and $\bar{G}_\Sigma: \Omega \to X$, $\bar{H}_\Sigma: X \to \Gamma$ viewed as R[z]-homomorphisms.

A state $x \in X$ is said to be controllable iff there exists $\omega \in \Omega$ such that

$$z^n \circ x + \bar{G}_\Sigma(\omega) = 0, \quad \partial^o \omega < n.$$

In other words, x is controllable if we can "transfer" x to the zero state by applying some input sequence.

The set of all controllable states will be denoted X_C. If $X = X_C$, Σ will be called completely controllable.

A subset Y of X will be called controllable in bounded time if there exists an integer $N \geq 0$ so that for all $x \in Y$, $\exists \omega \in \Omega$ such that

$$z^N \cdot x + \bar{G}_\Sigma(\omega) = 0, \quad \partial^o \omega < N$$

In other words, every state in Y can be transferred to zero in at most N steps.

Proposition 3.9. Let Σ be a D.L.T.I. system over R with reachable and controllable sets X_r and X_C respectively. Assume X_r is generated over R[z] by $\{g_1,\ldots,g_m\}$, where U is generated over R by $\{e_1,\ldots,e_m\}$ and $g_i = \bar{G}_\Sigma(e_i)$, $i = 1,\ldots,m$.

If $A(g_i)$ contains a monic polynomial of R[z], $i = 1,\ldots,m$, then

(i) $X_r \subseteq X_C$, and

(ii) X_r is controllable in bounded time.

Proof: Let $x \in X_r$, so we can write

$$x = \sum_{i=1}^{m} \omega_i(z)\, g_i, \quad \text{some } \omega_i(z) \in R[z].$$

For each g_i, let $q_i(z)$ be a monic polynomial in $A(g_i)$. Let $n_i = \partial^o q_i(z)$, $i = 1,\ldots,m$, and let $N = \max\{n_i\}$.

Now for each i, we can write

$$z^N \cdot \omega_i(z) = m_i(z)\, q_i(z) + r_i(z), \quad \partial^o r_i < N,$$

for some $m_i(z)$, $r_i(z) \in R[z]$. Rewriting, we have

$$z^N \cdot \omega_i(z) - r_i(z) = m_i(z)\, q_i(z).$$

Since $q_i(z) \cdot g_i = 0$, it follows that

$$(z^N \cdot \omega_i(z) - r_i(z)) \cdot g_i = 0, \quad i = 1,\ldots,m.$$

Hence, $\sum_{i=1}^{m} (z^N \circ \omega_i(z) - r_i(z)) \circ g_i = 0, \quad \partial^o r_i < N,$

or, $$z^N \cdot \sum_{i=1}^{m} \omega_i(z) \cdot g_i - \sum_{i=1}^{m} r_i(z) \cdot g_i = 0,$$

or, $$z^N \cdot x - \sum_{i=1}^{m} r_i(z) \circ g_i = 0.$$

let $$\omega = - \sum_{i=1}^{m} r_i(z) \circ e_i \qquad (\in \Omega, \partial^o \omega < N)$$

so that $$\bar{G}_\Sigma(\omega) = - \sum_{i=1}^{m} r_i(z) \cdot g_i$$

Hence, we have found an input sequence $\omega \in \Omega$ with $\partial^o \omega < N$ such that

$$z^N \circ x + \bar{G}_\Sigma(\omega) = 0,$$

as required. Thus $x \in X_C$, and we have proved $X_r \subseteq X_C$. But we have proved more, since N depends only on the degrees of the annihilators $q_i(z)$. Thus every $x \in X_r$ can be transferred to zero in at most N steps, and X_r is controllable in bounded time.

Corollary 3.9.1. Let Σ be a completely reachable D.L.T.I. system over R with state module X. Assume X is generated over R[z] by $\{g_1,\ldots,g_m\}$, where U is generated over R by $\{e_1,\ldots,e_m\}$ and $g_i = \bar{G}_\Sigma(e_i)$, $i = 1,\ldots,m$.

If $A(g_i)$ contains a monic polynomial of R[z], $i = 1,\ldots,m$, then Σ (i.e. X) is controllable in bounded time.

Proof: same as above, but here $X_r = X$ by assumption.

Corollary 3.9.2. Let R satisfy A.C.C., and let Σ be a completely reachable D.L.T.I. system over R with state module X. If X is F.G. over R, then Σ is controllable in bounded time.

Proof: That X is F.G. over R and that R satisfies A.C.C. guarantee the existence of the annihilators required by Corollary 3.9.1. Hence, by corollary 3.9.1, Σ is controllable in bounded time.

There is a partial converse to this theorem which holds when R is commutative:

Proposition 3.10. Let Σ be a completely reachable D.L.T.I. system over the commutative ring R with state module X. Assume X is generated over R[z] by $\{g_1,\ldots,g_m\}$, where U is generated by $\{e_1,\ldots,e_m\}$ and $g_i = \bar{G}_\Sigma(e_i)$, $i = 1,\ldots m$.

If each $g_i \in X$ is controllable, then there exists a monic annihilator of X in R[z] (hence X is F.G. over R).

Proof: Since every g_i is controllable, there exists an integer n_i and an $\omega_i \in \Omega = U[z]$, $\partial^o \omega_i < n_i$, such that

$$z^{n_i} \cdot g_i + \bar{G}_\Sigma(\omega_i) = 0$$

let $$\omega_i = \sum_{j=1}^{m} r_{i_j} \cdot (z) \cdot e_j, \qquad \partial^o r_{i_j} < n_i$$

Then $$\bar{G}_\Sigma(\omega_i) = \sum_{j=1}^{m} r_{i_j}(z) \cdot g_j, \qquad \partial^o r_{i_j} < n_i$$

Hence, for each i = 1,...,m we have a relationship like

$$z^{n_i} \cdot g_i + \sum_{j=1}^{m} r_{i_j}(z) \cdot g_j = 0, \quad \partial^o r_{i_j} < n_i.$$

We can summarize these relations in matrix form:

$$\begin{bmatrix} z^{n_1} + r_{11}(z) & r_{12}(z) & \cdots & r_{1m}(z) \\ r_{21}(z) & z^{n_2} + r_{22}(z) & \cdots & r_{2m}(z) \\ r_{m1}(z) & r_{m2}(z) & \cdots & z^{n_m} + r_{mm}(z) \end{bmatrix} \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_m \end{bmatrix} = 0$$

Let B(z) denote the matrix appearing the the above equation; B(z) can be viewed as an element of the ring of m X m matrices over the commutative ring R[z].

<u>Claim</u>: (det B(z))$\cdot g_i$ = 0, i = 1,...,m, and hence, det B(z) annihilates the module generated by the g_i, i.e., det B(z) is an annihilator of X in R[z].

Proof of claim: see Lang, S. [12], p. 335.

All we have to show is that det B(z) is a monic polynomial in R[z]; this follows immediately from the fact that $\partial^{o} r_{i_j}(z) < n_i$. Thus, the highest power of Z that will appear in the determinant expansion of B(z) is $n_1 + n_2 + \dots + n_m$, and the coefficient of this term is 1 because it is the product of the terms z^{n_i}.

Hence, det B(z) is a monic annihilator of X in R[z]. Consequently, X is F.G. over R, and in fact, Σ is controllable in bounded time. Q.E.D.

Unfortunately, this theorem does not seem to generalize to the case where R is noncommutative, even when R satisfies A.C.C. This raises the possibility of a linear system over a noncommutative ring R having states that take arbitrarily long times to reach from 0, yet all of whose states may be driven to 0 in N steps. On the other hand, it may be possible to recover the result by imposing other conditions on R, such as requiring R to be a F.G. algebra over some commutative ring.

Example 1. This is an example of a realizable linear system over a ring that is noncommutative but nevertheless satisfies A.C.C.. The example calculates explicitly the control to bring a reachable state to 0.

Let R be the ring of 2 X 2 matrices over the complex numbers C; let X, the state R-module, but the set of 2 X 3 matrices over C; let U, the input R-module, be C^2 = the two-dimensional vector space over C, and let Y, the output-module, equal X. Thus the module of input sequences Ω is $C^2[z]$. The system equations will take the form

$$x_{t+1} = x_t \cdot \Phi + u_t \cdot \Psi$$

where Φ is a 3 X 3 matrix over C, and Ψ is a 1 X 3 matrix over C. More explicitly, suppose

$$x_{t+1} = x_t \cdot \begin{bmatrix} 1 & 4 & 6 \\ 0 & 2 & 5 \\ 0 & 0 & 3 \end{bmatrix} + u_t \cdot [7, 8, 9]$$

Let $q(z) = z^3 + q_2z^2 + q_1z + q_o$ be the characteristic polynomial of Φ; $q(z) = (z-1)(z-2)(z-3)$. Clearly, $q(t)$ is a monic annihilator of $X \in R[z]$ if we view the coefficients q_i as scalar matrices in R. Expanding $q(z)$, we get $q(z) = z^3-6z^2 + 11z -6$. Suppose two inputs, u_o and u_1 are applied; first u_0 and then u_1. Suppose $u_0 = (1,2)^T$ and $u_1 = (3, 1)^T$. The input sequence is thus

$$\omega(z) = \begin{bmatrix} 1 \\ 2 \end{bmatrix} \cdot z - \begin{bmatrix} 3 \\ 1 \end{bmatrix} \in C^2[z].$$

To find a control to take the state thus reached we calculate the "remainder" mod $q(z)$ of $z^3\omega(z)$. It can be verified that

$$\begin{bmatrix} 1 \\ 2 \end{bmatrix} . z^4 + \begin{bmatrix} 3 \\ 1 \end{bmatrix} . z^3 = q(z) \begin{bmatrix} 1 \\ 2 \end{bmatrix} z + \begin{bmatrix} 9 \\ 3 \end{bmatrix}$$

$$+ \begin{bmatrix} 43 \\ 66 \end{bmatrix} z^2 - \begin{bmatrix} 93 \\ 131 \end{bmatrix} z + \begin{bmatrix} 54 \\ 78 \end{bmatrix}$$

The controlling sequence is: first apply $(-43, -66)^T$, then $(93, 131)^T$, and finally $(-54, -78)^T$. The system should be in the zero state.

This example could be extended to show how a control sequence can be simply updated as each input is applied.

3.6 Distinguishability and A.C.C.

The duality that exists between controllability and observability in the vector space case suggests that results similar to the above can be obtained from the standpoint of distinguishability.

Recall the definition of distinguishability: if $\Sigma = (\varphi, \psi, \eta)$ is a D.L.T.I. system, $x \in X$ is distinguishable (from the zero state) iff $\bar{H}_\Sigma(x) \neq 0$, where

$$\begin{aligned} \bar{H}_\Sigma &: X \to \Gamma \\ &: x \mapsto \sum_{j=1}^{\infty} (\eta \varphi^{j-1} x) z^{-j} . \end{aligned}$$

In other words, x is distinguishable iff $\exists j \geq 0$ such that $\eta \varphi^j x \neq 0$. The module X (or Σ) is completely distinguishable if every nonzero $x \in X$ is distinguishable, i.e., if $\ker \bar{H}_\Sigma = (0)$.

<u>Definition 3.8</u>. Let $\Sigma = (\varphi, \psi, \eta)$ be a completely distinguishable D.L.T.I. system. Σ or X is said to be distinguishable in bounded time (or distinguishable in time n) iff $\exists N > 0$ such that

$$\eta \varphi^i x = 0, \; j = 0,1,\ldots,N-1 \quad \Rightarrow \quad x = 0.$$

<u>Proposition 3.11.</u> If R satisfies A.C.C., and $\Sigma = (\varphi, \psi, \eta)$ is distinguishable in time N, then X is F.G. over R.

Proof: define

$$\text{Obs}: X \to Y^N: \ x \mapsto (\eta \cdot x, \eta\varphi \cdot x, \ldots, \eta\varphi^{N-1} \cdot \ x)$$

Clearly, Obs is an R-homomorphism. Since X is distinguishable in time N, Obs is injective. Thus, X is isomorphic to an R-submodule of Y^N. Since Y^N is F.G. over R and R satisfies A.C.C., Y^N satisfies A.C.C. and every submodule of Y^N is also F.G. over R. Hence, X is isomorphic to a finitely-generated submodule of Y^N, and so X is F.G. over R. Q.E.D.

Proposition 3.12. If Σ is completely distinguishable, and there exists a monic annihilator of X in R[z], then Σ is observable in bounded time.

Proof: Let $q(z) = z^N + q'(z)$, $\partial^o q' < N$, be a monic annihilator of X in R[z]; i.e., $q(\varphi) \cdot X = (0)$. Then $\forall x \in X$,

$$\varphi^N \cdot x = - q'(\varphi) \cdot x,$$

and in general, $\forall x \in X$, and $k \geq 0$,

$$\varphi^k \cdot x \sum_{j=0}^{N-1} r_j \, \varphi^j \cdot x \qquad \text{some } r_i \in R.$$

Hence,
$$\eta \, \varphi^k \cdot x = \sum_{j=0}^{N-1} r_j \, \eta\varphi^j \cdot x$$

Thus, if $\eta\varphi^j \cdot x = 0$, $j = 0,\ldots,N-1$, then

$$\eta\varphi^k \cdot x = 0 \quad \forall k \geq 0.$$

Thus $\bar{G}_\Sigma(x) = 0$. By hypothesis X is completely distinguishable, and so $\bar{G}_\Sigma(x) = 0 \Rightarrow x = 0$. We have proved that if

$$\eta \psi^j \cdot x = 0, \quad j = 0,\dots, N-1,$$

then $x = 0$. Hence, Σ is distinguishable in time N. Q.E.D.

3.7 Transfer Functions and A.C.C.

Here it is shown that the usual notion of a transfer function can be defined over any ring with identity and still retain the basic properties. In particular, it is shown that whenever the generators of a state module all possess monic annihilators, the input/output map can be expressed in terms of transfer functions. Thus, realizability is equivalent to the existence of a transfer function description of the input/output map.

Let U be an R-module generated by $\{e_1,\dots,e_m\}$ and let Y be a F.G. R-module; let $\Omega = U[z]$, $\Gamma = Y[[z^{-1}]]$ and let $f\colon \Omega \to \Gamma$ be a linear input/output map (=R[z]) homomorphism).

Since Ω is generated over R[z] by $\{e_1,\dots,e_m\}$, f is completely specified by the m sequences:

$$\gamma_i = f(e_i) \in \Gamma, \quad i = 1,\dots,m.$$

Let $\bar{G}_f\colon \Omega \to X_f = \Omega/\ker f$ be the canonical injection, so that

$$f = \bar{H}_f \cdot \bar{G}_f$$

We know that X_f is generated over R[z] by

$$\{g_i \mid g_i = \bar{G}_f(e_i), \ i = 1,\dots,m\}$$

Suppose each g_i has a monic annihilator $q_i(z) \in R[z]$,

i.e., $$q_i(z)\cdot q_i = 0, \quad i = 1,\ldots,m.$$

Then
$$\begin{aligned}
q_i(z)\cdot\gamma_i &= q_i(z)\cdot f(e_i) \\
&= f(q_i(z))\cdot e_i \\
&= \bar{H}_f\cdot\bar{G}_f(q_i(z)\cdot e_i) \\
&= \bar{H}_f(q_i(z)\cdot\bar{G}_f(e_i) \\
&= \bar{H}_f(q_i(z)\cdot g_i) \\
&= \bar{H}_f\ (0) \\
&= 0.
\end{aligned}$$

Consider the relationship $q_i(z)\cdot\gamma_i = 0$; $\gamma_i \in \Gamma$ and $q_i(z)$ monic. Recall that $R[z]$ operates on Γ by ordinary multiplication (which will be denoted by "$\times$") followed by deletion of nonnegative powers of z. If $\partial^o q_i = n$, we can write

$$\begin{aligned}
q_i(z) \times \gamma_i &= \theta_i(z) + q_i(z)\cdot\gamma_i \\
&= \theta_i(z),
\end{aligned}$$

where $\theta_i(z)$ is a polynomial of degree at most n-1 in $Y[z]$. Thus, a sequence $\gamma_i \in \Gamma$ and a monic annihilator $q_i(z)$ of degree n uniquely specify a polynomial $\theta_i(z) \in Y[z]$. However, it also true that $q_i(z)$ and $\theta_i(z)$ uniquely determine γ_i:

<u>Definition 3.9.</u> Let Y be an R-module, and let $\theta(z)$ be a polynomial of degree n-1 in $Y[z]$. Let $q(z)$ be a monic polynomial in $R[z]$ of degree n.

Then $\theta(z)/q(z)$, the quotient of $\theta(z)$ by $q(z)$, is that element of $Y[[z^{-1}]]$ obtained by formal long division of $\theta(z)$ by $q(z)$. (One must be careful in performing this division to keep in mind whether Y is a left or a right R-module).

For example, let $\theta(z) = \theta_1 z + \theta_0$ and let $q(z) = z^2 + r_0$. Then $\theta(z)/q(z)$ can be determined by:

$$
\begin{array}{r|llllll}
\multicolumn{1}{r}{} & \multicolumn{6}{l}{\theta_1 z^{-1} + \theta_0 z^{-2} - r_0\theta_1 z^{-3} - r_0\theta_0 z^{-4} \quad \cdots} \\
\cline{2-7}
z^2 + r_0 & \theta_1 z + \theta_0 & & & & & \\
 & \theta_1 z & & + r_0\theta_1 z^{-1} & & & \\
\cline{2-4}
 & & \theta_0 & - r_0\theta_1 z^{-1} & & & \\
 & & \theta_0 & & + r_0\theta_0 z^{-2} & & \\
\cline{3-5}
 & & & - r_0\theta_1 z^{-1} & - r_0\theta_0 z^{-2} & & \\
 & & & - r_0\theta_1 z^{-1} & & - r_0^2\theta_1 z^{-3} & \\
\cline{4-6}
 & & & & - r_0\theta_0 z^{-2} & + r_0^2\theta_1 z^{-3} & \\
 & & & & - r_0\theta_0 z^{-2} & & - r_0^2\theta_0 z^{-4} \\
\cline{5-7}
 & & & & & & \quad \cdots
\end{array}
$$

Thus, $\theta(z)/q(z) = \sum_{j=0}^{\infty} (-r_0)^j \theta_1 z^{-1-2j} + \sum_{j=0}^{\infty} (-r_0)^j \theta_0 z^{-2-2j}$.

Proposition 3.13. Let Y be an R-module, q(z) a monic polynomial in R[z] of degree n, θ(z) a polynomial in Y[z] of degree less than n, and γ an element of $Y[[z^{-1}]]$. Then

$$q(z) \times \gamma = \theta(z) \Leftrightarrow \gamma = \theta(z)/q(z)$$

Proof: Let $q(z) = z^n + \sum_{k=0}^{n-1} r_k z^k, \quad r_k \in R,$

and $\qquad \theta(z) = \sum_{j=0}^{n-1} \theta_j z^j, \qquad \theta_j \in Y.$

Assume $\qquad \gamma = \sum_{j=1}^{\infty} y_j z^{-j}, \qquad y_j \in Y.$

$$\text{So } q(z) \times \gamma = (z^n + \sum_{k=0}^{n-1} r_k z^k) \times \sum_{j=1}^{\infty} y_j z^{-j}$$

$$= \sum_{j=1}^{\infty} y_j z^{-j+n} + r_{n-1} \sum_{j=1}^{\infty} y_j z^{-j+n-1} + \cdots + r_0 \sum_{j=1}^{\infty} y_j z^{-j}$$

$$= \sum_{j=1}^{n} y_j z^{-j+n} + \sum_{j=n+1}^{\infty} y_j z^{-j+n}$$

$$+ r_{n-1} \left(\sum_{j=1}^{n-1} y_j z^{-j+n-1} + \sum_{j=n}^{\infty} y_j z^{-j+n-1} \right)$$

$$+ \cdots$$

$$+ r_0 \sum_{j=1}^{\infty} y_j z^{-j}$$

$$= \sum_{j=1}^{n} y_j z^{-j+n} + \sum_{j=1}^{\infty} y_{j+n} z^{-j}$$

$$+ r_{n-1} \left(\sum_{j=1}^{n-1} y_j z^{-j+n-1} + \sum_{j=1}^{\infty} y_{j+n-1} z^{-j} \right) \ldots$$

$$\cdots \quad + r_0 \sum_{j=1}^{\infty} y_j z^{-j}$$

$$= \sum_{j=1}^{n} y_j z^{-j+n} + r_{n-1} \sum_{j=1}^{n-1} y_j z^{-j+n-1} + \cdots + r_1 \sum_{j=1}^{1} y_j z^{-j+1}$$

$$+ \sum_{j=1}^{\infty} (y_{j+n} + r_{n-1} y_{j+n-1} + \cdots + r_1 y_{j+1} + r_0 y_j) z^{-j}$$

$$= \sum_{j=1}^{\infty} (y_{j+n} + r_{n-1} y_{j+n-1} + \cdots + r_0 y_j) z^{-j}$$

$$+ (y_n + r_{n-1} y_{n-1} + \cdots + r_1 y_1) z^0$$

$$+ (y_{n-1} + r_{n-1} y_{n-2} + \cdots + r_2 y_1) z^1$$

$$+ \cdots\cdot$$

$$+ (y_2 + r_{n-1} y_1) z^{n-2} + (y_1) z^{n-1}$$

$$= \sum_{j=0}^{n-1} \theta_j z^j, \qquad \text{by hypothesis.}$$

Equating coefficients of equal powers of z:

$$y_1 = \theta_{n-1}$$

$$y_2 + r_{n-1} y_1 = \theta_{n-2}$$

$$\vdots$$

$$y_n + r_{n-1} y_{n-1} + \cdots + r_1 y_1 = \theta_0$$

$$y_{j+n} + r_{n-1} y_{j+n-1} + \cdots + r_0 y_j = 0 , \qquad \forall_j \geq 1.$$

Thus,

$$y_1 = \theta_{n-1}$$

$$y_2 = \theta_{n-2} - r_{n-1} y_1$$

$$\vdots$$

$$y_n = \theta_0 - r_{n-1} y_{n-1} - \cdots - r_1 y_1,$$

and for all j ≥ 1,

$$y_{j+n} = - r_{n-1} y_{j+n-1} - \cdots - r_0 y_j$$

Thus, the equation $q(z) \times \gamma = \theta(z)$ has a unique solution γ given by the above recursion relations. It remains to show that the quotient $\theta(z)/q(z)$ is the solution γ found above. This will be done by obtaining recursion relations for w_j where

$$\theta(z)/q(z) = \sum_{j=1}^{\infty} w_j z^{-j}$$

To calculate $\theta(z)/q(z)$, i.e., the w_j, we write

$$\theta(z) = q(z)\, w_1 z^{-1} + t_1(z)\,,$$

where the highest power of z in $t_1(z)$ is less than the highest power of z in $\theta(z)$. This is the first step in the long division process. To do this, we must take

$$w_1 = \theta_{n-1}$$

We then successively form

$$t_1(z) = q(z)\, w_2 z^{-2} + t_2(z)$$

$$\vdots$$

$$t_{i-1}(z) = q(z)\, w_i z^{-i} + t_i(z)$$

and choose w_i so that the highest power of z in $t_i(z)$ is less than the highest power of z in $t_{i-1}(z)$. This requires that we take w_i equal to the coefficient of the highest power of z in $t_{i-1}(z)$. Thus we get

$$t_1(z) = (\theta_{n-1} z^{n-1} + \cdots + \theta_0) - (z^n + r_{n-1} z^{n-1} + \cdots + r_0) w_1 z^{-1}$$

$$= (\theta_{n-1} - w_1) z^{n-1} + (\theta_{n-2} - r_{n-1} w_1) z^{n-2} + (\theta_{n-3} - r_{n-2} w_1) z^{n-3} + \cdots$$

$$\cdots + (\theta_0 - r_1 w_1) z + r_0 w_1 z^{-1},$$

and choose $w_1 = \theta_{n-1}$, as indicated above. We also get

$$t_2(z) = t_1(z) - q(z) w_2 z^{-2}$$

$$= (\theta_{n-2} - r_{n-1} w_1 - w_2) z^{n-2} + (\theta_{n-3} - r_{n-2} w_1 - r_{n-1} w_2) z^{n-3} + \cdots$$

$$\cdots + (r_0 w_1 - r_1 w_2) z^{-1} - r_0 w_2 z^{-2},$$

and choose $w_2 = \theta_{n-2} - r_{n-1} w_1$.

Continuing in this way, we can show that the w_j satisfy the same recurrence relations as the y_j. Thus, the unique solution γ to $q(z) \times \gamma = \theta(z)$ is given by $\gamma = \theta(z)/q(z)$, and so

$$q(z) \times \gamma = \theta(z) \Leftrightarrow \gamma = \theta(z)/q(z). \qquad \text{Q.E.D.}$$

<u>Corollary 3.13.1</u>. Let U be an R-module generated by $\{e_1, \ldots, e_m\}$ and let Y be a F.G. R-module; let $\Omega = U[z]$; $\Gamma = Y[[z^{-1}]]$, and let $f\colon \Omega \to \Gamma$ be a linear input/output map.

If there exist monic polynomials $q_i(z) \in R[z]$ such that

$$q_i(z) \cdot f(e_i) = 0, \quad i = 1, \ldots, m,$$

then $$f(e_i) = \theta_i(z)/q_i(z)$$

where $\theta_i(z) \in Y[z]$ and $\partial^o\theta_i < \partial^o q_i$, $i = 1,\ldots,m$

Proof: follows directly from proposition 3.13.

Corollary 3.13.2. Let $f: \Omega \to \Gamma$ be a linear input/output map over R as in corollary 3.13.1, and let R satisfy A.C.C..

Then f is realizable if and only if for each $i = 1,\ldots,m$, $f(e_i) = \theta_i(z)/q_i(z)$, where $\theta_i(z)$ is some element of $Y[z]$ such that $\partial^o\theta_i < \partial^o q_i$, and $q_i(z) \in R[z]$ is monic.

Proof: $\Rightarrow$: if f is realizable, $X_f = \Omega/\ker f$ is F.G. over R. Let $\bar{G}_f: \Omega \to X_f$ be the canonical surjection. Then X_f is generated over $R[z]$ by $\{g_i = \bar{G}_f(e_i) | i = 1,\ldots,m\}$. By A.C.C., there exist monic annihilators $q_i(z)$ for each g_i. Hence there exist monic polynomials $q_i(z)$ such that

$$q_i(z)\cdot f(e_i) = 0, \quad i = 1,\ldots,m.$$

The result follows from corollary 3.13.1.

$\Leftarrow$: if $f(e_i) = \theta_i(z)/q_i(z)$, then

$$q_i(z) \times f(e_i) = \theta_i(z)$$

by proposition 3.13. Hence $q_i(z)\cdot f(e_i) = 0$, $i = 1,\ldots,m$, and so

$$q_i(z)\cdot\bar{G}_f(e_i) = 0, \quad i = 1,\ldots,m.$$

The result follows from corollary 3.5.1. Q.E.D.

Note that a result similar to corollary 3.13.2 can be obtained when R is merely required to be commutative.

The quotients $\theta_i(z)/q_i(z) = f(e_i)$ are also known as transfer functions. Because f is an R[z] homomorphism, it is true that for $u(z) \in R[z]$

$$f(u(z)e_i) = u(z)\cdot f(e_i)$$

$$= u(z)\circ\ \theta_i(z)/q_i(z).$$

In other words, the response after applying input $u(z)e_i$ is simply given by multiplying the transfer function by u(z). This multiplication is the "$\cdot$" or "shift and truncate" multiplication. Hence this response is easily obtained once given the transfer function. The system response during the application of u(z) is simply the terms of nonnegative exponent in $u(z) \times \theta_i(z)/q_i(z)$.

Suppose $\Gamma = Y[[z^{-1}]]$ and $Y = R^p$, some $p > 0$. Suppose that $\theta_i(z) \in Y[z]$. Then $\theta_i(z)$ can be represented by a "column vector" of p components drawn from R[z]. Thus $\theta_i(z)/q_i(z)$ can be represented by a column vector of p components having the form $\theta_{ij}(z)/q_i(z)$. Then m such vectors (one for each input "port") can be arranged in a p X m matrix W called a transfer matrix, with the usual interpretations.

3.8 Linear Systems over Noetherian Rings

Corollary 3.6.1 stated that if R is a commutative ring and $f: \Omega \rightarrow R$ is a linear input/output map over R, then f is realizable if, and only if, $A(X_f) \subseteq R[z]$ contains a monic polynomial (X_f denotes the R[z]-module Ω/ker f). If R also satisfies A.C.C., i.e., if R is Noetherian, some stronger statements can be made. In particular, if R is a Noetherian integral domain we have:

Proposition 3.14. Let $\mathbf{R}$ be a Noetherian domain. Let $\Omega = R^m[z]$ and $\Gamma = R^p[[z^{-1}]]$, some m, $p > 0$. Let $f\colon \Omega \rightarrow \Gamma$ be a linear input/output map over R.

Then f is realizable iff $A(X_f) \neq (0)$. ($A(X_f) \subseteq R[z]$ is the annihilating ideal of $X_f = \Omega/\ker f$).

Proof: $\Rightarrow$: if f is realizable, then $A(X_f)$ contains a monic polynomial by corollary 3.6.1. and is therefore non-zero.

$\Leftarrow$: Suppose $A(X_f) \neq (0)$. Then $A(X_f)$ contains some non-zero polynomial $a(z)$; suppose such an $a(z)$ is given by

$$a(z) = \sum_{i=0}^{n} a_i z^i, \qquad a_n \neq 0.$$

Let e_i, $i = 1,\ldots,m$ denote the natural basis elements for Ω: $e_1 = (1,0,\ldots,0)^T \in R^p \subseteq R^p[z]$, and so on.

Let $\gamma_i = f(e_i)$, $i = 1,\ldots,m$.

Since $\gamma_i \in \Gamma = R^p[[z^{-1}]]$, γ_i can be written

$$\gamma_i = \sum_{j=1}^{\infty} \underline{\gamma}_i(j)\cdot z^{-j}, \quad \underline{\gamma}_i(j) \in R^p.$$

Since $a(z)\cdot X_f = 0$, $a(z)\cdot\gamma_i = 0$, $i = 1,\ldots,m$. This is equivalent to saying that

$$a_0 \, \underline{\gamma}_i(j) + a_1 \, \underline{\gamma}_j(j+1) + \cdots + a_n \, \underline{\gamma}_j(j+n) = 0$$

for each $i = 1,\ldots,m$ and for all $j \geq 1$. If we define

$$H_j = [\, \underline{\gamma}_1(j), \, \underline{\gamma}_2(j), \ldots, \underline{\gamma}_m(j)] \; , \; j \geq 1$$

$$= \text{ a } p \times m \text{ matrix over } R$$

$$= \text{ the } j^{th} \text{ term of f's Hankel sequence,}$$

then the above equation can be written

$$a_0 \, H_j + a_1 \, H_{j+1} + \cdots + a_n \, H_{j+n} = 0, \quad \forall_j \geq 1$$

The first part of this proof will show that the entire semi-infinite sequence $H_1, H_2, \ldots$ is uniquely determined by $a(z)$ and $H_1, H_2, \ldots, H_n$:

<u>Claim</u>: let $K_1, K_2, \ldots$ be any semi-infinite sequence of $p \times m$ matrices over R such that

(1) $K_j = H_j, \quad j = 1,\ldots,n$

and

(2) $a_0 \, K_j + a_1 \, K_{j+1} + \cdots + a_n \, K_{j+n} = 0, \qquad \forall j \geq 1.$

Then $K_j = H_j, \quad \forall j \geq 1.$

<u>Proof of claim</u>: by induction on j. Take $j = 1$. Then

$$a_0 \, K_1 + a_1 \, K_2 + \cdots + a_n \, K_{n-1} = 0$$

and

$$a_0 \, H_1 + a_1 \, H_2 + \cdots + a_n \, H_{n+1} = 0$$

Since $H_j = K_j$, $j = 1,\ldots,n$, subtracting those two equations gives

$$a_n(K_{n+1} - H_{n+1}) = 0.$$

Since $K_{n+1} - H_{n+1}$ is a $p \times m$ matrix over R, and because R is an integral domain, $a_n \neq 0$ implies that

$$K_{n+1} - H_{n+1} = 0$$

Hence the claim is true for $j = 1$. The induction step is performed in exactly the same manner. Q.E.D. Claim

Note: the assumption that R be an integral domain is crucial, for it implies that the action of a_n on R is injective. This claim has shown that the whole sequence $H_1, H_2, \ldots$ is completely determined by its first n terms and by $a(z)$.

Define M by

$$M = \{(K_0, K_1, \ldots, K_n) \mid K_i \text{ is a } p \times m \text{ matrix over } R\}$$

$$= (R^{p \times m})^{n+1}, \text{ and let}$$

$$M[a(z)] = \{(K_0, K_1, \ldots, K_n) \in M \mid a_0 K_0 + \cdots + a_n K_n = 0\}$$

Clearly, M is a finitely generated R-module. It is easily verified that $M[a(z)]$ is a submodule of M.

Let $S_j = (H_j, H_{j+1}, \ldots, H_{j+n}) \in M, \quad \forall j \geq 1$

$= n+1$ consecutive terms of f's Hankel sequence, beginning at the j^{th}.

Since a(z) annihilates the Hankel sequence, it is clear that

$$S_j \in M[a(z)], \qquad \forall j \geq 1.$$

Now let

$$S = \text{the R-submodule of } M[a(z)]$$
$$\text{generated by } \{S_j | j \geq 1\}.$$

S is a submodule of M, and M is a F.G. module over a Noctherian ring. Hence, S satisfies A.C.C.. Let $<S_1,\ldots,S_\ell>$ denote the R-submodule of S generated by $\{S_1, S_2,\ldots,S_\ell\}$. By A.C.C., there exists an integer $k > 0$ such that

$$0 \subseteq <S_1> \subseteq \cdots \subseteq <S_1,\ldots,S_k> = <S_1,\ldots,S_k, S_{k+1}> = \cdots = S,$$

and so S is generated by $\{s_1,\ldots,s_k\}$.

Now define the map σ: $M \to M$ as follows:

$$\sigma: (K_0, K_1,\ldots,K_n) \mapsto (K_1, K_2,\ldots,K_n, 0)$$

let $V = \{(0,0,\ldots,U) \in M \mid U \text{ is any } p \times m \text{ matrix over } R\}$.

In the same fashion as the above claim, it can be shown that for all $x \in S$, there exists a unique $v \in V$ such that $\sigma x + v \in S$. Furthermore, it is clear that if v_j is the unique element of V such that

$$\sigma S_j + v_j \in S$$

then

$$\sigma S_j + v_j = S_{j+1}, \qquad \forall j \geq 1$$

In any case, we can define the map

$$\begin{aligned} z:&\ S \to S \\ :&\ x \mapsto \sigma x + v \end{aligned}$$

in an unambiguous way. It is easily verified that z: S → S is an R-endomorphism of S, and S can be made into an R[z]-module. It can also easily be shown that

$$z^{j-1}\cdot S_1 = S_j, \qquad \forall j \geq 1.$$

Now S is F.G. over R, R is Noetherian, and S is also an R[z]-module. Hence there exists a monic $q(z) \in R[z]$ that annihilates S_1 and hence S. Suppose

$$q(z) = z^k + \sum_{i=0}^{k-1} q_i\ z^i.$$

Then

$$\begin{aligned} z^j q(z)\cdot S_1 &= (z^{k+j} + \sum_{i=0}^{k-1} q_i\ z^{i+j})\ S_1 \\ &= q_0\ S_j + q_1\ S_{j+1} + \cdots + S_{j+k} \\ &= 0, \qquad \forall j \geq 0. \end{aligned}$$

It follows from this equation and the definition of S_j that

$$q_0\ H_j + q_1\ H_{j+1} + \cdots + S_{j+k} = 0, \qquad \forall j \geq 1.$$

This is equivalent to saying that q(z) is a monic annihilator of f's Hankel sequence, and hence that q(z) is a monic annihilator of X_f. Thus, f is realizable. Q.E.D.

This proof relied on the facts that R was Noetherian and the fact that the action of any non-zero element $\in$ R on R itself was injective. That R = a domain was merely sufficient to guarantee the latter condition. The same result could be obtained by requiring $A(X_f)$ to contain some polynomial whose leading coefficient had an injective action on R. Expanding on this idea would lead to a deeper involvement in Noetherian ring theory, and will not be done here.

It will be shown later how this proposition leads to the theorem of Rouchleau, Kalman, and Wyman that says "if R is a Noetherian domain, f is realizable over R iff f is realizable over R's field of quotients."

3.9. Summary

The chapter has imposed A.C.C. on the ring R and has constructed a network of relations connecting reachability, controllability, distinguishability, realizability, and the existence of monic annihilators. Most of these relations are familiar from the vector space theory of linear systems; interestingly enough, most of the results hold when R is commutative, even though R may not satisfy A.C.C.. A useful realizability criterion has been presented in the situation where R is a Noetherian domain.

4. TORSION LINEAR MACHINES OVER PRINCIPAL IDEAL DOMAINS WITH APPLICATIONS TO CODING.

4.1 Introduction

The theory of linear systems over fields is thoroughly developed partly because of the great mathematical tractibility of vector spaces and their linear transformations. For example, the structure of such a system's state set is completely determined by its dimension over the field involved. Such state sets are finitely generated modules over a field F. Convenient generalizations seem to be finitely generated modules over a principal ideal domain J and semisimple modules.

Included in the class of linear systems over a P.I.D. are those whose state sets are finite abelian groups. These groups are, in fact, torsion modules over the integers. Intuitively, it appears that such systems would be easy to build using digital adders and counters. Furthermore, the fact that finitely generated modules over a P.I.D. have a well-known structure draws one to their study in the context of linear dynamic systems.

On the other hand, of what practical use could a linear system whose state set forms a finite abelian group be?

This chapter (with some background material provided in Appendix 1) motivates the study of systems over P.I.D.s by an applications to coding. It will turn out that a broad class of codes can be constructed whose encoders and decoders require linear machines having finite abelian groups for state sets. Then it will be shown that a certain subclass of these codes possesses some interesting error-correcting properties, and the generic form of the encoders and decoders will be derived. The remaining problem will be that of simplifying and implementing the abelian group machines involved.

Secondly, this chapter analyzes linear systems over P.I.D.s where the state sets are required to be torsion modules. The result, though not a complete decomposition, is nonetheless a considerable simplification.

Thirdly, these simplification techniques are applied to the implementation problem arising from the error-correcting codes developed above.

4.2 Coding

4.2.1. Linear Codes and the Parity Check Matrix

(The reader is referred to Ash [13], Berlekamp [8] in particular, or Gallager [9], for extensive treatments of coding theory).

For our purposes, we will assume that at each instant of time some communication channel accepts any one of p^m digits, where p is some prime number and $m > 0$. Each of these p^m digits will be represented by an element of Jp^m.

Assume that we want to represent each of $(p^m)^k$, $k > 0$, distinct messages as a sequence of k digits drawn from Jp^m. However, in order to minimize the effects of channel noise, we will append r check digits to the k information digits determined by the message. Thus to send one of p^{mk} messages, we will actually transmit a sequence of length $n = k+r$ digits drawn from Jp^m. The question is how to choose the r check digits on the basis of the k information digits.

One of the simplest schemes is to generate the r check bits by a linear transformation of the k information digits: thus if we represent the r check digits by an element $\underline{c} \in (Jp^m)^r$ and the information digits by an element $\underline{x} \in (Jp^m)^k$ we would write

$$\underline{c} = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_r \end{bmatrix} = \begin{bmatrix} \text{some } r \times k \\ \text{matrix } H_1 \\ \text{with elements from} \\ Jp^m \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_k \end{bmatrix} = H_1\underline{x} \qquad 4.1$$

If we let $\underline{y}$ denote the complete codeword consisting of k information digits followed by r check digits, i.e.,

$$\underline{y} = \begin{bmatrix} \underline{x} \\ \\ \underline{c} \end{bmatrix} \qquad 4.2$$

then we see that

$$H\underline{y} = \begin{bmatrix} H_1 & -I_r \end{bmatrix} \underline{y} = \underline{0} \qquad 4.3$$

where I_r is the r X r identity matrix. Thus each possible codeword $\underline{y}$ (of length n = k + r) is such that $H\underline{y} = \underline{0}$ for some r X n matrix H; the matrix H is called a parity-check matrix.

Thus if a codeword is transmitted with no alteration by noise, the received word $\underline{y}$ of length n must satisfy the equation $H\underline{y} = \underline{0}$. On the other hand, if the codeword is altered by noise, then the received word $\underline{y}$ may be such that

$$\underline{s} = H\underline{y} \neq \underline{0} \qquad 4.4$$

The r-tuple $\underline{s} \in (Jp^m)^r$ is called the syndrome of the received word $\underline{y}$. If $\underline{s} \neq \underline{0}$ we are guaranteed that some error has occurred; the converse is not true however.

4.2.2. Error-Correcting Codes over Jp^m

In the case of error-correcting codes, it often turns out to be easier to choose the parity-check matrix H rather than the matrix H_1 appearing in equation 4.1. We now construct a code that will correct any error that occurs in any one of the n digit positions of $\underline{y}$. Suppose that individual digits are chosen from Jp^m, and that the required block length $n = p^d-1$. Let θ be a P-primitive element (see Appendix 1) in some local extension of Jp^m of degree d. Since θ^i can be represented by a d X 1 column vector $\underline{\theta}^i$, we consider the (1 + d) X (p^d-1) matrix H (with entries from Jp^m) given by:

$$H = \begin{bmatrix} 1 & 1 & \cdots\cdots & 1 & 1 & 1 \\ \underline{\theta}^{p^d-2} & \underline{\theta}^{p^d-3} & \cdots\cdots & \underline{\theta}^2 & \underline{\theta} & \underline{1} \end{bmatrix} \qquad 4.5$$

Let the codeword $\underline{y}$ be transmitted and suppose that the channel adds a noise vector $\underline{e}$ to $\underline{y}$. Assume that $\underline{e}$ has at most one nonzero component, i.e., an error occurs in at most one digit position. Then $(\underline{y} + \underline{e})$ is received and we calculate

$$\begin{aligned} \underline{s} &= H(\underline{y} + \underline{e}) \\ &= H\underline{e} \qquad 4.6 \end{aligned}$$

since $\underline{y}$ is a codeword. By the assumption on $\underline{e}$, $\underline{s}$ has the form: a times some column of H. That is

$$\underline{s} = \begin{bmatrix} \sigma_0 \\ \sigma_1 \end{bmatrix} = a \begin{bmatrix} 1 \\ \theta^i \end{bmatrix} \qquad 4.7$$

where $a \in Jp^m$ is the value of the single nonzero component of $\underline{e}$, $\sigma_0 \in Jp^m$, $\sigma_1 \in (Jp^m)^d$. The object is to solve 4.7 for the value of the error, a, and the position of the error which is represented by θ^i. Clearly, if $\sigma_0 = 0$, no error occurred. If $\sigma_0 \neq 0$, then an error of value $\sigma_0 = a$ has occurred. To find its position we solve

$$\sigma_1 = a\ \theta^i = \sigma_0\ \theta^i \qquad 4.8$$

for θ^i. If exactly one error occurred, 4.8 will be soluble for i. By Lemma A.7 (see Appendix 1) this solution is unique and the error occurred at that component of $\underline{y}$ corresponding to the column of the H matrix containing θ^i. Thus we can completely determine the error $\underline{e}$ and can subtract $\underline{e}$ from the received word to find the actual word $\underline{y}$ transmitted. If equation 4.8 has no solution for θ^i, more than one error occurred.

Notice that 4.7 represents two equations; this is not surprising since we have two unknowns, namely the error value and the error position. It seems intuitively plausible that to correct errors in any two distinct digits positions we will need four equations, since we will have four unknowns: two error values and two error positions. So, to correct any two errors we will try the $(1 + 3d) \times (p^d-1)$ parity check matrix H given by

$$H = \begin{bmatrix} 1 & \cdots & 1 & \cdots & 1 & 1 & 1 \\ \theta^{p^d-2} & \cdots & \theta^i & \cdots & \theta^2 & \theta & 1 \\ & & (\theta^i)^2 & \cdots & \theta^4 & \theta^2 & 1 \\ & & (\theta^i)^3 & \cdots & \theta^6 & \theta^3 & 1 \end{bmatrix} \tag{4.9}$$

Suppose an error of value a_1 occurs in the position of θ^i and an error of value a_2 occurs in the position of θ^j where $\theta^i \neq \theta^j$. Then we calculate the syndrome of the received word:

$$\underline{s} = \begin{bmatrix} \sigma_0 \\ \sigma_1 \\ \sigma_2 \\ \sigma_3 \end{bmatrix} = H\,(\underline{v} + \underline{e}) = H\underline{e} = a_1 \begin{bmatrix} 1 \\ \theta^i \\ (\theta^i)^2 \\ (\theta^i)^3 \end{bmatrix} + a_2 \begin{bmatrix} 1 \\ \theta^j \\ (\theta^j)^2 \\ (\theta^j)^3 \end{bmatrix} \tag{4.10}$$

where σ_0, a_1, $a_2 \in Jp^m$ and σ_1, σ_2, $\sigma_3 \in (Jp^m)^d$.

Let $x = \theta^i$

and $y = \theta^j$ 4.11

Equation 4.10 then yields the following four equations:

$$\sigma_0 = a_1 + a_2 \;, \tag{4.12}$$

$$\sigma_1 = a_1 x + a_2 y \;, \tag{4.13}$$

$$\sigma_2 = a_1 x^2 + a_2 y^2 \;, \tag{4.14}$$

and

$$\sigma_3 = a_1 x^3 + a_2 y^3 \;, \tag{4.15}$$

These four equations must now be solved for a_1, a_2, x, and y. We may obtain a_1 and a_2 in terms of x and y by viewing 4.12 and 4.13 as

$$\begin{bmatrix} \sigma_0 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ x & y \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} \qquad 4.16$$

The determinant (over $R = Jp^m[x]/\langle q(x)\rangle$) of the matrix in this equation is $(y-x) = (\theta^j - \theta^i)$. Since θ^j and θ^i are distinct, and since θ is P-primitive in R, θ^j and θ^i lie in different cosets of the maximal ideal P of R. Hence $\theta^j - \theta^i \notin P$, and so, because R is local, y-x is a unit of R. Hence the above matrix is invertible and we can write

$$\begin{bmatrix} a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ x & y \end{bmatrix}^{-1} \begin{bmatrix} \sigma_0 \\ \sigma_1 \end{bmatrix}$$

$$= (y-x)^{-1} \begin{bmatrix} y & -1 \\ -x & 1 \end{bmatrix} \begin{bmatrix} \sigma_0 \\ \sigma_1 \end{bmatrix} \qquad 4.17$$

<u>Remark</u>: to do this we view a_1, a_2 and σ_0 as elements of R as opposed to J Jp^m, i.e., as d-tuples instead of scalars. We must be careful using this notation because a_1, a_2 and σ_0 are treated as scalars in equation 4.10; they are so treated for the sake of economy of check digits, and because at this stage no interpretation is attached to non-scalar errors. It appears possible to consider non-scalar errors, but this is a subject for later study. In any case, we should regard the scalars a_1, a_2 and σ_0 of 4.10 as being

shorthand for the d-tuples $[a_1, 0, 0,\ldots,0]^T$, etc. Then if equation 7-38 results in elements a_1 or a_2 having nonzero components along coordinates other than the first, we know a mistake has occurred - presumably the assumption that we have no more than two errors has been violated.

Returning to the main development, we can write 4.14 and 4.15 as

$$\begin{bmatrix}\sigma_2\\ \sigma_3\end{bmatrix} = \begin{bmatrix}x^2 & y^2\\ x^3 & y^3\end{bmatrix}\begin{bmatrix}a_1\\ a_2\end{bmatrix} \tag{4.18}$$

$$= (y-x)^{-1}\begin{bmatrix}x^2 & y^2\\ x^3 & y^3\end{bmatrix}\begin{bmatrix}y & -1\\ -x & 1\end{bmatrix}\begin{bmatrix}\sigma_0\\ \sigma_1\end{bmatrix} \tag{4.19}$$

$$= (y-x)^{-1}\begin{bmatrix}x^2y-xy^2 & y^2-x^2\\ x^3y-xy^3 & y^3-x^3\end{bmatrix}\begin{bmatrix}\sigma_0\\ \sigma_1\end{bmatrix}$$

$$= \begin{bmatrix}-xy & x+y\\ -xy(x+y) & x^2+xy+y^2\end{bmatrix}\begin{bmatrix}\sigma_0\\ \sigma_1\end{bmatrix}, \tag{4.20}$$

where 4.17 was used to obtain 4.19.

Define $$z_1 = xy \tag{4.21}$$

and $$z_2 = x+y \tag{4.22}$$

Note that $-xy(x+y) = z_1z_2$ and $x^2+xy + y^2 = z_2^2 = z_1$. We can rewrite 4.20 as

$$\begin{bmatrix}\sigma_2\\ \sigma_3\end{bmatrix} = \begin{bmatrix}-z_1 & z_2\\ -z_1z_2 & z_2^2-z_1\end{bmatrix}\begin{bmatrix}\sigma_0\\ \sigma_1\end{bmatrix}$$

or
$$\sigma_2 = -\sigma_0 z_1 + \sigma_1 z_2 \tag{4.23}$$

$$\sigma_3 = -\sigma_0 z_1 z_2 + \sigma_1 (z_2^2 - z_1) \tag{4.24}$$

We can eliminate z_2 by multiplying 4.24 by σ_1 and then substituting $\sigma_1 z_2 = \sigma_2 + \sigma_0 z_1$ from 4.23. After cancellation:

$$(\sigma_1\sigma_3 - \sigma_2^2) = (\sigma_0\sigma_2 - \sigma_1^2) z_1 \tag{4.25}$$

In a similar fashion:

$$(\sigma_0\sigma_3 - \sigma_1\sigma_2) = (\sigma_0\sigma_2 - \sigma_1^2) z_2 \tag{4.26}$$

Now consider equations 4.21, 4.22; write $y = x^{-1} z_1$ and substitute in 4.22:

$$z_2 = x + x^{-1} z_1$$

or,
$$x^2 = z_2 x + z_1 = 0 \tag{4.27}$$

Note from the symmetry of 4.21, 4.22, that y is also a root of 4.27. Multiplying 4.27 by $(\sigma_0\sigma_2 - \sigma_1^2)$ we obtain:

$$(\sigma_0\sigma_2 - \sigma_1^2) x^2 - (\sigma_0\sigma_3 - \sigma_1\sigma_2) x + (\sigma_1\sigma_3 - \sigma_2^2) = 0 \tag{4.28}$$

We have the following result (using Lemma A7): if two or fewer errors occur in transmission and $(\sigma_0\sigma_2 - \sigma_1^2) \neq 0$, equation 4.28 has exactly two distinct roots of the form θ^i. These two roots determine precisely the <u>location</u> of the errors, whose <u>values</u> can be determined from 4.19. If $(\sigma_0\sigma_2 - \sigma_1^2) = 0$, then all coefficients of 4.28 are 0 (because of 4.25 and 4.26) and we obtain no information from 4.28.

Since the quantity $(\sigma_0\sigma_2-\sigma_1^2)$ seems critical to this error-correcting code, we want to know under what conditions $(\sigma_0\sigma_2-\sigma_1^2) = 0$. Substituting from 4.12, 4.13, and 4.14,

$$\begin{aligned}(\sigma_0\sigma_2-\sigma_1^2) &= (a_1 + a_2)(a_1x^2 + a_2y^2) - (a_1x + a_2y)^2 \\ &= a_1^2x^2 + a_1a_2y^2 + a_1a_2x^2 + a_2^2y^2 \\ &- a_1^2x^2 - 2a_1a_2xy - a_2^2y^2 \\ &= a_1a_2(y^2+x^2 - 2xy) \\ &= a_1a_2(x-y)^2 \qquad 4.29\end{aligned}$$

Since $x = \theta^i \neq y = \theta^j$, $(x-y)$ and $(x-y)^2$ are units of R. Hence, $(\sigma_0\sigma_2-\sigma_1^2) = 0$ if and only if the two error values a_1, a_2 are such that $a_1a_2 = 0$. Note that if a_1, a_2 are elements of Jp instead of Jp^m, $a_1a_2 = 0$ implies either $a_1 = 0$ or $a_2 = 0$ (or both). Thus it appears in general that this code cannot correct all errors in two or fewer positions. On the other hand, we could argue that $a_1 \neq 0$, $a_2 \neq 0$ and $a_1a_2 = 0$ is an event of low probability in a code over Jp^m, $m > 1$, and that the resulting decoder failure may not be serious. This might be reasonable if we could detect the event $a_1 = 0$ or $a_2 = 0$ whenever $a_1a_2 = 0$.

In any case, the generalization of this scheme to codes that correct errors in more than two positions appears straightforward but tedious. This extension is not carried out here. It is sufficient for the purposes of this chapter to motivate coding over Jp^m using parity check matrices H whose columns have the form $[1, \theta^i, (\theta^i)^2, \ldots]^T$ (where θ is a P-primitive element of $R = Jp^m[x]/\langle q(x)\rangle$).

4.2.3 Implementation of Linear Codes

Turning to the implementation problem, we can identify three main subsystems of a coding/decoding system. The first is the encoder which calculates the r check digits after receiving the k information digits. The second calculates the syndrome $\underline{s}$ of a received word, and the third processes the syndrome to identify errors. The following discussion is confined to the encoder and the syndrome calculator.

Suppose the parity check matrix H is an r X (k+r) matrix with entries from Jp^m; the columns of H can be viewed as elements of the module $(Jp^m)^r$. Suppose further that the columns of H can be arranged in the form

$$H = \left[\varphi^{n-1}\underline{b}, \ldots, \varphi\underline{b}, \underline{b} \right] \qquad 4.30$$

where $\underline{b}$ is an element of $(Jp^m)^r$ and φ is an (abelian group) endomorphism of $(Jp^m)^r$. Now let $\underline{u}$ denote the received word, $\underline{u} = [u_0, u_1, \ldots, u_{n-2}, u_{n-1}]^T$. Clearly,

$$\underline{s} = H\underline{u} = \sum_{i=0}^{n-1} \varphi^{n-1-i}\, \underline{b}\, u_i \qquad 4.31$$

The important thing here is that now $\underline{s}$ can be viewed as the state of a linear system

$$\underline{s}_{t+1} = \varphi \underline{s}_t + \underline{b}\, u_t , \qquad \underline{s}_0 = \underline{0}, \qquad 4.32$$

which is reached after the application of the n (scalar) inputs $u_0, u_1, \ldots,$ u_{n-1} (in this order). In other words, the syndrome $\underline{s}$ can be calculated by feeding the incoming digits u_i into the linear system 4.3.2.. After n inputs, the state $\underline{s}_n$ of the represented by the contents of r registers say, is precisely the syndrome $\underline{s}$. Now $\underline{s}$ can be used by the rest of the error processor and the linear system can be reset to the zero state prior to receiving more words.

This seems to be a practical scheme for calculating the syndrome, and so it is worth some effort to put H in the form 4.30. (It may also be possible to choose a specific endomorphism φ and then analyze the properties of a code with parity check matrix given by 4.30.)

Given a parity check matrix as in 4.30, can we also calculate the r check digits in a straightforward manner? Let the rightmost r columns be considered as a matrix H_2:

$$H_2 = \left[\varphi^{r-1}\underline{b}, \ldots, \varphi\underline{b}, \underline{b}\right] \qquad 4.33$$

Then the matrix H can be written

$$H = \left[\varphi^{k-1}\underline{h}, \ldots, \varphi\underline{h}, \underline{h} \quad H_2\right] \quad , \qquad 4.34$$

where $$h = \varphi^r\underline{b} \qquad 4.35$$

Let the codeword $\underline{y}$ be $[u_0, u_1, \ldots, u_{k-1}, c_1, c_2, \ldots, c_r]^T$ where the u_i are information digits and the c_i are check digits; it is required to find the c_i from $H\underline{y} = \underline{0}$ from $H\underline{y} = \underline{0}$ we obtain

$$-H_2 \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_r \end{bmatrix} = \begin{bmatrix} \varphi^{k-1}\underline{c}, \ldots, \varphi\underline{c}\,, \ \underline{c} \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_{k-1} \end{bmatrix} \qquad 4.36$$

We must now require that H_2 be invertible. This can be guaranteed in various ways: notice that if no r X r submatrix of H is invertible, then in general H cannot uniquely determine r check digits at all. So we can always assume that H contains an invertible r X r submatrix. To guarantee that such a submatrix appears at the right of H, we only have to require that $\varphi^t = 1$ for some t sufficiently large. This will always be the case if φ is invertible - i.e., if φ is an element of the group of units in a ring of r X r matrices over any finite ring. In practice, φ will always be invertible, and hence H_2 will always be invertible.

Given that H_2 is invertible, we can rewrite 4.36:

$$\underline{c} = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_r \end{bmatrix} = -H_2^{-1} \begin{bmatrix} \varphi^{k-1}\underline{h}, \ldots, \varphi\underline{h}, \ \underline{h} \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_{k-1} \end{bmatrix} \qquad 4.37$$

Hence, $\underline{c} = -H_2^{-1} \sum_{i=0}^{k-1} \varphi^{k-1-i} \ \underline{h}\ u_i,$ $\qquad$ 4.38

Consequently, the check digits $\underline{c}$ can be viewed as the output $\underline{c}_k$ at time k of the linear system

$$\underline{x}_{t+1} = \varphi \underline{x}_t + \underline{h}\, u_t, \qquad \underline{x}_0 = \underline{0},$$

$$\underline{c}_t = -H_2^{-1}\, \underline{x}_t \qquad 4.39$$

driven by the (scalar) sequence $u_0, u_1, \ldots, u_{k-1}$. In other words the r check digits can be calculated by the linear system 4.39. These r digits can be placed in a shift register at time k and then shifted into the channel sequentially immediately after the digits u_i have been transmitted.

In summary, if the parity check matrix H of a linear code can be put in the form 4.30, the encoder and syndrome calculator can be conveniently implemented by means of linear systems whose state sets are finite abelian groups, In particular, the error-correcting codes developed above fall into this class: the matrix φ is simply related to the matrix representation of a P-primitive element in a local extension of Jp^m.

The next section of this chapter analyzes a general class of linear systems that includes those described by 4.39. The following section will apply these results towards implementing several error-correcting codes of the type discussed above. These examples will be

(1) a single error correcting code over Jp^m

(2) double error correcting codes over J_n, n not a prime power.

4.3 Linear Systems over Principal Ideal Domains J

4.3.1 General Formulation

Definition 4.1: A (discrete-time, time-invariant) linear system Σ over a principal ideal domain J is a triple $\Sigma = (\psi, \varphi, \eta)$ where $\psi: U \to X$, $\varphi: X \to X$, $\eta: X \to Y$ are J homomorphisms. U, X, and Y are finitely generated (F.G.) J-modules; U is the input module, X is the state module, and Y is the output module. Σ is interpreted as describing the dynamic equations

$$x_{t+1} = \varphi(x_t) + \psi(u_t) \qquad 4.40$$

$$y_t = \eta(x_t) \qquad 4.41$$

where x_t, $x_{t+1} \in X$ are the states of Σ at times t, t+1 respectively, $u_t \in U$ is the input applied at time t, and $y_t \in Y$ is the output at time t.

As discussed before, X can be veiwed as a J[z]-module and Σ induces a J[z]-homomorphism $f: \Omega \to \Gamma$ where $\Omega = U[z]$ and $\Gamma = Y[[z^{-1}]]$. f can be factored as $f = H \circ G$ where $G: \Omega \to X$ and $H: X \to \Gamma$ are also J[z]-homomorphisms. Σ is reachable if G is onto and distinguishable if H is 1-1; Σ is canonical if it is both reachable and distinguishable.

One of the properties of a F.G. module M over a P.I.D. J is that M is the direct product of a free module M_f and a torsion module M_t, both of which, of course, are finitely generated. (A torsion J-module M_t is one in which every element x is a torsion element, i.e., there exists $r \in J$, $r \neq 0$, such that $rx = 0$). Hence in the definition above, we can write

$$U = U_f \oplus U_t$$

$$X = X_f \oplus X_t \qquad 4.42$$

and $$Y = Y_f \oplus Y_t$$

where the subscripts f and t denote free and torsion modules.

The complete theory of such systems will be taken up elsewhere: roughly speaking this study breaks up into the study of linear systems whose state sets are free modules and the study of linear systems whose input, state, and output sets are all torsion modules over the P.I.D. J. It is the latter type that will be discussed in this chapter.

Definition 4.2: A finite abelian machine (F.A.M.) is a linear system $\Sigma = (\psi: U \to X, \varphi: X \to X, \eta: X \to y)$ over a P.I.D. J such that U, X, and Y are all F.G. torsion modules over J. A F.A.M. will also be called a torsion linear machine over a P.I.D..

Note that a F.A.M. over the integers is an example of a group homomorphic machine as defined by Brockett and Willsky [4] and Arbib [5]. Furthermore the encoders and decoders discussed in the previous section are all F.A.M.s.

4.3.2 Endomorphisms of F.G. Torsion Modules over a P.I.D.

The problem of F.A.M. decomposition can be viewed as that of decomposing a F.G. torsion J-module X over an endomorphism φ where J is a P.I.D.. Equivalently, the problem is that of decomposing a J[z]-module X where J is a P.I.D., and X is a F.G. torsion J-module. The starting point for our analysis is the well-known decomposition of F.G. torsion module over a P.I.D.:

Definition 4.3: Let J be a P.I.D., X = a J-module, and p = any prime (irreducible) element of J. Then X[p] is defined by

$$X[p] = \{x \in X \mid p^r x = 0, \text{ some } r > 0\}. \qquad 4.43$$

A module X such that $\forall x \in X$, $p^r x = 0$, some $r > 0$ is known as a p-module.

Proposition 4.1 (Decomposition of F.G. torsion modules over a P.I.D.) Let J be a P.I.D. and X be a F.G. torsion J-module.

Then

(a) $$X = \bigoplus_p X[p] \qquad 4.44$$

where the direct sum is taken over all primes p such that $X[p] \neq 0$, and

(b) each p-module X[p] can be written as the direct sum of certain cyclic submodules $J_{p^{m_i}}$, $m_i > 0$,

$$X[p] = J_{p^{m_i}} \oplus \dots \oplus J_{p^{m_3}} \qquad 4.45$$

where $J_{p^{m_i}} \simeq J/\langle p^{m_i}\rangle$, $i = 1,\dots,s$,

$\langle p^{m_i}\rangle$ is the ideal of J generated by p^{m_i},

and $m_1 \leq m_2 \leq \dots \leq m_s$ 4.46

The sequence $m_1, m_2, \dots,_s$ is uniquely determined.

Proof: see any algebra textbook.

The state set of a F.A.M. is thus of the form described by 4.44 and 4.45. This theorem spells out the basic structure of the module upon which the endomorphism φ operates. We will now investigate how φ interacts with this structure.

<u>Proposition 4.2.</u> Let X be a F.G. torsion module over J = a P.I.D., and let $\varphi \in \text{End}_J(X)$. Thus each p-submodule X[p] of X is φ-invariant. Thus the action of φ on X can be completely characterized by its action on each of the direct summands X[p].

<u>Proof</u>: Let $X[p] \neq 0$ be one of the direct summands of X over J, and let $x \in X[p]$. Then $p^r x = 0$, some $r \geq 1$. Since φ is a homomorphism, $p^r\varphi(x) = \varphi(p^r x) = \varphi(0) = 0$. Hence, $\varphi(x) \in X[p]$, i.e., X[p] is φ-invariant. Q.E.D.

In terms of a matrix representation for φ, the above lemma states that φ can be represented as

$$\varphi = \begin{bmatrix} \varphi_1 & 0 & 0 \\ 0 & \varphi_2 & 0 \\ 0 & 0 & \ddots\varphi_q \end{bmatrix} \qquad 4.47$$

where each submatrix φ_i represents the action of φ on $X[p_i]$. This corresponds to a decomposition of X over J[z] into a direct sum of J[z]-submodules. Hence our problem reduces to that of investigating the endomorphisms of F.G. p-modules X[p] over a P.I.D. J.

The approach now taken relies on the theory developed in chapter 5 (below) for the general cascade decomposition of linear systems over rings with chain conditions. Specifically it will be first shown that F.G.

p-modules over a P.I.D. J satisfy both ascending and descending chain conditions. From Chapter 5 it will follow immediately that if φ is an endomorphism of X[p], then X[p] is the direct sum of two φ-invariant submodules X_a, X_n where the action of φ is an automorphism on X_a and is nilpotent on X_n.

Proposition 4.3. Let X be a F.G. torsion module over a P.I.D. J. Then X satisfies (a) the ascending and (b) the descending chain conditions on submodules.

Proof. See Appendix 2.

Proposition 4.4. Let J be a P.I.D.; let X[p] be a F.G. p-module over J, and let φ be a J-endomorphism of X[p]. Then $X[p] = X_a \oplus X_n$ where X_a and X_k are φ-invariant and

(1) the restriction of φ to X_a is an automorphism

and (2) the restriction of φ to X_n is nilpotent.

Proof: by proposition 4.3, X[p] satisfies both ascending and descending chain conditions. The statement follows from the results of chapter 5.

Corollary 4.4.1. Let J be a P.I.D.; let X be a F.G. torsion module over J and let φ be a J-endomorphism of X. Then X is the direct sum of certain φ-invariant p-submodules where the action of φ on each such submodule is either nilpotent or bijective.

Proof: Combining propositions 4.2 and 4.4 yields the result immediately.

The problem now breaks up into two parts: first, the analysis of automorphisms of p-modules, and secondly, the analysis of nilpotent endomorphisms on p-modules.

4.3.3 Automorphisms of F.G. p-Modules

As discussed previously, a F.G. p-module X contains a submodule X_p consisting of all elements x in X such that $px = 0$. X_p is a finite-dimensional vector space over $J_p = J/(p)$, and we know a great deal about vector spaces. The general technique to be used will be to analyze how X_p is related to X and, in particular, how the operation of the endomorpisn ϕ on X_p can be related to its operation on all of X.

Definition 4.3 Let $X \neq (0)$ be a F.G. p-module. The period of X is defined to be p^r where r is the least positive integer such that $p^r X = (0)$. The exponent of X is defined to be the number r such that p^r is the period of X.

Let $x \in X$. The period of $x \in X$ is defined to be p^r where r is the least positive integer such that $p^r x = 0$. The exponent of x is defined to be the number r such that p^r is the period of x.

Proposition 4.5: Let X be a F.G. p-module, $X_p = \{x \in X | px = 0\}]$ Then every non-zero submodule of X has a nontrivial (i.e., $\neq (0)$) intersection with X_p.

Proof: Let $Y \neq (0)$ be a submodule of X. Since $Y \neq (0)$. $\exists$ $y \in Y$ such that $y \neq 0$. Since X is a p-module, y has a finite period r. Since r is the least positive integer such that $p^r y = 0$, we have that $p^{r-1} y \neq 0$. Since $y \in Y$, $p^{r-1} y \in Y$. But $p(p^{r-1}y) = 0$, and so $p^{r-1}y \in X_p$. Thus we have

$$0 \neq p^{r-1} y \in Y \cap X_p.$$ **Q.E.D.**

Proposition 4.6: Let X be a F.G. p-module, $X_p = \{x \in X | px = 0\}$. Suppose φ: X X $\in$ $\mathrm{End}_J(X)$. Then φ is an automorphism of X if and only if the restriction of φ to X_p is an automorphism.

Proof: $\Rightarrow$: Let φ be an automorphism of X. Clearly, X_p is φ-invariant. Thus φ is an injective endomorphism of X_p. Since φ^{-1} exists, φ is also an automorphism of X_p

: Let the restriction of φ to X_p be an automorphism. Now suppose φ is not an injective endomorphism of X, so that ker $\varphi \neq (0)$. By Proposition 4.5, ker φ must have a non-zero intersection with X_p; i.e., $\exists\ 0 \neq y \in X_p$ such that $\varphi(y) = 0$. But this contradicts the fact that the restriction of φ to X_p is an automorphism.

Hence φ: X → X is injective. So, $\varphi(X) \simeq X$ and $\varphi(X) \subseteq X$. By the descending chain condition, we have $\varphi(X) = X$, and hence φ is surjective.

Thus φ, being both injective and surjective, is an automorphism of X.

Q.E.D.

The above lemma has the practical consequence that to test whether a given φ is an automorphism, where φ: X → X, we only have to check whether φ is a nonsingular transformation of the vector space X_p. If φ is given as a matrix, then we merely reduce all its coefficients modulo p and calculate the determinant of the result. This technique can be immensely convenient if the exponent of X is very large.

This last lemma also illustrates the usefulness of investigating the action, of φ on the vector space X_p embedded in X.

Definition 4.4 Let X be a module over J. A set $\{g_1,\ldots,g_s\}$ of generators for X will be called a t-basis for X iff $X = \bigoplus_{i=1}^{s} \langle g_i \rangle$, where $\langle g_i \rangle$ denotes the cyclic submodule of X generated by g_i.

Proposition 4.7: A set of generators $\{g_1,\ldots,g_s\}$ for a J-module X is a t-basis if $\sum_{i=1}^{s} a_i g_i = 0$ implies $a_i g_i = 0$, $i = 1,\ldots,s$, where $a_i \in J$, $i = 1,\ldots,s$.

Proof: $\Rightarrow$: Let $\{g_1,\ldots,g_s\}$ be a t-basis for X, so that $X = \bigoplus_{i=1}^{s} \langle g_i \rangle$, and suppose $\sum_{i=1}^{s} a_i g_i = 0$, $a_i \in J$. Suppose further that $a_1 g_1 \neq 0$. Then $a_1 g_1 = - \sum_{i=2}^{s} a_i g_i \neq 0$. But then $\langle g_1 \rangle \cap \bigoplus_{i=2}^{s} \langle g_i \rangle \neq 0$, which contradicts the fact that $X = \langle g_1 \rangle \oplus (\bigoplus_{i=2}^{s} \langle g_i \rangle)$. Thus $a_1 g_1 = 0$. Continuing in this way a finite number of times, we conclude that $a_i g_i = 0$, $i = 1,\ldots,s$.

: Let $\{g_1,\ldots,g_s\}$ be a set of generators for X with the property that $\sum_{i=1}^{s} a_i g_i = 0$ implies $a_i g_i = 0$, $i=1,\ldots,s$. Since $\{g_1,\ldots g_s\}$ generate X, we have $X = \sum_{i=1}^{s} \langle g_i \rangle$. Claim: $X = \langle g_1 \rangle \oplus \sum_{i=2}^{s} \langle g_i \rangle$. Clearly, $X = \langle g_1 \rangle + (\sum_{i=2}^{s} \langle g_i \rangle)$. All we have to show is that $\langle g_1 \rangle \cap (\sum_{i=2}^{s} \langle g_i \rangle) = (0)$.

Suppose $x \in <g_1> \cap (\sum_{i=2}^{s} <g_i>)$. Since $x \in <g_1>$, $x = a_1g_1$, some $a_1 \in J$. Since $x \in (\sum_{i=2}^{s} <g_i>)$, $x = \sum_{i=2}^{s} a_ig_i$, some $a_i \in J$, $i = 2,\ldots,s$. Hence, $x = a_1g_1 = \sum_{i=2}^{s} a_ig_i$, and so $a_1g_1 + \sum_{i=2}^{s} (-a_i) g_i = 0$. By assumption then, $a_ig_i = 0$, $i = 1,\ldots,s$. Thus $x = 0$; i.e., $<g_1> \cap (\sum_{i=2}^{s} <g_i>) = (0)$, and $X = <g_1> \oplus \sum_{i=2}^{s} <g_i>$. In a similar fashion we can show that $\sum_{i=2}^{s} <g_i> = <g_2> \oplus \sum_{i=3}^{s} <g_i>$. Proceeding in this fashion a finite number of times, we find that $X = \overset{s}{\underset{i=1}{\oplus}} <g_i>$, and hence $\{g_1,\ldots,g_s\}$ is a t-basis for X. Q.E.D.

<u>Proposition 4.8</u>: Let X be a F.G. p-module over a P.I.D. J, and let $\{f_1,\ldots,f_s\}$ be a basis for the embedded vector space X_p. Then we can find a t-basis $\{e_1,\ldots,e_s\}$ for X such that

$$\forall i = 1,\ldots,s, \qquad p^{m_i-1} \cdot e_i = f_i \ , \quad \text{for some } m_i \geq 1 \qquad 4.48$$

<u>Proof</u>: By induction on s. If X_p is s-dimensional over J_p, then $X \simeq \overset{t}{\underset{i=1}{\oplus}} J_p{}^{m}i$, let $\{g_1,\ldots,g_t\}$ be a t-basis for X, and let p^{m_i} be the period of g_i. Then $\{p^{m_i-1} g_i\}_{i=1}^{t}$ is a basis for X_p. Thus if X_p is s-dimensional, t = s).

Suppose s = 1. Then $X \simeq J_{p^{m_i}}$ and $X_p \simeq J_p$. Let $\{f_1\}$ be a basis for X_p and let g_1 be any generator of X. Then $0 \neq p^{m_1-1} g_1 \in X_p$. But $X_p \simeq J_p$ which is a field. Thus we can divide f_1 by $p^{m_1-1} g_1$ to obtain an element $a \in X_p$ such that $a\, p^{m_1-1} g_1 = f_1$. Clearly $a \not\equiv 0 \pmod{p}$. Let b be any element of J such that $b \equiv a \pmod{p}$. Then let $e_1 = bg_1$. Then $p^{m_1-1} e_1 = f_1$. Since $p^{m_1-1} e_1 \neq 0$, e_1 has period p^{m_1}, and so is also a generator of $X \simeq J_{p^{m_1}}$. Thus $X = \langle e_1 \rangle$ and $p^{m_1-1} e_1 = f_1$ as required. So the statement is true for s = 1.

Assume the statement is true for all $s \leq k$. Suppose X_p is of dimension k+1, and let $\{f_1, \ldots, f_{k+1}\}$ be a given basis for X_p. Let $G = \{g_1, \ldots, g_{k+1}\}$ be any t-basis for X; we can let p^{m_i} be the period of each g_i, $m_1 \leq \ldots \leq m_{k+1}$.

Let $$f_1 = \sum_{i=1}^{k+1} a_i g_i, \qquad a_i \in J. \qquad 4.49$$

Since $pf_1 = 0$, $$\sum_{i=1}^{k+1} pa_i g_i = 0 \qquad 4.50$$

Since G is a t-basis, $pa_i g_i = 0$, $i = 1, \ldots, k+1$.

Thus $a_i p \equiv 0 \pmod{p^{m_i}}$, and hence p^{m_i-1} divides a_i.

Let $$a_i = p^{m_i-1} b_i \qquad i = 1, \ldots, k+1 \qquad 4.51.$$

We can then write

$$f_1 = \sum_{i=1}^{k+1} b_i\, p^{m_i-1} g_i \qquad 4.52$$

Clearly, not all $b_i \equiv 0 \pmod{p}$, or else f_1 would = 0.

Hence there exists a largest integer $j \leq k+1$ such that:

$$i < j \quad \text{implies } b_i \equiv 0 \pmod{p}.$$

Then we can write

$$f_1 = \sum_{i=j}^{k+1} b_i p^{m_i - 1} g_i \tag{4.53}$$

By the ordering of the m_i, we have $m_j \leq \ldots \leq m_{k+1}$, and so we can write

$$f_1 = p^{m_j - 1} \sum_{i=j}^{k+1} b_i \, p^{m_i - m_j} g_i \tag{4.54}$$

Let

$$e_1 = \sum_{i=j}^{k+1} b_i \;\; p^{m_i - m_j} g_i \tag{4.55}$$

By 7.62, we have $p^{m_j - 1} . \, e_1 = f_1$, as required. 4.56

Since $pf_1 = 0$, we have $p^{m_j} e_1 = 0$.

Thus $<e_1> \simeq J_p{}^{m_j}$, where $<e_1>$ is the cyclic submodule generated by e_1 and $<e_1>$ is also isomorphic to $<g_j>$, which is one of the direct summands of X. Thus for some submodule X_2, we can write $X = <e_1> \oplus X_2$.

Now all we have to show is that $\{f_2, \ldots, f_{k+1}\}$ is a basis for the embedded vector space X_{2p} of X_2. Then we can apply the induction hypothesis and the theorem is proved. However, X_p was assumed to be (k+1)-dimensional, and is easy to argue that X_{2p} is k-dimensional. Since $<e_1> \cap X_2 = 0$, $<f_1> \cap X_{2p} = 0$ also. Therefore $<f_1> \oplus X_{2p} = X_p$. But $\{f_2, \ldots, f_{k+1}\}$

generates a k-dimensional subspace of X_p disjoint from $<f_1>$; hence $\{f_2,\ldots,f_{k+1}\}$ is a basis for X_{2p}. By the induction hypothesis we can find a t-basis $\{e_2,\ldots,e_{k+1}\}$ for X_2 such that $\forall i = 2,\ldots,k+1$

$$p^{m_i-1} e_i = f_i, \qquad \text{for some } m_i \geq 1$$

Hence we have found a t-basis $\{e_1,\ldots,e_{k+1}\}$ for X such that $\forall i$, $p^{m_i-1} e_i = f_i$ some $m_i \geq 1$

Q.E.D.

The content of the above lemma is simply that a set of "axes" for X_p can be extended to a set of "axes" or "coordinates" for X. We can then always embed a particular one-dimensional subspace of X_p in a cyclic direct summand of X. Thus a particular "orientation" of X_p can be extended to a similar orientation for X.

This is important because we are able to find bases of X_p with aggreeable properties, such as invariance under φ. The above lemma will help us extend these properties to all of X. A basis for X_p of particular interest is that provided by the rational canonical form for a matrix representing a vector space endomorphism. The results needed are summarized below (see Herstein [14]):

Proposition 4.9: Let V be a finite dimensional vector space over the field F. Let the matrix T represent an endomorphism φ of V. Then V is a F.G. torsion module over the P.I.D. F[x] (with $x \cdot v = \varphi(v)$ for $v \in V$), and is consequently the direct sum of certain p-modules V[p], (where p = prime = irreducible polynomial $\in$ F[x], and p^e V[p] = 0). Each p-module V[p] is the direct sum of cyclic p-modules with periods p^{e_i}, $e_i \geq e$. A basis can be found for each cyclic p-module of period p^{e_i} such that T (restricted to this subspace) takes the form:

$$\begin{bmatrix} 0 & 0 & 0 & & 0 & -a_0 \\ 1 & 0 & 0 & & 0 & -a_1 \\ 0 & 1 & 0 & & 0 & -a_2 \\ 0 & 0 & 1 & & 0 & -a_4 \\ & \cdots & & & & \\ 0 & 0 & 0 & & 1 & -a_{n-1} \end{bmatrix} \qquad 4.57$$

Here, a_i is the coefficient of x^i in the polynomial p^{e_i}. Note that with respect to this basis, say $\{f_1,\ldots,f_n\}$, we have

$$f_i = \varphi^{i-1}(f_1), \qquad 1 \le i < n \qquad 4.58$$

and

$$\varphi^n(f_1) = (-\sum_{i=0}^{n-1} a_i\varphi^i)\cdot f_1 \qquad 4.59$$

Furthermore, $$p^{e_i} = x^n + \sum_{i=0}^{n-1} a_i x^i \in F[x]. \qquad 4.60$$

Returning to our original problem, let X be a F.G. p-module over the P.I.D. J and let X_p be the vector space (over J_p) embedded in X. Let φ be an automorphism of X (and of X_p) as before. The above theorem tells us that X_p can be written as the direct sum of φ-invariant subspaces,

$$X_p = \bigoplus_{j=1}^{k} Xpj \qquad 4.61$$

and for each $X_{p,j}$ there exists a basis $\{f_{j1},\ldots,f_{j-n_j}\}$ with respect to which we have

$$f_{ji} = \varphi^{i-1}(f_{j1}), \tag{4.62}$$

$$\varphi^{n_j}(f_{j1}) = -\sum_{i=0}^{n_j-1} a_i\,\varphi^{i}(f_{j1}), \qquad a_i \in J_p \tag{4.63}$$

and $$q_j(x) = x^{n_j} + \sum_{i=0}^{n_j-1} a_i\,x^{i} = (p(x))^{r_j} \tag{4.64}$$

for some irreducible polynomial $p(x) \in J_p[x]$. Implicit in this is the fact that $q_j(x)$ is the polynomial of least degree such that $q_j(\varphi)\cdot f_{j1} = 0$.

What we would like to do now is extend the basis found above for X_p to a t-basis for X as in proposition 4.8 and next show that if $\{f_{j1},\ldots,f_{jn_j}\}$ is extended to $\{e_{j1},\ldots,e_{jn_j}\}$, then the submodule generated by $\{e_{j1},\ldots,e_{jn_j}\}$ is in fact a φ-invariant direct summand of X. We would also like equations similar to 4.62-4.64 valid for the submodule $\{e_{j1},\ldots,e_{jn_j}\}$.

Unfortunately, we will not be able to guarantee the φ-invariance of the direct summands of X so generated. The exact result is:

<u>Proposition 4.10</u>: Let φ be a automorphism of the F.G. p-module X. Then (i) X can be written as the direct sum $\bigoplus_{j=1}^{k} X_j$ of certain submodules X_j where

(ii) $i < j$ implies: exponent of $X_j \leq$ exponent of X_j; 4.65

(iii) $X_j \simeq (J_{p^{m_j}})^{n_j}$, some m_j, $n_j > 0$, $j = 1,\ldots,k$ 4.66

(iv) each X_j has a t-basis $\{g_{ji}\}_{i=1}^{n_j}$ such that

$$g_{ji} = \varphi^{i-1}\circ g_{j1}, \quad i = 1,\ldots,n_j \tag{4.67}$$

(v) k = the number of φ-invariant subspaces in a rational canonical decomposition of X_p over φ.

(vi) for each $j = 1,\ldots,k$, thene exist polynomials $q_{ji}(x) \in J[x]$ with $\partial^o q_{ji} < n_i$ such that

$$\varphi^{n_j}\circ g_{j1} = \sum_{i=1}^{k} q_{ji}(\varphi)\cdot g_{i1} \tag{4.68}$$

(this follows directly from (i) and (iv) above, since $\varphi^{n_j}\cdot g_{j1} \in X = \bigoplus_{j=1}^{k} X_j$.)

(vii) Finally, for each $j = 1,\ldots,k$, if all the coefficients of $x^{n_j} - q_{jj}(x)$ are reduced modulo p, the result equals a power of some irreducible polynomial $\in J_p[x]$. In particular, the constant term in $q_{jj}(x)$ is nonzero modulo p.

Proof: We start by putting the restriction of φ to X_p in rational canonical form, i.e., we find a basis $\{f_{ji}\}_{j=1,\ i=1}^{k \quad n_j}$ for X_p so that equations 4.61-4.64 are satisfied. We extend this basis to a t-basis $\{e_{ji}\}_{j=1,\ i=1}^{k \quad n_j}$ for X; now relabel the k subspaces as follows: choose any generator e_{st} having maximal exponent m, and observe that $p^{m-1}\ e_{st}$ must be a basis vector f_{ji} in some φ-invariant subspace of X_p. Call this the k^{th} subspace of X_p so that j is replaced by k. Replace s by k, and let $m_k = m$. We then have $p^{m_k-1}\ e_{kt} = f_{ki}$, where e_{kt} is of maximum exponent. Now $f_{ki} = \varphi^r \cdot f_{k1}$ for some r, $0 \leq r < n_k$. Hence $f_{k1} = \varphi^{-r} \cdot f_{ki}$, since φ is an automorphism. Then take

$$g_{k1} = \varphi^{-r} \cdot e_{kt} \qquad 4.69$$

and let

$$g_{ki} = \varphi^{i-1} \cdot g_{k1}, \quad i = 1,\ldots,n_k-1 \qquad 4.70$$

Clearly,

$$\begin{aligned} p^{m_k-1}\ g_{ki} &= \varphi^{i-1} \cdot p^{m_k-1}\ g_{k1} \\ &= \varphi^{i-1-r}\ p^{m_k-1}\ e_{kt} \\ &= \varphi^{i-1-r}\ f_{ki} \\ &= \varphi^{i+1} \cdot f_{k1} \\ &= f_{ki}, \qquad i = 1,\ldots,n_{k-1} \qquad 4.71 \end{aligned}$$

So we now have a set $\{g_{ki}\}_{i=1}^{n_k}$ where

$$q_{ki} = \varphi^{i-1} \cdot g_{k1}, \qquad i = 1, \ldots, n_k,$$

$$p^{m_k - 1} g_{ki} = f_{ki} \qquad i = 1, \ldots, n_k,$$

and $\{f_{ki}\}_{i=1}^{n_k}$ is a basis for a φ-invariant subspace of X_p. Clearly, each g_{ki} is of maximal exponent m_k in X. Let X_k be the submodule of X generated by $\{g_{ki}\}_{i=1}^{n_k}$. We will now show that $\{g_{ki}\}_{i=1}^{n_k}$ is in fact a t-basis for X_k so that X_k is the direct sum of the cyclic submodules generated by the g_{ki}. Since g_{ki} is of maximal exponent m_k, we will have $X_k \simeq (J_{p^{m_k}})^{n_k}$. To show this, suppose that

$$\sum_{i=1}^{n_k} a_i \, g_{ki} = 0, \qquad a_i \in J \qquad 4.72$$

Multiplying by $p^{m_k - 1}$, we obtain $\sum_{i=1}^{n_k} a_i \, f_{ki} = 0$. Since the f_{ki}'s are linearly independent, we must have $a_i \equiv 0 \pmod p$ for $i = 1, \ldots, n_k$, i.e., $a_i = b_i p$ for some b_i. Substituting in 7.37 for the a_i and this time multiplying by $p^{m_k - 2}$, we obtain $\sum_{i=1}^{n_k} b_i \, f_{ki} = 0$. Hence $b_i \equiv 0 \pmod p$, and thus $a_i = c_i p^2$ for some c_i, $i = 1, \ldots, n_k$.

Continuing in this fashion a finite number of times, we conclude that $a_i \equiv 0 \pmod{p^{m_k}}$, $i = 1,\ldots,n_k$. Hence $a_i\, g_{ki} = 0$, $i = 1,\ldots,n_k$. This shows that $\{g_{ki}\}_{i=1}^{n_k}$ is a t-basis for X_k, and hence that $X_k \simeq (J_{p^{m_k}})^{n_k}$.

Since X_k is of maximum possible exponent m_k in X, we know that $X \simeq (\bigoplus_{i=1}^{n} J_{p^{m_i}}) \oplus (J_{p^{m_k}})^s$ for some s, where $m_i < m_k$ for all i. Then $p^{m_k-1}X \sim (J_p)^s$. If $s < n_k$; then $p^{m_k-1} X_k = (J_p)^{n_k} \subseteq (J_p)^s$, which is impossible because $(J_p)^s$ is a vector space and $(J_p)^{m_k}$ a subspace. Therefore $s \geq n_k$, and X_k is a direct summand of X.

Thus we can write $X = Y \oplus X_k$. for some submodule Y of X. Now the embedded vector space in X_k is precisely the φ-invariant subspace of X_p with basis $\{f_{ki}\}_{i=1}^{n_k}$. Clearly, Y must contain the remaining φ-invariant subspaces of X_p. Hence we may proceed by induction and show that $X = \bigoplus_{j=1}^{k} X_j$. This decomposition has been shown to satisfy properties (i)-(v) given in the statement of this theorem.

Because of the relationships amongst the generators $\{g_{ji}\}_{i=1}^{n_j}$ of a submodule X_j as above, any element $x_j \in X_j$ can be written in the form

$$x_j = \sum_{i=0}^{n_j-1} a_i\, \varphi^i \cdot g_{j1} \qquad 4.73$$

$$= q_j(\varphi)\cdot g_{j1} \qquad 4.74$$

where $q_j(x)$ is a polynomial of degree less than n_j (whose coefficients can be considered elements of J). Since $X = \overset{k}{\underset{j=1}{\oplus}} X_j$ any element $x \in X$ can be written in the form

$$x = \sum_{j=1}^{k} q_j(\varphi)\cdot q_{j1}, \qquad \partial^o q_j < n_j \tag{4.75}$$

Consequently, for each j = 1,...,k we can write

$$\varphi^{n_j}\cdot g_{j1} = \sum_{i=1}^{k} q_{ji}(\varphi)\cdot g_{i1}, \qquad \partial^o q_{ji} < n_i \tag{4.76}$$

Note that $\varphi^{n_j}\cdot g_{j1}$ is not restricted to lie in X_j. We do not know at this point if X_j is φ-invariant; however we do know that the vector space embedded in X_j is, by construction, φ-invariant. Thus if we multiply 7.41 by p^{m_j-1} and transpose $q_{jj}(\varphi)\cdot f_{j1}$, we get

$$\varphi^{n_j}\cdot f_{j1} - q_{jj}(\varphi)\cdot f_{j1} = p^{m_j-1} \sum_{\substack{i=1 \\ i\neq j}}^{k} q_{ji}(\varphi)\cdot g_{i1} \tag{4.77}$$

where $(\varphi^{n_j} - q_{jj}(\varphi))\cdot f_{j1} \in X_j$ and the right side is contained in $\underset{i\neq j}{\oplus} X_i$. Hence, because X is a direct sum,

$$[\varphi^{n_j} - q_{jj}(\varphi)]\cdot f_{j1} = 0, \qquad \partial^o q_{jj} < n_j \tag{4.78}$$

Consequently, $\varphi^{n_j} - q_{jj}(\varphi)$ annihilates that φ-invariant vector space over J_p that contains f_{j1}. But we know this space has a unique polynomial $\in J_p[x]$ of degree n_j, which happens to be the power of some irreducible polynomial

$\in J_p[x]$. It follows that when the coefficients of $\varphi^{n_j} - q_{jj}(\varphi)$ are reduced modulo p, the result must be this unique minimal polynomial.

Furthermore if the constant term in $q_{jj}(\varphi)$ were $\equiv 0 \pmod{p}$, then the minimal polynomial would have a constant term of $0 \in J_p$. But this would imply that the polynomial of which it is some power also has a constant term of 0, contradicting its irreducibility. Hence the constant term in $q_{jj}(\varphi)$ is non-zero modulo p (i.e., it is not divisible by p). This completes the proof of all statements in Proposition 4.10. Q.E.D.

<u>Corollary 4.10.1</u> Let φ be an automorphism of the F.G. p-module X. Then a t-basis $\{g_{ji}\}_{j=1}^{k}{}_{,\ i=1}^{n_j}$ can be found for X with respect to which φ has the matrix representation shown below:

$$\left[\begin{array}{ccccccccc}
0 & & & q_{11}^{(0)} & 0 & & & q_{21}^{(0)} & \\
1 & & & q_{11}^{(1)} & 0 & & & q_{21}^{(1)} & \\
 & 1 & & q_{11}^{(2)} & 0 & & & q_{21}^{(2)} & \\
 & & & & & \cdots\cdots & & & \cdots \\
 & & 1 & q_{11}^{(n_1-1)} & 0 & & & q_{21}^{(n_1-1)} & \\
0 & & & q_{12}^{(0)} & 0 & & & q_{22}^{(0)} & \\
0 & & & q_{12}^{(1)} & 1 & & & q_{22}^{(1)} & \\
 & \cdots\cdots & & & & & & & \\
0 & & & q_{12}^{(n_2-1)} & & & 1 & q_{22}^{(n_2-1)} &
\end{array}\right] \qquad 4.79$$

In other words, the matrix is divided into blocks where the diagonal blocks are in companion form and the off-diagonal blocks are zero except for their right-most columns.

<u>Proof</u>: By theorem 4.10, $X = \bigoplus_{j=1}^{k} X_j$ where $X_j \simeq (J_p m_j)^{u_j}$ and each X_j has a t-basis $\{g_{ji}\}_{i=1}^{n_j}$ such that

$$g_{ji} = \varphi^{i-1} g_{j1} \qquad i = 1,\dots,u_j \qquad 4.80$$

We also know that

$$\varphi^{n_j} \cdot g_{j1} = \varphi \cdot g_{jn_j} = \sum_{i=1}^{k} q_{ji}(\varphi) \cdot g_{j1}, \qquad \partial^o q_{ji} < n_i \qquad 4.81$$

Let the coefficient of φ^{ℓ} in $q_{ji}(\varphi)$ be called $q_{ji}^{(2)}$. We can then write

$$\varphi \cdot g_{jn_j} = \sum_{i=1}^{k} \sum_{\ell=0}^{n_i-1} q_{ji}^{(2)} \quad q_{i\ell} \qquad 4.82$$

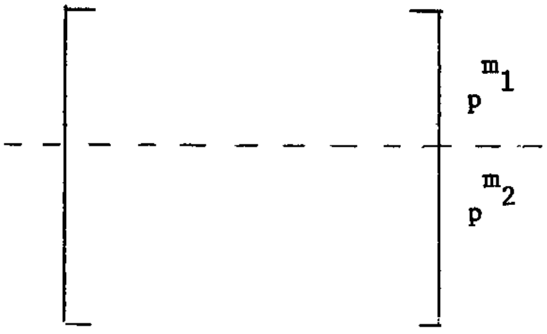
Writing out the effect of φ on each of the t-basis elements:

$$\begin{array}{lll}
\varphi \cdot g_{11} & = & q_{12} \\
\varphi \cdot g_{12} & = & q_{13} \\
\dots & & \dots \\
\varphi \cdot g_{1,n_1-1} & = & g_{1n_1} \qquad 4.83 \\
\varphi \cdot g_{1\,n_1} & = & q_{11}^{(0)} \, g_{11} + q_{11}^{(1)} \, q_{12} + \dots + q_{11}^{(n_1-1)} g_{1\,n\,1} + q_{12}^{(0)} g_{21} + q_{12}^{(1)} g_{22} + \dots \\
\varphi \cdot g_{21} & = & g_{22} \qquad g_{22} \\
\varphi \cdot g_{22} & = & g_{23}
\end{array}$$

If we write each element of x as a column "vector" with components in X_1 at the top and components in X_k at the bottom, we see after a little thought that φ can indeed be represented by a matrix in the form of 4.79.

Q.E.D.

One must be careful in using this matrix, since the various direct summands are not necessarily isomorphic; in particular the period of one block may well be different from that of another. It is well to think of each column of this matrix as a "vector" in X with the top n_1 components describing a "vector" in X_1, where X_1 has period p^{m1}, etc. It may also be helpful to write down beside the matrix the extent and period of each direct summand X_j as shown below:



A matrix in the form 4.79 will be said to be in quasi rational form. Unfortunately, writing a matrix in this form may not always be helpful. In fact it hardly represents a decomposition of X over φ at all, it is not even in block triangular form which would lead to an acceptable cascade machine decomposition, much less is it in block diagonal form which would represent a parallel machine decomposition. The problem is that the blocks X_j (where $X_j \sim (J_{p^{m_j}})^{n_j}$ and $X = \overset{k}{\underset{j=1}{\oplus}} X_j$) are not φ-invariant.

On the other hand, the process that leads to a quasi-rational matrix for φ establishes a t-basis with respect to which φ has a standard simplified form. From the point of view of implementation, the quasi rational form is very simple: the only thing missing is the complete independence (φ-invariance) of the direct summand subsystems. The fact that the quasi rational form consists largely of zeroes is a feature of this simplicity relative to φ's original representation.

Note that if the matrix representing the action of φ on $X_p \subseteq X$ has only one companion block, then the same is true of the matrix representing the action of φ on X. In other words, if X_p is a cyclic $J_p[z]$-module, then X is a cyclic J[z]-module. The converse may not be true, however.

4.3.4. Nilpotent Endomorphisms of F.G. p-Modules

The study of nilpotent endomorphisms of F.G. p-modules appears to be more difficult than that of automorphisms. At least the idea of extending knowledge of φ's operation on the embedded vector space does not seem to carry over to the case where φ is nilpotent.

Furthermore, nilpotent endomorphisms do not occur in the examples considered here. For example, the transformations φ that are used to implement the encoders and decoders discussed in section 4.2.3 are always automorphic. In at least one other situation of interest (to be discussed below), the same is true.

For these reasons, the study of nilpotent endomorphisms of torsion modules will not be pursued here.

4.3.5 Implementation of Torsion Systems

The ease with which an automorphism of a F.G. p-module can be implemented is illustrated below by an example. Let X be an abelian p-group isomrophic to $J_{p^2} \oplus J_{p^2} \oplus J_{p^2} \oplus J_{p^3} \oplus J_{p^3}$, or more compactly, $(J_{p^2})^3 \oplus (J_{p^3})^2$. where J denotes the integers. If φ is an automorphism of X, then Lemma 7.17 tells us that there exists a t-basis for X with respect to which φ can be represented in quasi-rational form (Q.R.F.). One possibility is that φ assume the form

$$\varphi = \begin{array}{c} \left[\begin{array}{ccccc} 0 & 0 & a_0 & 0 & c_0 \\ 1 & 0 & a_1 & 0 & c_1 \\ 0 & 1 & a_2 & 0 & c_2 \\ 0 & 0 & b_0 & 0 & d_0 \\ 0 & 0 & b_1 & 1 & d_1 \end{array}\right] \end{array} \begin{array}{c} \\ p^2 \\ \\ p^3 \\ \\ \end{array} \tag{4.84}$$

Suppose that φ is the state transition matrix (homomorphism) of a F.A.M. with state set X. With 0 input, we can write

$$\begin{bmatrix} x_1(t+1) \\ x_2(t+1) \\ x_3(t+1) \\ x_4(t+1) \\ x_5(t+1) \end{bmatrix} = \begin{bmatrix} 0 & 0 & a_2 & 0 & c_0 \\ 1 & 0 & a_1 & 0 & c_1 \\ 0 & 1 & a_2 & 0 & c_2 \\ 0 & 0 & b_0 & 0 & d_0 \\ 0 & 0 & b_1 & 1 & d_1 \end{bmatrix} \begin{bmatrix} x_1(t) \\ x_2(t) \\ x_3(t) \\ x_4(t) \\ x_5(t) \end{bmatrix} \begin{array}{c} \\ p^2 \\ \\ p^3 \\ \\ \end{array} \tag{4.85}$$

where state components x_1, x_2, x_3 will be contained in "mod p^2 registers" while state components x_4, x_5 will be contained in "mod p^3 registers". A schematic diagram of a circuit that implements this transformation is given below. Note that the circuits are basically shift registers with provision between stages for adding in scalar multiples of the contents of certain other registers.

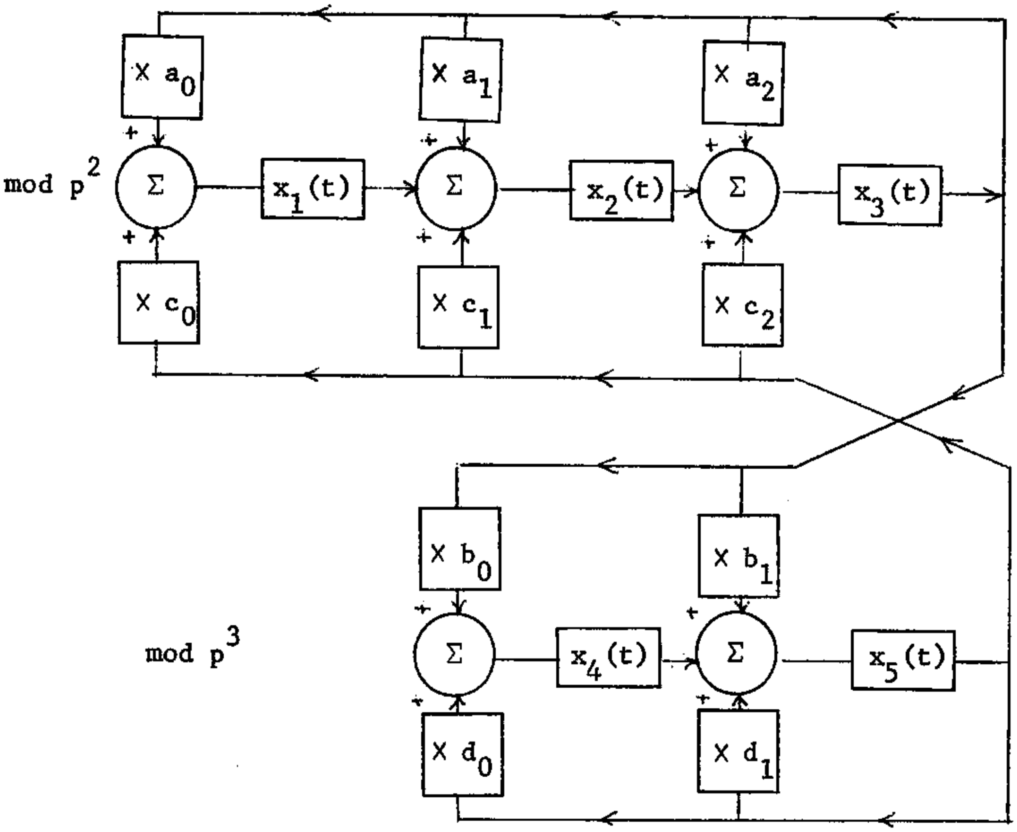


Figure 4.1 - Implementation of a Finite Abelian Machine in Q.R.F.

A potentially simpler implementation may be obtained by performing a similarity transformation on φ. The form of the resulting matrix is the transpose of Q.R.F.. This transformation is obtained as follows.

Consider a diagonal block of a matrix in Q.R.F., and its rightmost column, say $(a_0, a_1, \ldots, a_n)^T$. By the construction of Q.R.F., the polynomial $x^{n+1} + \Sigma\, a_i\, x^i$ yields a power of some irreducible polynomial in $J_p[x]$. This means, in particular, that $a_0 \not\equiv 0$ (mod p), for otherwise 0 would be a root of this polynomial. Hence, if $a_0 \in J_pm$, a_0 must be a unit, and so must be any power of a_0; in other words in any ring of the form J_pm, there exists an element a_0^{-1} such that $a_0a_0-1 = 1$. It follows that the matrix

$$Y = \begin{bmatrix} & & & a_0 & 0 \\ 0 & & a_0 & a_1 & 0 \\ & \cdot\, a_0 & \cdot\, a_1 & \cdot\, a_2 & 0 \\ \cdot^{\cdot^{\cdot}} & \cdot^{\cdot^{\cdot}} & \cdot^{\cdot^{\cdot}} & \vdots & \\ a_0 & a_1 & a_2 & a_{n-1} & 0 \\ 0 & 0 & 0 \;\ldots & 0 & 1 \end{bmatrix} \qquad 4.86$$

is always invertible. Now it can be verified thatif A is a diagonal block of Q.R.F. whose rightmost column is $(a_0, \ldots, a_n)^T$, then it is always true that

$$A\,Y = Y\,A^T \qquad 4.87$$

Since Y is invertible, we have that

$$Y^{-1}A\,Y = A^T \qquad 4.88$$

This is a similarity transformation. If our matrix φ in Q.R.F. has several diagonal blocks, then we can perform the similarity transformation consisting of diagonal blocks, each one of which will transpose a given diagonal block of φ. It is easy to verify that the resulting matrix is in the *form* of Q.R.F. transpose; it is not *equal* to the transpose of φ. However, the diagonal blocks of the result *are* the transpose of the corresponding blocks of φ. This form will be denoted Q.R.F.T.

To exhibit the difference in implementation, suppose

$$\varphi = \begin{array}{c@{\quad}l} \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ a_0 & a_1 & a_2 & e_0 & e_1 \\ 0 & 0 & 0 & 0 & 1 \\ f_0 & f_1 & f_2 & d_0 & d_1 \end{bmatrix} & \begin{array}{l} \\ p^2 \\ \\ \\ p^3 \end{array} \end{array} \qquad 4.89$$

is in Q.R.F.T. With 0 input the dynamic equations are

$$\begin{bmatrix} x_1(t+1) \\ x_2(t+1) \\ x_3(t+1) \\ x_4(t+1) \\ x_5(t+1) \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ a_0 & a_1 & a_2 & e_0 & e_1 \\ 0 & 0 & 0 & 0 & 1 \\ f_0 & f_1 & f_2 & d_0 & d_1 \end{bmatrix} \begin{array}{c@{\quad}l} \begin{bmatrix} x_1(t) \\ x_2(t) \\ x_3(t) \\ x_4(t) \\ x_5(t) \end{bmatrix} & \begin{array}{l} \\ p^2 \\ \\ \\ p^3 \end{array} \end{array} \qquad 4.90$$

A circuit that implements this transformation is:

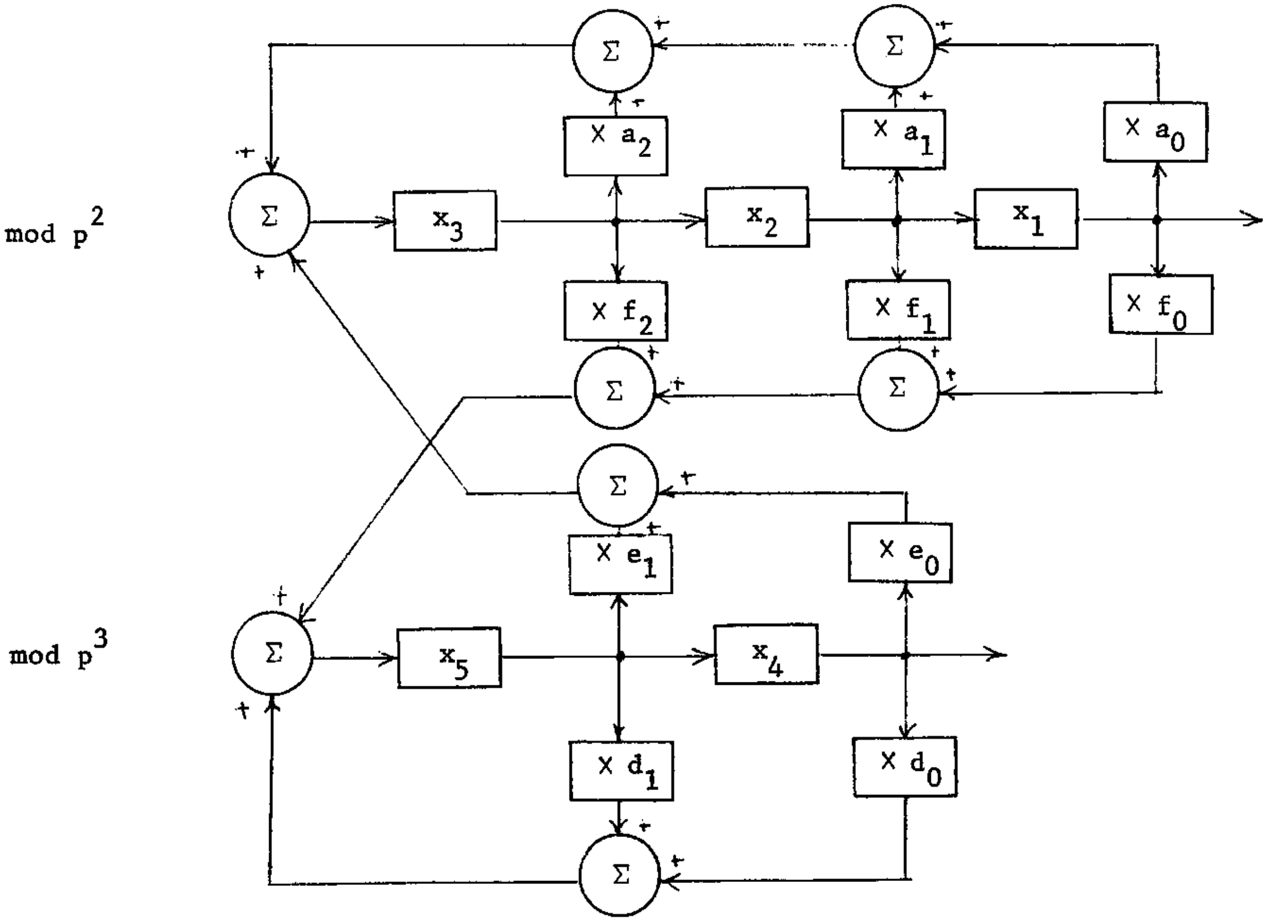


Figure 4.2 - Implementation of a Finite Abelian Machine in Q.R.F.T.

Practically speaking, this machine may be simpler because it can be built with shift registers that have no provision between stages for addition of external values. Note this diagram is only schematic and does not explicitly show how values in mod p^m registers can be multiplied and added to a value in a mod p^m register.

One final point. The reduction of an automorphism φ to Q.R.F. simplifies its matrix representation but requires a "shift of coordinates", i.e., a similarity transformation $\varphi \mapsto Q = Y^{-1} \varphi Y$ to do so. Thus if a finite abelian machine is originally described by

$$\underline{x}_{t+1} = \varphi\cdot\underline{x}_t + \psi\cdot\underline{u}_t \qquad 4.91$$

$$\underline{y}_t = \eta\cdot\underline{x}_t \qquad 4.92$$

and we change coordinates via Y, we obtain a new machine

$$\underline{z}_{t+1} = Q\,\underline{z}_t + Y^{-1}\,\psi\cdot\underline{u}_t \qquad 4.93$$

$$\underline{y}_t = \eta\, Y\cdot\underline{z}_t \qquad 4.94$$

where

$$\underline{z}_t = Y^{-1}\underline{x}_t \qquad 4.95$$

Here Q is in Q.R.F. The point is that by simplifying the state transition matrix φ, we may well have complicated the input and output matrices ψ and η respectively. Consequently it may not always be clear a priori whether reduction to Q.R.F. or Q.R.F.T. actually leads to a more economical implementation.

In summary, an attempt has been made to simplify the representation of an automorphism operating on a F.G. torsion module X over a P.I.D. J. It has also been shown that if φ is any endomorphism of X, then X is the direct sum of a submodule X_a where φ's action is automorphic and a submodule X_n where φ's action is nilpotent. The nilpotent part has not been considered here.

4.4. Examples

4.4.1. A Single-error-correcting Code Over J_3m

Problem: (1) with p = 3, construct a code capable of correcting any error value in any single digit position. Minimize the block length, so that this error correction capability will have maximum effect (note: there is no need to specify the m of J_3m).

(2) give a schematic diagram of the encoder and syndrome calculator after simplifying their dynamics:

(3) illustrate the error-correction procedure by example.

Solution: (1) the first step is to settle on the block length n, i.e., the degree of d of the extension we will be using. To correct a single position, we need $r = d+1$ check digits. However in any local extension of J_pm of degree d, we have at most p^d-1 useful powers of a P-primitive element, and the block length n must be greater than r. Here we are trying to minimize the block length, so we want the smallest d such that $p^d-1 > d+1$. Clearly, if p = 3, d must be greater than 1. However d = 2 will do, since $3^2-1 > 3$.

Thus we can work over $J_3m[x]/<x^2 + 1>$, which is a local extension of degree 2 (since $x^2 + 1$ is irreducible over J_3). Hence we will have d + 1 = 3 check digits. The shortest block length we can have is therefore n = 4. This will give us a single information digit.

The second step is to find a P-primitive element θ of $R = J_3m[x]/<x^2+1>$. This is done by first finding a primitive element ω of $F = J_3[x]/<x^2+1>$, and choosing θ so that $[\theta]p = \omega$, where P is the maximal ideal of R. To find the primitive element ω all we need do is consider the $(p^2-1)^{th} = (3^2-1)^{th} =$ 8^{th} cyclotomic polynomial $f_8(x)$ whose roots are precisely the primitive elements of $F = GF(3^2)$. Now $f_8(x) = x^4 + 1$, and we must find one of its roots in F. If we let i denote a root of $x^2 + 1$ in $F \mp J_3[x]/\langle x^2+1\rangle$, we will be looking for a root of $f_8(x)$ in the form $a_0 + a_1 i$, where $a_0, a_1 \in J_3$. A little calculation shows that $(1 - i)$ is a root of $f_8(x)$ in F, and hence $\omega = (1 - i)$ is a primitive element of F. The column vector representation of ω is $[1, -1]^T$. Clearly, a representative θ for ω in R is $[1, -1]^T$.

The third step is to explicitly give the parity-check matrix H, which will be a 3 X 4 matrix over $J_p m$. To do this, we construct the operator representation H of θ. We recall that if $\underline{\theta} = [1, -1]^T$, then

$$H = \begin{bmatrix} \underline{\theta}, & \varphi\underline{\theta} \end{bmatrix} \qquad 4.96$$

where

$$\varphi = \begin{bmatrix} 0 & -q_0 \\ 1 & -q_1 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \qquad 4.97$$

where $q(x) = x^2 + q_1x + q_0 = x^2 + 1$ and $R = J_p m[x]/\langle q(x)\rangle$. Thus

$$H = \begin{bmatrix} \begin{matrix} 1 \\ -1 \end{matrix} & \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \qquad 4.98$$

In this case, the 3 X 4 parity check matrix H is given by

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ \textcircled{H}^3\underline{1} & \textcircled{H}^2\underline{1} & \textcircled{H}\underline{1} & \underline{1} \end{bmatrix} \qquad 4.99$$

where $\underline{1} = [1, 0]^T$. Hence

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & -1 & 0 \end{bmatrix} \qquad 4.100$$

Note that if we let

$$\Phi = \begin{bmatrix} 1 & 0 & 0 \\ 0 & & \\ 0 & \textcircled{H} & \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & -1 & 1 \end{bmatrix} \qquad 4.101$$

and $\underline{b} = [1, 1, 0]^T$, 4.102

we can then write

$$H = \begin{bmatrix} \Phi^3\underline{b}, & \Phi^2\underline{b}, & \Phi\underline{b}, \ b \end{bmatrix} \qquad 4.103$$

To explicitly calculate the check digits $[c_1, c_2, c_3]^T$ based on the single information digit u, we can form the equation H $[u, c_1, c_2, c_3]^T = 0$; using 4,103, this yields:

$$H_2 \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & -1 & 0 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = - \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} u \qquad 4.104$$

The next step is to invert the matrix H_2 (being careful to perform operations mod p^m, not mod p !). It turns out that

$$H_2^{-1} = \begin{bmatrix} 1 & -1 & 0 \\ 1 & -1 & -1 \\ -1 & 2 & 1 \end{bmatrix} \qquad 4.105$$

Hence,
$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = - \begin{bmatrix} 1 & -1 & 0 \\ 1 & -1 & -1 \\ -1 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} u = \begin{bmatrix} 0 \\ 1 \\ -2 \end{bmatrix} u \qquad 4.106$$

part (2): according to 4.106, the encoder is trivial and need not involve any dynamics at all. A diagram is given below (the check digits c_i are contained in a shift register).

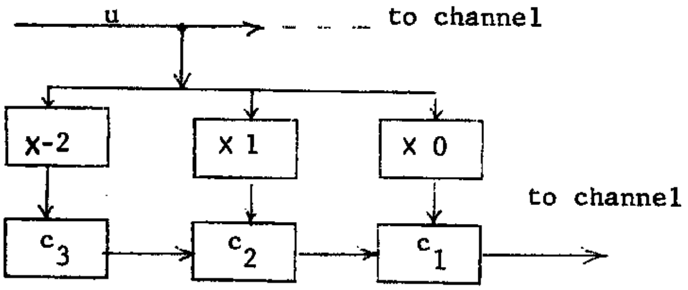


Figure 4.3 Encoder for single-error-correcting code

According to 4.103, the syndrome calculator can be implemented by the system

$$\underline{s}_{t+1} = \Phi \, \underline{s}_t + \underline{b} \, u_t, \quad \underline{s}_0 = \underline{0} \qquad 4.107$$

where $\underline{s}_t \in X = (J_3m)^3$ and Φ, $\underline{b}$ are given by 4.101 and 4.102. The problem now is to simplify Φ by putting Φ in quasi-rational form (Q.R.F.) by an appropriate similarity transformation. Note that Φ is already in block diagonal form, where the upper block is trivial. So we only have to simplify the lower block $\textcircled{H}$.

To do this, we must investigate the operation of H on the embedded vector space of $(J_3m)^2$. A step in this direction is to obtain the characteristic polynomial of $\textcircled{H}$ when its coeffients are reduced mod p = 3:

$$\det\,(xI - \textcircled{H}) = \det\begin{bmatrix} x-1 & -1 \\ 1 & x-1 \end{bmatrix} = (x-1)^2 + 1 = x^2-2x + 2$$

It easily verified that this polynomial is irreducible over J_3. Consequently, H has only one block in its rational canonical form. It follows that H has only one block in its quasi-rational form over J_3m, namely

$$\textcircled{H}' = \begin{bmatrix} 0 & -2 \\ 1 & +2 \end{bmatrix} \qquad 4.108$$

We must now find a similarity transformation A such that $A^{-1}\textcircled{H}A = \textcircled{H}'$; the basic method of doing this in the vector space case is explained in books on linear algebra. The reader can verify that if we choose

$$A = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix},\quad A^{-1} = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} \qquad 4.109$$

then

$$A^{-1}\,\textcircled{H}\,A = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & -2 \\ 1 & +2 \end{bmatrix} = \textcircled{H}' \qquad 4.110$$

From 4.110 we have $\textcircled{H} = A\,\textcircled{H}'\,A^{-1}$. From 4.101 we obtain

$$\Phi = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \multicolumn{2}{c}{A\;H'\;A^{-1}} \\ 0 & & \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \multicolumn{2}{c}{A} \\ 0 & & \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & \multicolumn{2}{c}{\textcircled{H}'} \\ 0 & & \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & \multicolumn{2}{c}{A^{-1}} \\ 0 & & \end{bmatrix}$$

Substituting this in 4.107 and performing the transformation

$$\underline{x}_t = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \multicolumn{2}{c}{A^{-1}} \\ 0 & & \end{bmatrix}\underline{s}_t \qquad 4.111$$

we get

$$\underline{x}_{t+1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & 1 & +2 \end{bmatrix} \underline{x}_t + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} u_t$$

and

$$\underline{s}_t = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & -1 \end{bmatrix} \underline{x}_t ,$$

or

$$\underline{x}_{t+1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & 1 & +2 \end{bmatrix} \underline{x}_t + \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} u_t \qquad 4.112$$

and

$$\underline{s}_t = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & -1 \end{bmatrix} \underline{x}_t$$

Equations 4.112 and 4.113 are the dynamic equations in Q.R.F. for the syndrome calculator. Writing out equations 4.112 and 4.113 in terms of components:

$$\begin{aligned} x_1(t+1) &= x_1(t) + u_t \\ x_2(t+1) &= -2x_3(t) + u_t \\ x_3(t+1) &= x_2(t) + 2x_3(t) \end{aligned}$$

$$\begin{aligned} s_1(t) &= x_1(t) \\ s_2(t) &= x_2(t) + x_3(t) \\ s_3(t) &= -x_3(t). \end{aligned}$$

The circuit corresponding to these equations is:

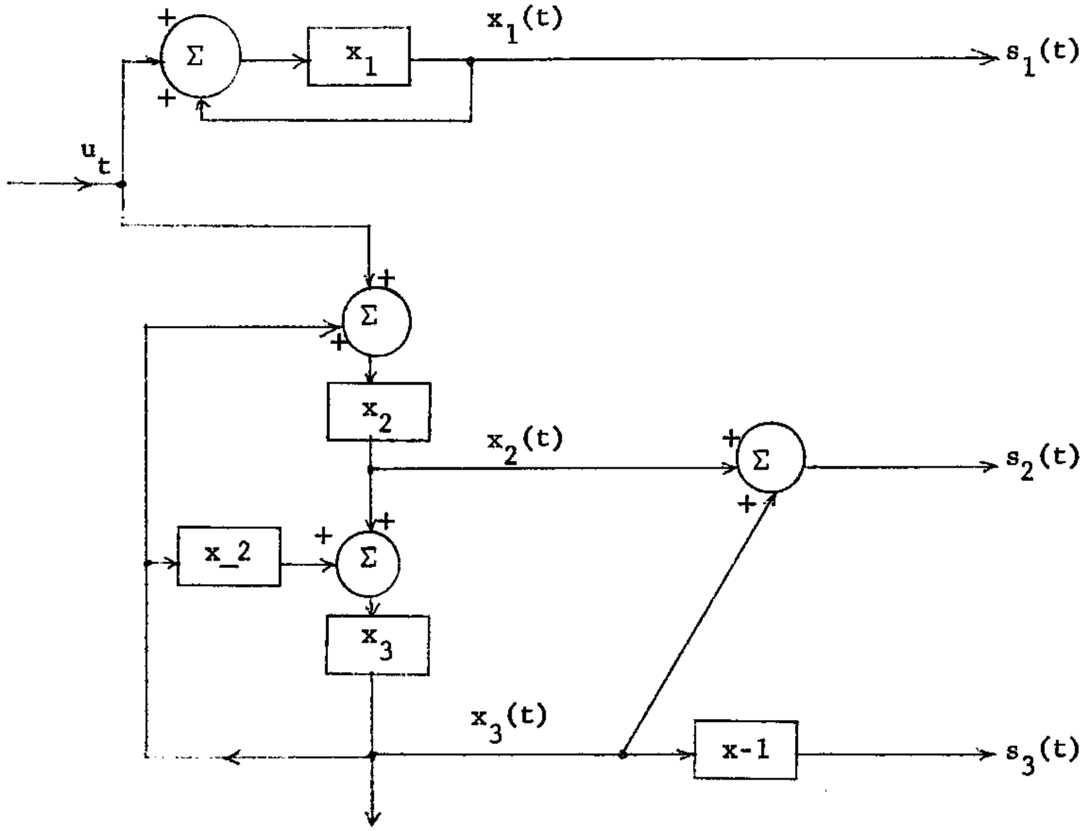


Figure 4.4. Syndrome Calculator; Single-error Example

This completes the first example of an error-correcting code over J_{p^m} where p = 3 in this case. Note that the entire procedure is independent of the value of m.

4.4.2. Double-error-correcting codes over J_n, and n.

The possibility of constructing error-correcting codes over p^m allows us to construct error-correcting codes over the integers modulo q, where q is any integer. The idea of course is to factor q into its prime-power factors, say $q = p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k}$. By the Chinese Remainder Theorem, we know that J_q is ring-isomorphic to $J_{p_1^{m_1}} \oplus J_{p_2^{m_2}} \oplus \cdots \oplus J_{p_k^{m_k}}$.

We can now construct appropriate codes over each of these direct factors, each code having the same block length n. To illustrate, suppose a code over J_q, $q = 675 = 3^3 \cdot 5^2$, is required that corrects any two errors a_1, a_2 as long as $a_1\ a_2 \not\equiv 0 \bmod 3^3$ and $a_1\ a_2 \not\equiv 0 \bmod 5^2$. We can obtain a code of block length $n = 8 = 3^2 - 1 \leq 5^2 - 1$ with local extensions of degree $d = 2$. This will require $r = 3d + 1 = 7$ check digits. Again, we get only one information digit in this example.

It turns that $q(x) = x^2 - x + 2$ is irreducible over J_3 and over J_5. Thus $R_1 = J_3 3[x]/\langle q(x)\rangle$ and $R_2 = J_5 2[x]/\langle q(x)\rangle$ are both local extensions of degree 2. We chose a polynomial that was "irreducible over both J_3 and J_5" for convenience; not out of necessity. (As usual, considerable care may have to be exercised to keep track of the ring or module under discussion).

The next step is to find primitive elements of $F_1 = J_3[x]/\langle x^2\text{-}x\text{+}2\rangle$ and of $F_2 = J_5[x]/\langle x^2\text{-}x\text{+}2\rangle$. It turns out that $\omega_1 = [1, -1]^T$ is a primitive element of F_1; this can be verified by showing that ω_1 is a root of the cyclotomic polynomial $f_2 3(x) = x^4 + 1$ in $J_3[x]/\langle x^2\text{-}x\text{+}2\rangle$. We can then take as our P-primitive element $\underline{\theta}_1 = [1, -1]^T \in R_1$. The operator representation $\textcircled{H}_1$ for θ_1 is

$$\textcircled{H}_1 = \left[\underline{\theta}_1 \ , \ \begin{bmatrix} 0 & -2 \\ 1 & 1 \end{bmatrix} \theta_1 \right] = \left[\begin{bmatrix} 1 \\ -1 \end{bmatrix} , \ \begin{bmatrix} 0 & -2 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right]$$

so

$$\textcircled{H}_1 = \begin{bmatrix} 1 & 2 \\ -1 & 0 \end{bmatrix} \qquad 4.114$$

We must now find a primitive root ω_2 of F_2, i.e. a root of the cyclotomic polynomial $f_{24}(x) = f_{23.3}(x) = f_{2.3}(x^4)$. Now, $f_{2.3}(x^4) = f_3(-x^4)$

$$\begin{aligned} &= (-x^4)^2 + (-x^4) + 1 \\ &= x^8 - x^4 + 1 \end{aligned}$$

(The cyclotomic polynomials were calculated according to Lang [1971, p. 206]). After a search for a root of this polynomial, we obtain $\omega_2 = [0, 1]^T \in F_2$ for example. We can then take as our P-primitive element $\underline{\theta}_2 = [0, 1]^T \in R_2$. The operator representation $\textcircled{H}_2$ for θ_2 is

$$\textcircled{H}_2 = \left[\underline{\theta}_2 , \begin{bmatrix} 0 & -2 \\ 1 & 1 \end{bmatrix} \underline{\theta}_2 \right] = \left[\begin{matrix} 0 \\ 1 \end{matrix} , \begin{bmatrix} 0 & -2 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right]$$

so

$$H_2 = \begin{bmatrix} 0 & -2 \\ 1 & 1 \end{bmatrix} \tag{4.115}$$

The 7 x 8 parity-check matrix H_1 for the $J_3 3$ part is:

$$H_1 = \begin{bmatrix} 1 & & 1 & 1 \\ \textcircled{H}_1^{7}\underline{1} & & \textcircled{H}_1\underline{1} & \underline{1} \\ (\textcircled{H}_1^{7})^2\underline{1} & \cdots & \textcircled{H}_1^{2}\underline{1} & \underline{1} \\ (\textcircled{H}_1^{7})^3\underline{1} & & \textcircled{H}_1^{3}\underline{1} & \underline{1} \end{bmatrix} \tag{4.116}$$

The 7 x 8 parity-check matrix H_2 for the $J_5 2$ part is:

$$H_2 = \begin{bmatrix} 1 & & 1 & 1 \\ \textcircled{H}_2^{7}\underline{1} & & \textcircled{H}_2\underline{1} & \underline{1} \\ (\textcircled{H}_2^{7})^2\underline{1} & \cdots & \textcircled{H}_2^{2}\underline{1} & \underline{1} \\ (\textcircled{H}_2^{7})^3\underline{1} & & \textcircled{H}_2^{3}\underline{1} & \underline{1} \end{bmatrix}$$

The implementation proceeds as follows. A single information digit $u \in J_{3^3 . 5^2}$ is presented to the system. One circuit calculates $[u]_{3}3$, the class of u mod 3^3. The digit $[u]_{3}3 \in J_{3}3$ is then presented to a circuit which calculates the 7 check digits $\in J_{3}3$ according to H_1. Another circuit which calculates the 7 check digits $\in J_{5}2$ according to H_2. The two sets of 7 check digits can then be combined to form a sequence of 7 check digits $\in J_{3^3 . 5^2}$ preparatory to transmission.

Similarly, the decoder will first split a received sequence of 8 digits $\in J_{3^3 . 5^2}$ into two sequences of 8 digits, one consisting of digits $\in J_{5}2$. These two sequences would be decoded according to the general ideas of section 4.2.2, and then combined to give the decoders best estimate of the transmitted message.

This discussion is only an outline, so as not to obscure the simple ideas involved and thus to suggest the plausibility of constructing error-correcting codes over J_n, n = any integer.

5. CHAIN CONDITIONS AND DECOMPOSITION

5.1 Introduction: Machine Decompositions

The main result of this chapter provides a "cascade" decomposition of an R[z]-module X satisfying A.C.C. over R (i.e., every R-submodule of X is F.G.). This result can be viewed both (i) as a strictly algebraic result concerning the decomposition of a module over an endomorphism and (ii) as a system-theoretic method of decomposing a linear machine into some interconnection of "simpler" machines. Increasingly more detailed results are obtained as further conditions are imposed on R or X.

For details regarding the notions of cascade, serial, and parallel machine decompositions, see Hartmanis, J., and Stearns, R. [1], Arbib, M. [15], and Kalman, R., Falb, P., and Arbib, M. [10]. Roughly speaking, however, a parallel decomposition of a machine corresponds to a decomposition of the state set into "direct summand machines," each "summand" operating independently of the others; i.e., the next state of a direct summand machine depends only on the input and its own current state. The current state of the original machine can be reconstructed by some functions of the current states of the component machines. For linear systems over R, this means decomposing the state module into a direct sum of R[z] modules.

A cascade decomposition of a machine, however, corresponds to a simulation of the original machine by simpler machines that do not necessarily operate independently. In particular, the component machines are to be thought of as arranged in a chain, where the next state of a given machine may depend not only on the input and its own current state, but also on the current state of the machine preceeding it in the chain. Intuitively, it should seem reasonable that a serial decomposition can be achieved under conditions weaker than those for a parallel decomposition, since the feature of complete independence is lost. To show that this is the case is one of the objectives of this chapter.

The basic decomposition of a F.D.L.T.I. system over R with R satisfying A.C.C. will be achieved by embedding the state module X in a direct product of "simpler" R-modules where the action of z is more easily described. In other words, X will be viewed as a sub-direct product.

Outline of this Chapter

Section 5.2 discusses certain basic features of decomposing a linear system Σ into simpler linear systems. The idea is to first find submodules P and Q of the state module X such that $P \cap Q = (0)$. Subsequently, X is embedded in $X/P \oplus X/Q$, and a new system Σ' is constructed with this state set. The input/output properties of Σ and Σ' are to be identical.

The problem is thus to find P, Q (where $P \cap Q = (0)$) that lead to simplifications in the description of Σ'. Section 5.2 suggests particular choices for P and Q.

Section 5.3 establishes that when the state module satisfies A.C.C., then the program suggested in 5.2 can be repeatedly carried out so long as the next state endomorphism of a component machine is neither injective nor nilpotent. Specifically we have

Theorem: Let Σ be a D.L.T.I. system over a ring R, where Σ's state module X satisfies A.C.C.. If φ, the next-state endomorphism of Σ is neither injective nor nilpotent, then a finite cascade Σ' of linear systems can be found with the same input/output properties as Σ. The next-state endomorphism of the head machine is injective, while the next state endomorphisms of other systems in the cascade are equal to 0 (i.e., the other machines are "resets").

The practicality of this decomposition is severely limited by the need to find explicit formulas for reconstructing the original state from a subdirect product. On the other hand, the decomposition provides a conceptual canonic form for all linear systems whose state sets satisfy A.C.C.

Section 5.5 imposes the descending chain condition on the state module in addition to A.C.C. An immediate result is Corollary to Theorem (above): Under the same conditions as in the above theorem and if X also satisfies D.C.C., then the next-state endomorphism of the head machine is an automorphism.

This result is interesting because it suggests a connection with the decomposition of a finite automaton into "permutation" and "reset" components.

However, the main interest in requiring A.C.C. and D.C.C. is that Jordan-Holder and Krull-Schmidt theories apply to the state module. The precise result appears as corollary 5.6.1 below, but is stated here as well:

Theorem: Let $\Sigma = (\varphi\colon X \to X, \varphi, \eta)$ be a D.L.T.I. system over R, where X satisfies both chain conditions. Then Σ can be expressed uniquely (in the Krull-Schmidt sense) as a parallel connection of D.L.T I. whose next-state endomorphisms are either automorphic or nilpotent.

This theorem is given a categorical interpretation in terms of factoring certain diagrams. In any case, the theorem provides a certain uniqueness to the "finest" possible parallel decompositon that can be applied to a linear system. It also provides the form for the next-state endomorphisms of these "finest possible" parallel components.

Section 5.6 then requires that the state module X be semisimple (in the sense of Lang, S. [12]). This implies that X satisfies both chain conditions. The decomposition results obtained here are the most important in this chapter. They are

Theorem: Let $\Sigma = (\varphi, \psi, \eta)$ be a D.L.T.I. system over R whose state module is semisimple. Let

$$\Sigma = \Sigma_1 \oplus \cdots \oplus \Sigma_n$$

be a parallel decomposition of Σ into indecomposable component systems $\Sigma_i = (\varphi_i, \psi_i, \eta_i)$ with state modules X_i, i = 1, ..., n. Then X_i is the (finite) direct sum of isomorphic simple modules, and φ_i is either nilpotent or automorphic, i = 1, ..., n.

Theorem: Let $\Sigma = (\varphi, \eta, \psi)$ be an indecomposable system in the above decomposition, where φ is nilpotent. Then

$$X = \bigoplus_{j=0}^{k-1} <\varphi^j(g)> \text{, some } g \in X;$$

here $<\varphi^j(g)>$ denotes the (cyclic) R-submodule of X generated by $\varphi^j(g)$. (Thus X, viewed as a R[z]-module is cyclic. Furthermore, the action of φ an X can be represented by a nilpotent companion matrix of order k).

Theorem: Let $\Sigma = (\varphi, \eta, \psi)$ be an indecomposable component system in the above decomposition, where φ is an automorphism.

(1) If X, viewed as an R[z]-module is cyclic, then

$$X = \bigoplus_{j=0}^{k-1} <\varphi^j(g)>, \text{ some } g \in X.$$

(Thus the action of φ can be represented by an invertible companion matrix of order k).

(2) In general, φ can be represented by a block triangular matrix whose diagonal blocks are invertible and in companion form. (This leads to a unique, irreducible cascade decomposition for Σ).

5.2. General Requirements for Cascade Decompositions

The systems discussed here are those describable by

$$x_{t+1} = \varphi(x_t) + \psi(u_t) \qquad 5.1$$

where x_t, $x_{t+1} \in X$, $u_t \in U$; X and U are both F.G. R-modules, and φ: $X \to X$, ψ: $U \to X$ are both R-homomorphisms. It will be convenient to define

$$v_t = \psi(u_t). \qquad 5.2$$

<u>Proposition 5.1.</u> Let P and Q be two submodules of an R-module X. Suppose $P \cap Q = (0)$.

If $x \equiv_p y$ and $x \equiv_q y$, then $x = y$.

($x \equiv_p y$ means that $x - y \in P$).

<u>Proof.</u> clear.

This trivial proposition turns out to be most important to the process of finding cascade decompositions. The crucial implication is that if a coset of P and a coset of Q overlap (i.e. have a non-empty intersection), then there is a unique element $x \in X$ in that intersection. Hence, if we formed the direct sum $Y = X/P \oplus X/Q$, we could define a function

$$f: Y \to X \cup \{\phi\} \qquad \text{by}$$
$$f: ([x]_p, [y]_q) \mapsto [x]_p \cap [y]_q$$

Furthermore, if we let T be the subset of $Y = X/P \oplus X/Q$ such that $([x]_p, [y]_q \in T$ iff $[x]_p \cap [y]_q \neq \phi$, we see that $f|_T$ (the restriction of f to T) is a well-defined function $f|_T: T \to X$. In fact, T is a submodule of Y which is isomorphic to X; we say that T is a subdirect product isomorphic to X, or that X can be embedded in the direct sum $X/P \oplus X/Q$. We will denote the inverse of $f|_T$ by f^{-1}.

Suppose that P and Q are two R-submodules in the state module X of the linear system 5.1. such that $P \cap Q = (0)$. Consider the possibility of "simulating" that system by two "smaller" systems with state modules X/P and X/Q respectively. The above arguments are meant to suggest that in certain situations we can reconstruct the current state in X given the current states in two systems with state modules X/P and X/Q by means of the function $f|_T$. In order to do this, we must require that if s_t is the current state in X, then $[x_t]_p$ and $[x_t]_q$ are the current states in X/P and X/Q respectively. Hence we insist that the (yet to be found) dynamics of the quotient machines have the following property: if $[x_t]_p$ and $[x_t]_q$ are the current states in the quotient systems, then the next states must be $[x_{t+1}]_p$ and $[x_{t+1}]_q$ respectively, where x_{t+1} is given by equation 5.1. Thus, the next states in X/P and X/Q must somehow satisfy

$$[x_{t+1}]_p = [\varphi(x_t)]_p + [v_t]_p \,, \qquad 5.3$$

and

$$[x_{t+1}]_q = [\varphi(x_t)]_q + [v_t]_q \,. \qquad 5.4$$

The problem now is to find $[\varphi(x_t)]_p$ and $[\varphi(x_t)]_q$ using only information given by the current states in X/P and X/Q.

Definition 5.1. Let γ_p and γ_q denote the canonical surjections

$$\gamma_p : X \to X/P$$

and

$$\gamma_q : X \to X/Q.$$

Now, using the fact that $([x_t]_p, [x_t]_q) \in T$, we can rewrite 4.3 and 4.4 as follows:

$$[x_{t+1}]_p = \gamma_p \cdot \varphi \cdot f|_T ([x_t]_p, [x_t]_q) + \gamma_p(v_t), \qquad 5.5$$

and

$$[x_{t+1}]_q = \gamma_q \cdot \varphi \cdot f|_T ([x_t]_p, [x_t]_q) + \gamma_q (v_t) \qquad 5.6$$

We can now view X/P and X/Q, along with the dynamic equations 5.5 and 5.6 as two coupled dynamic systems. These two systems can simulate the original system in the sense that they contain enough information to calculate the motion of x_t.

The next step is to find a more explicit form for $f|_T ([x_t]_p, [x_t]_q)$, or perhaps for $\varphi \cdot f|_T ([x_t]_p, [x_t]_q)$. It would be convenient, of course, to be able to write

$$f|_T ([x]_p, [y]_q) = \alpha_p ([x]_p) + \alpha_q ([y]_q) \qquad 5.7$$

where $\alpha_p : X/P \to X$ and $\alpha_q : X/Q \to X$ are R-homomorphisms. Unfortunately, this is not possible unless $X = P \oplus Q$:

Proposition 5.2. Let P, Q be two submodules of X such that $P \cap Q = (0)$. There exists two R-homomorphisms

$$\alpha_p : X/P \to X \tag{5.8}$$

and

$$\alpha_q : X/Q \to X \tag{5.9}$$

such that

$$\alpha_p([x]_p) + \alpha_q([y]_q) = [x]_p \cap [y]_q \tag{5.10}$$

it and only if, $X = P \oplus Q$.

Proof: $\Leftarrow$: if $X = P \oplus Q$, then $X/P \simeq Q$ and $X/Q \simeq P$. In this case, α_p and α_q are just the canonical injections. $\Rightarrow$: If α_p and α_q are as in 5.8 and 5.9 then $\forall$ x, y, $\alpha_p([x]_p) + \alpha_q([y]_q) \in X$. If equation 4.10 is satisfied, we have that $[x]_p \cap [y]_q \in X$, for all x,y. In other words, every pair of cosets $[x]_p$, $[y]_q$ has a non-empty intersection. Since this intersection is unique, we have that $X = P \oplus Q$. Q.E.D.

So it is not always possible to write $f|_T$ in the form 5.7. On the other hand, if $X = P \oplus Q$, equations 5.5, 5.6 become

$$[x_{t+1}]_p = \gamma_p \cdot \varphi \cdot \alpha_p([x_t]_p) + \gamma_p \cdot \varphi \cdot \alpha_q([x_t]_q) + \gamma_p(v_t), \tag{5.11}$$

and

$$[x_{t+1}]_q = \gamma_q \cdot \varphi \cdot \alpha_p([x_t]_p) + \gamma_q \cdot \varphi \cdot \alpha_q([x_t]_q) + \gamma_q(v_t). \tag{5.12}$$

More compactly, they become:

$$[x_{t+1}]_p = \alpha_{pp}([x_t]_p) + \alpha_{pq}([x_t]_q) + \gamma_p(v_t) \tag{5.13}$$

and

$$[x_{t+1}]_q = \alpha_{qp}([x_t]_p) + \gamma_{qq}([x_t]_q) + \gamma_q(v_t). \tag{5.14}$$

For example, if X is a vector space over F, then for any convenient subspace P of X, we can always find another subspace Q such that $X = Q \oplus Q$. Hence we can always decompose a linear system over a field F into two coupled systems as in 5.13 and 5.14, and continue this process until each state space is one-dimensional.

Returning to the general case, we can exercise some of our options in choosing P and Q. It would seem reasonable to try

$$P = \ker \varphi = \{x \in X \mid \varphi(x) = 0\}.$$

The effect of this choice is important: the next state in X/P no longer depends on the current state in X/Q. Not only that, the next state in X/Q no longer depends on its own current states. Thus, choosing $P = \ker \varphi$, $P \cap Q = (0)$ effects a partial decoupling of the quotient systems. This can be illustrated by the diagram

$$\begin{tikzcd}
X/Q & \\
X \arrow[u, "\gamma_q"] \arrow[r, "\text{(onto)}", "\varphi"'] \arrow[d, "\gamma_p"'] & \operatorname{im} \varphi \subseteq X \\
X/\ker \varphi \arrow[ur, "\beta\ (1\text{-}1,\ \text{onto})"'] &
\end{tikzcd}$$

Figure 5.1.

The point here is that the <u>next</u> state in X can be determined by knowledge of the current state in X/ ker φ (and the input), because

$$\varphi(x_t) = \beta \cdot \gamma_p(x_t) = \beta([x_t]_p).$$

In terms of the above notation,

$$\varphi \cdot f|_T([x_t]_{\ker \varphi}, [x_t]_q) = \beta([x_t]_p) \qquad 5.15$$

The previous dynamic equations become (with P = ker φ):

$$[x_{t+1}]_p = \gamma_p \cdot \beta([x_t]_p) + \gamma_p(v_t) \qquad 5.16$$

and

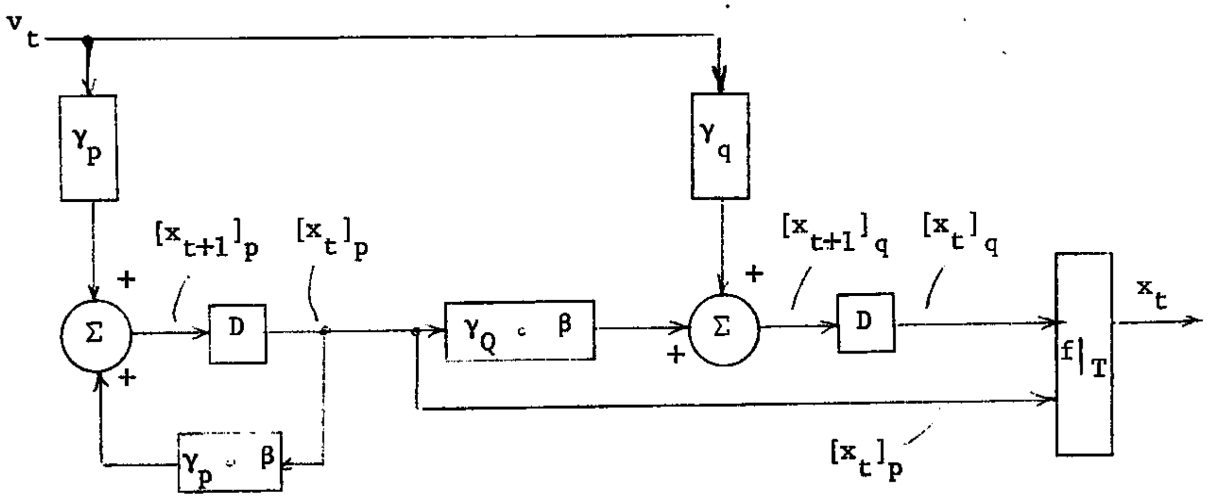
$$[x_{t+1}]_q = \gamma_q \cdot \beta([x_t]_p) + \gamma_q(v_t) \qquad 5.17$$

Note that the current state in X/Q is irrelevant to determining the next states in both X/P and X/Q. A machine diagram of the decomposition is given in Figure 5.2, where the boxes marked D represent "delay elements" with unit delay; they merely indicate the separation of events by one unit of time in the intended interpretation.

The machine with state module X/ker φ is known as the head machine; its next state is independent of the current states of other machines. The machine with state module X/Q is known as a tail machine. It should be emphasized here that the tail machine's next state is independent of its current state; in the language of finite-state machine theory, this tail machine would be called a <u>reset</u> machine. In the language of linear system theory, the action of Z on X/Q is nilpotent of index 1, i.e., is the zero endomorphism. In any case, the original linear system described by 5.1 has been decomposed into a cascade connection of the two machines described by 5.16 and 5.17 under the assumption that a submodule $Q \subsetneq X$ could be found such that ker $\varphi \cap Q = (0)$.

Clearly, if φ is injective, this approach cannot be used. However, if φ is not injective and ker $\varphi \neq (0)$, we must find Q such that ker $\varphi \cap Q = (0)$. So one question is: when does such a Q exist? Another question is: how

Figure 5.2: One Step in Cascade Decomposition



$$[x_{t+1}]_p = \gamma_p \circ \phi'([x_t]_p) + \gamma_p(v_t)$$

$$[x_{t+1}]_q = \gamma_q \circ \phi'([x_t]_p) + \gamma_q(v_t).$$

Boxes marked D are "unit delays"

far can this cascade decomposition process be carried out in successive head machines?

5.3 A.C.C. and Cascade Decomposition

Proposition 5.3. Let φ be an endomorphism of the R-module X where X satisfies A.C.C. Assume $\ker \varphi \neq (0)$. Then either there exists a non-zero submodule Q such that $\ker \varphi \cap Q = (0)$, or else there exists an integer $n > 0$ such that $\varphi^n(X) = (0)$.

Proof. Let (φ^k) denote $\ker \varphi^k = \{x \in X \mid \varphi^k(x) = 0\}$. Clearly, $(\varphi) \subseteq (\varphi^2) \subseteq \ldots$ is an ascending chain of submodules of X. By A.C.C., there exists a (least) integer n such that $(\varphi^n) = (\varphi^{n+1}) = \ldots.$ Consider $\operatorname{im} \varphi^n = \varphi^n(X)$.

Claim: $(\varphi^n) \cap \operatorname{im} \varphi^n = (0)$. Proof of claim: $x \in (\varphi^n) \cap \varphi^n(X) \Rightarrow \varphi^n(x) = 0$ and $x = \varphi^n(y)$, some $y \in X$. But then $\varphi^{2n}(y) = 0$, i.e., $y \in (\varphi^{2n})$. But $(\varphi^n) = (\varphi^{n+1}) = \ldots = (\varphi^{2n}) = \ldots.$ Hence $y \in (\varphi^n)$, so that $\varphi^n(y) = 0$. Thus $x = \varphi^n(y) = 0$ Q.E.D.

However, $\ker \varphi = (\varphi) \subseteq (\varphi^n)$, and $\varphi^n(X) \cap (\varphi^n) = (0)$; therefore, $\ker \varphi \cap \varphi^n(X) = (0)$. Thus we can take $Q = \varphi^n(X)$, unless $\varphi^n(X) = (0)$. Q.E.D.

The above proposition tells us that we can continue the cascade decomposition until the endomorphism of the head machine is either injective or nilpotent. In any case, the first step in decomposing X over φ yields a head machine with state module $X/\ker \varphi$ and with next-state endomorphism $\gamma_p \cdot \beta$. Since $\varphi = \beta \cdot \gamma_p$ and β is an isomorphism,

$$\gamma_p = \beta^{-1} \varphi,$$

and

$$\gamma_p \cdot \beta = \beta^{-1} \varphi\, \beta. \qquad 5.18$$

In other words, the action of $\gamma_p \cdot \beta$ on $X/\ker \varphi$ is <u>similar</u> to the action of φ on $\varphi(X)$: they are related by the similarity transformation β. Hence

$$\begin{aligned} x \in \ker \gamma_p \cdot \beta &\Leftrightarrow x \in \ker \beta^{-1}\varphi\beta \\ &\Leftrightarrow \beta^{-1}\varphi\beta(x) = 0 \\ &\Leftrightarrow \varphi\beta(x) = 0 \\ &\Leftrightarrow \beta(x) \in \ker \varphi \\ &\Leftrightarrow x \in \beta^{-1}(\ker \varphi) \end{aligned}$$

Since the domain of β^{-1} is $\varphi(X)$, we can also write

$$x \in \ker \gamma_p \cdot \beta \Leftrightarrow x \in \beta^{-1}(\ker \varphi \cap \varphi(X))$$

Hence,

$$\ker \gamma_p \cdot \beta = \beta^{-1}(\ker \varphi \cap \varphi(X))$$

Thus,

$$\begin{aligned} (X/\ker \varphi)/\ker \gamma_p \cdot \beta &\simeq \varphi(X)/(\ker \varphi \cap \varphi(X)) \\ &\simeq X/\ker \varphi^2, \end{aligned} \qquad 5.19$$

as is easy to demonstrate.

The next step in the decomposition of $(X/\ker \varphi)$ requires us to find a submodule Q of $(X/\ker \varphi)$ such that $Q \cap \ker \gamma_p \cdot \beta = (0)$. Hence we must find a submodule Q' of $\varphi(X)$ such that $Q' \cap (\ker \varphi \cap \varphi(X)) = (0)$. It is easy to show that we can take $Q' = \varphi^n(X) \subseteq \varphi(X)$. Hence

$$\begin{aligned} \varphi(X)/Q' &\simeq \varphi(X)/\varphi^n(X) \\ &\simeq X/\varphi^{n-1}(X) \end{aligned} \qquad 5.20$$

We have now decomposed the original machine into a cascade of three machines: the first or head machine has state set $X/\ker \varphi^2$; the next has state set $X/\varphi^{n-1}(X)$, and the third has state set $X/\varphi^n(X)$. This can be indicated schematically by

$$X/\ker \varphi^2 \to X/\varphi^{n-1}(X) \to X/\varphi^n(X).$$

Figure 5.2.

Clearly, this process can only be carried until the head machine has state module $X/\ker \varphi^n$, for then the action of φ induced on this module is injective and therefore has kernel = (0), and the decomposition process stops. The overall result is:

<u>Proposition 5.4.</u> Let $\Sigma = (\varphi:X \to X, \psi:U \to X, \eta:X \to Y)$ be a D.L.T.I. system over R, and let X satisfy A.C.C. over R.

Then Σ can be simulated (i.e., f_Σ can be realized) by a cascade connection of D.L.T.I. systems over R where the next state endomorphism of the head machine is injective, and all other machines are reset machines. The state modules appearing in the decomposition are arranged in the sequence

$$X/\ker \varphi^n \to X/\varphi(X) \to X/\varphi^2(X) \to \dots \to X/\varphi^n(X)$$

where n is the least integer such that $\ker \varphi^n = \ker \varphi^{n+1} = \dots$; If φ is injective or nilpotent, no decomposition can be carried out. Each step in the decomposition embeds the state module of the head machine in a direct product of two other modules; to obtain a practical decomposition, explicit formulas for the inverse of this embedding must be found.

5.4. Discussion

The difficulty with the above decomposition is finding formulas for the inverse embeddings. The problem arose because this decomposition is based on ideas from finite-state machine theory, where these inverse maps can always be calculated explicitly. Proposition 5.2. states that the inverse map is a homomorphism if, and only if, $X = P \oplus Q$. In general, this will not be the case; thus, a practical decomposition in the above form will not always be possible.

On the other hand, the decomposition gives some theoretical insight into the operation of a large class of linear systems. Perhaps more importantly, the technique can be used as a starting point for investigating systems with more detailed structure. Furthermore, the technique can always be used in the situation where X is finite.

5.5. The Descending Chain Condition and Decomposition

Definition 5.2. An R-module X is said to satisfy the descending chain condition iff every descending chain of submodules

$$M_0 \supset M_1 \supset \dots \supset M_i \supset \dots$$

is finite, i.e., there exists an integer $k \geq 0$ such that

$$M_k = M_{k+1} = \dots.$$

A ring R satisfies D.C.C. iff it satisfies D.C.C. as a (left) module over itself.

The class of modules satisfying D.C.C. indlude finite modules, vector spaces, and semisimple modules (which are discussed below). It is easy to show that if X satisfies D.C.C., then so does every submodule and homomorphic image of X.

Proposition 5.5. Let X be an R-module satisfying both chain conditions. Let $\varphi: X \to X$ be an R-endomorphism. If φ is either injective or surjective, φ is an automorphism.

Proof. see Jacobson, N. [11], p. 154.

Corollary 5.5.1. Let $\Sigma = (\varphi: X \to X, \psi: U \to X, \eta: X \to Y)$ be a D.L.T.I. system over R, and let X satisfy both chain conditions. Let Σ be decomposed as in proposition 5.4. Then the next-state endomorphism of the resulting head machine is in fact an automorphism.

Proof. by the facts that this endomorphism is injective and the head machine's state module satisfies both chain conditions, and by proposition 5.5.

This last result only serves to solidify the connection between the above decomposition and the decomposition of finite state machines into permutation and reset machines. However, more powerful decomposition results can be obtained:

Proposition 5.6. Let X be an R-module satisfying both chain conditions, and let $\varphi: X \to X$ be an R-endomorphism.

Then X can be expressed as the direct sum of φ-invariant submodules X_i, $i = 1, \ldots, s$ where the action of φ on X_i is either automorphic or nilpotent. This decomposition is unique in the sense specified by the Krull-Schmidt theorem (see Jacobson, N. [11]. pp. 156-158).

Furthermore, these modules X_i are indecomposable in the sense that X_i cannot be expressed as a direct sum of (non-zero) φ-invariant submodules.

Proof. view X as an R[z]-module, with the action of z defined by the action of φ. Since X satisfies A.C.C. and D.C.C. as an R-module, it certainly satisfies A.C.C. and D.C.C. as an R[z]-module. By the Krull-Schmidt theorem, X can be expressed "uniquely" as the direct sum of indecomposable R[z]-modules X_i, $i = 1, \ldots, s$. The fact that X_i is an R[z]-module means that X_i is φ-invariant.

The fact that X_i is indecomposable over R[z] means that X_i cannot be expressed as the direct sum of two (non-zero) φ-invariant submodules. Let Q_i denote the restriction of φ to X_i. It can be shown that if φ_i is neither nilpotent nor automorphic, then X_i is the direct sum of $\ker \varphi_i{}^n$ and $\varphi_i{}^n(X_i)$ where n is the least integer such that $\ker \varphi_i{}^n = \ker \varphi_i{}^{n+1} = \ldots$; for a proof, see Jacobson, N. [11], p.155-156. Hence, if X_i is indecomposable, φ_i must be either automorphic or nilpotent. Q.E.D.

Corollary 5.6.1. Let $\Sigma = (\varphi:X \to X, \psi:U \to X, \eta:X \to Y)$ be a D.L.T.I. system over R, where X satisfies both chain conditions. Then Σ can be expressed uniquely (in the Krull-Schmidt sense) as a "parallel" connection of D.L.T.I. systems whose next state endomorphisms are either automorphic or nilpotent.

Proof. follows directly from proposition 4.6 by defining the parallel connection of two D.L.T.I. systems

$$\Sigma_1 = (\varphi_1:X_1 \to X_1, \psi_1:U \to X_1, \eta_1:X_1 \to Y)$$

and

$$\Sigma_2 = (\varphi_2 : X_2 \to X_2,\ \psi_2 : U \to X_2,\ \eta_2 : X_2 \to Y)$$

to be the D L.T.I. system

$$\begin{aligned}\Sigma_1 \oplus \Sigma_2 = [(\varphi_1,\varphi_2) &: X_1 \oplus X_2 \to X_1 \oplus X_2 : (x_1,x_2) \mapsto (\varphi(x_1), \varphi(x_2))\\ (\psi_1,\psi_2) &: U \to X_1 \oplus X_2 : u_t \mapsto (\psi_1(u), \psi_2(u))\\ (\eta_1,\eta_2) &: X_1 \oplus X_2 \to Y : (x_1,x_2) \mapsto \eta_1(x_1) + \eta_2(x_2)]\end{aligned}$$

A parallel decomposition into two systems corresponds to factoring the diagram

$$U \xrightarrow{\psi} X \xrightarrow{\varphi} X \xrightarrow{\eta} Y$$

as

$$\begin{tikzcd}
 & X_1 \arrow[r, "\varphi_1"] & X_1 \arrow[dr, "\eta_1"] & \\
U \arrow[ur, "\psi_1"] \arrow[dr, "\psi_2"'] & & & \Sigma \\
 & X_2 \arrow[r, "\varphi_2"'] & X_2 \arrow[ur, "\eta_2"'] &
\end{tikzcd}$$

where $X = X_1 \oplus X_2$.

The main effect of this theorem is to provide the "finest" possible parallel decomposition of a linear system. Further decomposition must proceed by different techniques; in particular, any further decomposition will probably be in a strictly cascade form.

5.6. Semisimplicity: Introduction

The decomposition of corollary 4.6.1 can be carried further if the R-module to be considered here is one in which every submodule can be viewed as a direct summand. Such modules are called semisimple. A ring is said to be semisimple if it is semisimple as a (left) module over itself. Examples of semisimple modules are vector spaces, group algebras, and any module which is the direct sum of a family of simple submodules. The group algebra case is of particular interest and will be discussed later.

Details concerning semisimple modules can be found in Lang, S., [12], chapter 18, Herstein, I.N. [14], and van der Waerden, B L. [17], chapter 13.

Definition 5.3. A unitary R-module X is said to be semisimple iff X is the sum of a finite number of simple submodules.

Proposition 5.7. Let X be a unitary R-module.

(i) X is semisimple iff X is the direct sum of a finite number of simple submodules

(ii) X is semisimple iff every submodule F of X is a direct summand, i.e., $X = F \oplus E$ for some submodule E.

(iii) if X is semisimple, every submodule and homomorphic image of X is also semisimple.

(iv) if X is semisimple, X satisfies both A.C C. and D.C.C.

Proof. (i) - (iii): see Lang, S. [12], p. 442.

(iv): if X is semisimple, X is the direct sum of a finite number of simple submodules. It is easy to show that a unitary simple module is cyclic so that X is F.G. over R. By (iii), every submodule of a semisimple module X is a direct summand of X, and must therefore be a homomorphic image of X. Every homomorphic image of an F.G. R-module is also F.G., so every submodule of X is F.G. Thus X satisfies A.C.C.

To show that if X is semisimple then X satisfies D.C.C., assume the contrary. Let $X_0 \supset X_1 \supset X_2$ .... be an infinite descending sequence of submodules in the semisimple module X, ordered by proper inclusion. Since every $X_i \subset X$ is also semisimple, we can find $Y_i \neq (0)$ such that

$$X_i = Y_i \oplus X_{i+1}, \quad \forall_i \geq 0.$$

$Y_i \neq (0)$ because the inclusion $X_{i+1} \subset X_i$ is proper. Hence

$$(y_0) \subset (Y_0, Y_1) \subset (Y_0, Y_1, Y_2) \subset \dots.$$

is an infinite properly ascending sequence of submodules. This contradicts A.C.C. Hence, no infinite properly descending sequence of submodules can exist in a semisimple module X; i.e., X satisfies D.C.C. as well. Q.E.D.

Thus, if Σ is a D.L.T I. system over R whose state module is semisimple, the decomposition of corollary 4.6.1 applies. The next step is to analyze the action of automorphisms and nilpotent endomorphisms φ on semisimple modules. We only have to consider modules that are indecomposable in that they cannot be expressed as the direct product of φ-invariant submodules.

Proposition 5.8. Let φ be an endomorphism of the semisimple R-module X. If X is indecomposable over R[z], X is the direct sum of isomorphic simple R-modules.

Proof. Suppose not all of the simple direct summands of X are isomorphic. Let X_1 be one of the simple direct summands and let $Y = \overset{r}{\underset{i=1}{\oplus}} X_i$ be the direct sum of all summands isomorphic to X_1. Consider $\varphi(X_1)$. Since X_1 is simple, either $\varphi(X_1) = 0$ or $\varphi(X_1) \simeq X_1$, and $\varphi(X_1)$ is also simple. If $\varphi(X_1) = 0$,

$\varphi(X_1) \subseteq Y$. Now suppose $\varphi(X_1) \neq 0$. Since $\varphi(X_1)$ is simple, $Y \cap \varphi(X_1) = 0$ or $\varphi(X_1)$. If $Y \cap \varphi(X_1) = \varphi(X_1)$, $\varphi(X_1) \subseteq Y$. Suppose $Y \cap \varphi(X_1) = 0$. Then X can be expressed as $X = Y \oplus \varphi(X_1) \oplus Z$, for some module Z

$$= \left(\bigoplus_{i=1}^{r} X_i \right) \oplus \varphi(X_1) \oplus Z.$$

However, in this decomposition there are r + 1 direct summands isomorphic to X_1.

Now each direct summand of X, being simple, is indecomposable as an R-module. By the Krull-Schmidt theorem, these indecomposable direct summands are unique in number and are uniquely specified up to isomorphism. It is therefore impossible that X has two decompositions into indecomposable submodules, where one decomposition has exactly r simple modules isomorphic to X, and the other has exactly r + 1 simple modules isomorphic to X_1. Thus $\varphi(X_1) \subseteq Y$. Since this is true for every direct summand of Y,

$$\varphi(Y) \subseteq Y.$$

Thus, if φ is an endomorphism of the semisimple module X, every submodule Y consisting of the direct sum of all isomorphic simple direct summands of X is φ-invariant. Hence, if the simple direct summands of X are not isomorphic to each other, X is decomposable over R[z]; that is, X is the direct product of two (non-zero) φ-invariant submodules. Q.E.D.

<u>Corollary 5.8.1.</u> Let $\Sigma = (\varphi, \psi, \eta)$ be a D.L.T.I. system over R whose state module X is semisimple. Let

$$\Sigma = \Sigma_1 \oplus \Sigma_2 \oplus \cdots \oplus \Sigma_n$$

be a parallel decomposition of Σ into indecomposable components $\Sigma_i = (\varphi_i, \psi_i,$

η_i) with state module X_i, i = 1, ..., n. Then X_i is the (finite) direct sum of isomorphic simple modules, and φ_i is either nilpotent or automorphic, i = 1, ... n.

Proof. follows from corollary 4.6.1 and proposition 4.8.

Proposition 5.9. Let X be a semisimple R-module, and let $\varphi: X \to X$ be a nilpotent endomorphism of index k.

If X is indecomposable over R[z]. then

$$X = \bigoplus_{i=0}^{k-1} < \varphi^{i} \cdot g >$$

where g is some element of X, and $< \varphi \cdot^{i} g >$ denotes the cyclic R-submodule of X generated by $\varphi^{i}(g)$. (These cyclic direct summands are isomorphic because of indecomposability).

Proof. (i) Since φ is nilpotent of index k, there exists a $g \in X$ such that $\varphi^{k-1}_{\cdot} \neq 0$. Let M be the submodule generated by $\{g, \varphi \cdot g, \ldots, \varphi^{k-1}_{\cdot} g\}$.
Claim: $M = \bigoplus_{i=0}^{k-1} < \varphi^{i}_{\cdot} g >$.

Proof of claim: suppose

$$\sum_{i=0}^{k-1} r_i \varphi^{i} \cdot g = 0. \qquad 5.21$$

Operating on this equation by φ^{k-1} yields

$$r_0 \varphi^{k-1}_{\cdot} g = \varphi^{k-1}(r_0 g) = 0.$$

Hence, $r_0 g \in$ kernel of (φ^{k-1} restricted to $<g>$). It is easy to show that, because X is semisimple, any cyclic submodule is simple (and conversely); consequently, $<g>$ is simple. Thus,

$$\text{kernel of } (\varphi^{k-1} \text{ restricted to } <g>) = 0;$$

otherwise would contradict fact that $\varphi^{k-1} g \neq 0$. Hence $r_0 g = 0$. Then, equation 5.21 can be rewritten

$$\sum_{i=1}^{k-1} r_i \varphi^i \cdot g = 0 \qquad 5.22$$

Operating on this last equation with φ^{k-2} yields

$$r_1 \varphi^{k-1} \cdot g = 0.$$

By the same argument as above, $r_1 g = 0$.

Repeating this process enough times will yield that $r_i g = 0$, and hence that $r_i \varphi^i \cdot g = 0$, $i = 0, 1, \ldots k-1$. We have proved that

$$\sum_{i=0}^{k-1} r_i \varphi^i \cdot g = 0 \Rightarrow r_i \varphi^i \cdot g = 0, \quad 0 \leq i < k.$$

Thus every element of M can be expressed uniquely as a sum of elements from $<\varphi^i \cdot g>$, $0 \leq i < k$. Hence

$$M = \bigoplus_{i=0}^{k-1} <\varphi^i \cdot g> \qquad \text{Q.E.D. Claim.}$$

So, if φ is nilpotent of index k, there exists a submodule $M = \bigoplus_{i=0}^{k-1} <\varphi^i \cdot g>$, for some $g \in X$ such that $\varphi^{k-1} \cdot g \neq 0$.

(ii) The next step is to show that if X is indecomposable over R[z], then in fact $M = X$. This proof is carried out for the vector space case in Finkbeiner, D.T. [18], pp. 146-148, but applies equally well to nilpotent endomorphisms of semisimple modules. The actual statement there is that there exists a φ-invariant module N of X such that $X = M \oplus N$. This contradicts indecomposability unless $N = 0$, in which case $M = X$. Q.E.D.

The matrix interpretation of this theorem is that, under the conditions specified, a set of independent generators can be found for X with respect to which the representation of φ is

$$\begin{bmatrix} 0 & & & & 0 \\ 1 & & & & 0 \\ & 1 & & & 0 \\ & & \cdots & & \\ & & & 1 & 0 \end{bmatrix}$$

A linear system having a next-state endomorphism in this form is simply a shift register with no feedback.

<u>Proposition 5.10.</u> Let X be a semisimple R-module cyclic over $R[z]$, where the action of z is given by an automorphism φ. Then $X = \bigoplus_{i=0}^{k-1} <\varphi^{i} \cdot g>$, some $g \in X$; all direct summands are isomorphic to each other and any minimum degree monic annihilator $g(z)$ of g has degree k.

<u>Proof.</u> Let g be a generator of X over $R[z]$, and let $X_i = <\varphi^i \cdot g>$, $i \geq 0$. Hence $X_{i+1} = \varphi(X_i)$, $i \geq 0$. Since $X_0 = <g>$ is cyclic, X_0 is simple. Since φ is an automorphism, X_i is also simple, for all i. Hence, $X_0 \cap X_1 = (0)$ or X_1. If $X_0 \cap X_1 = X_1$, then $X_1 \subseteq X_o$, in which case $zg \cdot \in X_0$ and $X = X_0$. If

$X_0 \cap X_1 = (0)$, let $Y_1 = X_0 \oplus X_1$ and consider X_2. Again, X_2 is simple, so $Y_1 \cap X_2 = (0)$ or X_2. Continue in this way until the least value k is found such that

$$X_k \subseteq \bigoplus_{i=0}^{k-1} X_i .$$

Then, clearly, $X = \bigoplus_{i=0}^{k-1} X_i = \bigoplus_{i=0}^{k-1} <\varphi^i \cdot g>$. Furthermore, by the method of construction, $\varphi^m g \notin \sum_{i=0}^{m-1} <\varphi^i \cdot g>$ for any $m < k$. Hence every minimum degree monic annihilator of g has degree k. The summands are all isomorphic to each other since φ is an automorphism. Q.E.D.

The matrix interpretation of this theorem is that, under the conditions specified, a set of independent generators can be found for X with respect to which a representation of φ is

$$\begin{bmatrix} 0 & & & & -r_0 \\ 1 & & & & -r_1 \\ & 1 & & & -r_2 \\ & & \cdots & & \\ & & & 1 & -r_{k-1} \end{bmatrix} \qquad 5.24$$

A linear system having a next-state endomorphism in this form is simply a shift register with feedback from the "last" component. This theorem is restricted to the case where X is cyclic over R[z]; this situation occurs, for example, when the input module of a linear system over R is cyclic. In this case, all R[z]-indecomposable factors of X are also cyclic since they are homomorphic images of X. Thus, if the input module is cyclic (i.e., a "single-input" system), the system can be decomposed into a parallel connection of systems whose next-state endomorphisms can be represented by either 5.23 or 5.24. By the Krull-Schmidt theorem, if these systems are indecomposable, they are unique in a certain sense.

If X is not cyclic over R[z] and the action of z is automorphic, the situation seems considerably more complicated. In the vector space case, a component of X which is indecomposable over R[z] must be cyclic; this may not be so here. The problem seems to be that we do not have unique factorization in R[z] and that X is not necessarily a free R-module. Hence, without further information about decomposability, it is necessary to look for different kinds of state-module reductions.

In particular, a cascade decomposition can always be achieved whose components are unique in a sense specified by the Jordan-Holder theorem. This is proved below.

Proposition 5.11. Let X be a semisimple R-module which is indecomposable over R[z], where the action of z on X is given by an automorphism φ. Then an independent set of generators for X can be found with respect to which φ can be represented by a block triangular matrix. The diagonal blocks are invertible and in companion form (5.24).

Proof. The fact that X is indecomposable over R[z] simply implies that X is the direct sum of simple R-submodules that are isomorphic to each other (by proposition 5.8).

Since X satisfies both chain conditions as an R-module, X certainly satisfies both chain conditions as an R[z]-module. The Jordan-Holder theorem then states that X has a composition series of R[z]-submodules

$$X = X_0 \supset X_1 \supset X_2 \supset \cdots \supset X_t \supset X_{t+1} = (0) \qquad 5.25$$

whose factors X_i/X_{i+1} are simple R[z]-modules; the theorem states that any other composition series for X will have exactly these factors (in some order).

Assume that 5.25 is a composition series of R[z]-submodules for our original module X. Since X_t is simple over R[z], it is necessarily cyclic. Since X is semisimple, we can find an R-submodule Y_t such that $X = X_t \oplus Y_t$. Since X_t is an R[z]-submodule, it is closed under the action of φ. However Y_t will not be φ-invariant if X is indecomposable over R[z]. Suppose $X_t \simeq S^{n_1}$ and $Y_t \simeq S^{n_2}$ where S is the simple R-module component of X. Then the action of φ on X can be represented by a matrix of the form

$$\begin{array}{c|cc|c} & n_1 & n_2 & \\ n_1 & \varphi_{11} & \varphi_{12} & X_t \\ \hline n_2 & 0 & \varphi_{22} & Y_t \end{array}$$

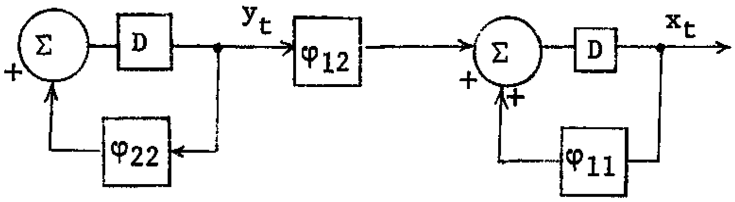
where φ_{11} describes the action of φ on X_t, and φ_{12}, φ_{22} together describe the action of φ on Y_t. Since φ is an automorphism, it follows that both φ_{11} and φ_{22} are invertible. Since X_t is cyclic over R[z], it follows that φ_{11} can be put in the form 5.24 (companion form).

This procedure can now be repeated by considering the action of the automorphism φ_{22}: $Y_t \rightarrow Y_t$; this is equivalent to decomposing the R[z]-

module X/X_t. Eventually, the representation of φ will be in (upper) block triangular form whose diagonal blocks are invertible and in companion form as required.

Q.E.D.

The decomposition given by 4.26 has an interesting system-theoretic interpretation. If φ is the next-state endomorphism of a linear system Σ satisfying the conditions specified, Σ is equivalent to a cascade of two machines Σ_1, Σ_2:



One-step Decomposition of Semisimple System

Figure 5.3

This concludes the preliminary decomposition theory for linear systems whose state modules are semisimple. The potential applications and extentions of this theory will be discussed in chapters 6 and 7, respectively.

6. APPLICATIONS AND EXAMPLES

6.1. Introduction

This chapter introduces some applications of the theory developed so far and formulates some interesting systems to be eventually analyzed by this theory.

Section 6.2 presents an alternate proof of the Rouchaleau-Kalman-Wyman realizability result for Noetherian domains. This follows almost trivially from proposition 3.14, which states that: if R is a Noetherian domain, $f: R^m[z] \to R^p[[z^{-1}]]$ is realizable over R if, and only if, $A(X_f) \neq (0)$, where $X_f = R^m[z]/\ker f$ and $A(X_f) \subseteq R[z]$ is the annihilating ideal of X_f.

Section 6.3 considers the problem of digitally implementing a system with a given transfer function over Q, where Q is the field of quotients of some unique factorization domain. Section 6.4 considers the problem of decomposing a linear system over a unique factorization domain.

Section 6.5 interprets realization theory over a P.I.D. in the context of a partial difference system. Finally, section 6.6 considers a potentially important type of semisimple system.

6.2. Alternate Proof of the Rouchaleau-Kalman-Wyman Result on Realizability over Noetherian Domains

Theorem: Let R be a Noetherian integral domain, and let K be R's field of quotients. Let $f: R^m[z] \to R^p[[z^{-1}]]$ be a linear input/output map over R.

Then, f is realizable over R if, and only if, f is realizable over K.

Proof. $\Rightarrow$: if f is realizable over R, then since R is embedded in K, f is *a forteriori* realizable over K.

$\Leftarrow$: Assume f is realizable over K. This says that f's Hankel sequence $H = \{H_j \in R^{p\times m} \mid j \geq 1\}$ can be constructed as $H_j = \eta \cdot \varphi^{j-1} \cdot \psi, \forall_j \geq 1$, where $\varphi \in K^{n\times n}$, $\psi \in K^{n\times m}$, and $\eta \in K^{p\times n}$; here, $K^{s\times t}$ denotes the set of $s \times t$ matrices over K.

Since f is realizable over K, H posses a monic annihilator $q(z) \in K[z]$. Now we can multiply q(z) by some $r \in R$ to eliminate the denominators of the coefficients in q(z); the result is that $rq(z) \in R[z]$. Clearly, $rq(z) \in R[z]$ is a non-zero annihilator of H. Thus, $A(X_f) = A(R^m[z]/\ker f) \neq 0$. By proposition 3.14, f is then realizable over R. Q.E.D.

6.3. Example for R = Unique Factorization Domain

Suppose that from frequency response considerations we are required to implement a single input-single output filter with z-transform (transfer function)

$$W(z) = p(z)/q(z)$$

where $p(z), q(z) \in Q[z]$, Q = the rational numbers, and $\partial^o p < \partial^o q$. The filter is to be implemented on a digital computer, and as a first approximation, we will assume that computations are to be performed with integers only. In other words, to avoid problems with multiple precision and arithmetic underflow, we will want to perform all calculations using integer arithmetic. The inputs to the filter are to be discretized and represented as integers. The outputs are to be integers as well.

Clearly, this is possible if and only if $W(z) = p(z)/q(z) \in J[[z^{-1}]]$, where J = the integers. The question is then, "what conditions on p and q are necessary and sufficient to have $p(z)/q(z) \in J[[z^{-1}]]$?" It is certainly sufficient to require that $p(z) \in J[z]$ and $q(z) =$ monic $\in J[z]$. However this is also necessary, as will be shown below. The point is that unless these criteria are satisfied, then there is no way to exactly implement $W(z)$ using integer arithmetic alone.

Claim: if $p(z)$, $q(z)$ are polynomials $\in Q[z](\partial^o p < \partial^o q$ and $q(z)$ monic) with no common factors and such that $p(z)/q(z) \in J[[z^{-1}]]$, then $p(z)$ and $q(z)$ are both elements of $J[z]$.

Proof. Suppose $p(z)/q(z) \in J[[z^{-1}]]$, where $p(z)$ and $q(z)$ have no common factor. Then $q(z)$ is an annihilator of least degree for $p(z)/q(z)$. Let $r \in J$ be such that $rq(z) \in J[z]$. Now the annihilating ideal of $p(z)/q(z)$ $\in J[z]$ is principal and generated by a monic polynomial $a(z)$ (Rouchaleau, Y. [7], p. 30, shows that this ideal is principal ($J[z]$ is a U.F.D.); the ideal contains some monic polynomial because the sequence is realizable over Q and hence over J: this monic polynomial is a multiple of the ideal's generator, which must therefore be monic itself). Hence, $rq(z) \in <a(z)>$; $a(z)$ cannot be of lower degree than $q(z)$, for $q(z)$ is an annihilator of minimum degree over Q, and hence over J. Thus, $rq(z) = ka(z)$, some $k \in J$. Since $q(z)$ is monic, $r = k$, and hence $a(z) = q(z)$. In other words, $q(z)$ is a monic-polynomial in $J[z]$, as required.

To show that $p(z) \in J[z]$, consider applying the sequence $q(z) \in R[z]$ as input to a system with transfer function $p(z)/q(z) \in J[[z^{-1}]]$. By a previous theorem,

$$q(z) \chi -p(z)/q(z) = p(z).$$

Consequently, $p(z)$ is the output sequence occurring during the time that $q(z)$ is applied. Since the output at every instant of time is to be an integer, it follows that $p(z) \in J[z]$. Q.E.D.

6.4. Restricted Decomposition over a U.F.D.

Under certain restricted conditions, we can obtain a direct sum decomposition of the canonic system associated with a linear input/output map over a U.F.D. Let R be U.F.D., and let $f\colon R[z] \to R^p[[z^{-1}]]$ be an input/output map over R, with $X_f = R[z]/\ker f$. Then X_f is cyclic over $R[z]$, generated by g, say, and $X_f \simeq R[z]/A(g)$. If R is Noetherian and f is realizable, we know that $A(g) = \langle q(z) \rangle$, for some monic $q(z) \in R[z]$. Since $R[z]$ is also a U.F.D., we can write

$$q(z) = p_1^{e_1}(z) \cdot \ldots \cdot p_k^{e_k}(z),$$

where the $p_i(z)$ are distinct irreducible (prime) elements in $R[z]$, $i = 1, \ldots, k$. It is easy to show that

$$\langle q(z) \rangle = \bigcap_{i=1}^{k} \langle p_i^{e_i}(z) \rangle;$$

this is a primary decomposition of $\langle q(z) \rangle$. Since R is also integrally closed the $p_i(z)$ are also irreducible over $K[z]$, where K = R's field of quotients. Working now over K, we can express the g.c.d. of $\{p_i^{e_i}, \ldots, p_k^{e_k}\}$ (which is 1) as follows:

$$1 = r_1(z)\, p_i^{e_i}(z) + \ldots + r_k(z)\, p_k^{e_k}(z),$$

with $r_i(z) \in K[z]$, $i = 1, \ldots, k$. We can multiply both sides of this equation by some $h \in R$ to eliminate the denominators of coefficients in $r_1, \ldots, r_k$, to obtain

$$h = hr_1(z) \cdot p_1^{e_1}(z) + \ldots + hr_k(z) \cdot p_k^{e_k}(z),$$

with $hr_i(z) \in R[z]$, $i = 1, \ldots, k$.

It will sometimes happen that we can take $h = 1$. If this occurs, we have $r_i(z) \in R[z]$, $i = 1, \ldots, k$, and (in $R[z]$)

$$1 \in \sum_{i=1}^{k} \langle p_i^{e_i}(z) \rangle, \quad \text{so that}$$

$$R[z] = \sum_{i=1}^{k} \langle p_i^{e_i}(z) \rangle.$$

Under these circumstances,

$$X_f \simeq R[z]/\langle q(z) \rangle \simeq \bigoplus_{i=1}^{k} R[z]/\langle p_i^{e_i}(z) \rangle$$

This is a direct sum decomposition of the state module X_f.

Whether or not $h = 1$, we have the fact that

$$R[z] \cdot h = \langle h \rangle \subseteq \langle p_i^{e_i}(z), \ldots, p_k^{e_k}(z) \rangle.$$

This says that if we restrict instantaneous input values to multiples of h, then the set of reachable states lies entirely within $\langle p_i^{e_i}, \ldots, p_k^{e_k} \rangle$. This latter submodule is now decomposable as a direct sum. Restricting input values to multiples of h corresponds to multiplying the input matrix of a realization by h. To recover the original input/output map, we must multiply the output matrix by h^{-1} (if this is allowed, for the result will not strictly speaking be a realization over R).

6.5. Realization Example Over a P.I.D.

As discussed in chapter 1, certain partial difference systems can be formulated as linear systems over the ring $R[\hat{x}]$, where R = the real numbers and the circumflex over the $\hat{x}$ merely indicates that x is invertible; in other words, $R[\hat{x}] \simeq R[x, y]/\langle xy - 1\rangle$. It is easily shown that $R[\hat{x}]$ is a P.I.D. (by noticing that every element in $R[\hat{x}]$ can be written $x^j \cdot p(x)$ where $p(x) \in R[x]$ and j is some positive or negative integer.)

We can then think of realizing a (Hankel) sequence of maps H_j: $(R[\hat{x}])^m \to (R[\hat{x}])^p[[z^{-1}]]$.

Consider the scalar Hankel sequence

$$H_j = (x^{j-1} + x^{-j+1})\ S(x), \quad j \geq 1,$$

where S(x) is any element of $R[\hat{x}]$. This sequence can be interpreted as two "patterns" (distribution of coefficients) moving in opposite directions along a one-dimensional bar. We will show that this sequence is realizable and find a minimal realization.

Consider the expression $H_{j+2} - (x + x^{-1})\ H_{j+1} + H_j$:

$$\begin{aligned} H_{j+2} - (x + x^{-1})\ H_{j+1} + H_j &= \Big[x^{j+1} + x^{-j-1} - (x + x^{-1})(x^j + x^{-j}) \\ &\qquad + x^{j-1} + x^{-j+1}\Big] \cdot S(x) \\ &= \Big[x^{j+1} + x^{-j-1} - x^{j+1} - x^{-j+1} - x^{j-1} \end{aligned}$$

$$- x^{-j-1} + x^{j-1} + x^{-j+1}\Big] \cdot S(x)$$

$$= 0$$

Thus, $z^2 - (x + x^{-1})z + 1 \in (R[\hat{x}])[z]$ is a monic annihilator of the sequence, and so H_j is realizable over $R[\hat{x}]$. Note that the above polynomial can be factored into irreducible components as $(z - x)(z - x^{-1})$. A realization for H_j is given by

$$H_j = [1, 1] \begin{bmatrix} x & 0 \\ 0 & x^{-1} \end{bmatrix}^{j-1} \begin{bmatrix} S(x) \\ S(x) \end{bmatrix}$$

This is a free, two-dimensional, realization over $R[\hat{x}]$; we know that every canonical realization over a P.I.D. is free. This realization is canonical and minimal.

Hopefully, this approach could be helpful in solving discretized versions of constant-coefficient partial differential equations. It will be an interesting problem to somehow incorporate boundary conditions into the formulation.

6.6. Finite Discretization of Partial Differential Systems.

This example shows how certain partial differential systems can be discretized and formulated as linear systems over a group ring (or group algebra). The approach seems particularly relevant to systems with periodic boundary conditions or forcing functions.

Consider the wave equation in two spatial dimensions

$$\frac{\partial^2 E}{\partial t^2} = \alpha^2 \left(\frac{\partial^2 E}{\partial x_1^2} + \frac{\partial^2 E}{\partial x_2^2} \right)$$

assumed to hold throughout the (x_1, x_2)-plane for all time t. Suppose that the (x_1, x_2)-plane is discretized, i.e., replaced by a two-dimensional grid $= J \oplus J$, where J = the integers. Then at any instant of time, the states of the system are represented by maps $E_t\colon J \oplus J \to R$, where R = real numbers.

Now suppose that the system has periodic boundary conditions or forcing functions so that the states have the same values every n grid points in either the x_1 or x_2 direction. Such a situation might model a crystal, an antenna array, an interdigital filter, or periodically loaded beam.

In any case, we only have to know the value of E_t, say, at n^2 points to know E_t throughout the two-dimensional grid. We see that we can represent states as elements of the ring

$$K = R[z_1, z_2]/\langle z_1^{\,n}-1,\ z_2^{\,n}-1\rangle$$

where R = the real numbers, $R[z_1, z_2]$ = ring of polynomials in two indeterminates z_1, z_2 over R, and $\langle z_1^{\,n}-1,\ z_2^{\,n}-1\rangle$ is the ideal generated by $z_1^{\,n}-1$ and $z_2^{\,n}-1$. Here the coefficient of $z_1^{\,r} z_2^{\,s}$ $(0 \le r, s < n)$ represents the value of the state at the point (r,s) in the $n \times n$ representative subgrid.

Define $\quad E_1(t) = E(t) \in K$

and $\quad E_2(t) = E(t+1) \in K$

We can represent the Laplacian operator as

$$\alpha^2 \left(\frac{\partial}{\partial x_1^2} + \frac{\partial}{\partial x_2^2} \right) \mapsto \alpha^2 [z_1^{-1}(z_1-1)^2 + z_2^{-1}(z_2-1)^2];$$

define: $q(z_1, z_2) = \alpha^2[z_1^{-1}(z_1-1)^2 + z_2^{-1}(z_2-1)^2] \in K$. This means that the action of the Laplacian on a state $E(t) \in K$ can be modelled by the multiplication of $E(t)$ by$q(z_1, z_2)$ in the ring K.

We can approximate $\partial^2 E(t)/\partial t^2$ by

$$E(t+2) - 2E(t+1) + E(t).$$

The wave equation is thus approximated by

$$E(t+2) - 2E(t+1) + E(t) = q(z_1, z_2) \cdot E(t).$$

In terms of E_1 and E_2 we can then write

$$\begin{bmatrix} E_1 \\ E_2 \end{bmatrix}_{t+1} = \begin{bmatrix} 0 & 1 \\ q(z_1, z_2)-1 & 2 \end{bmatrix} \begin{bmatrix} E_1 \\ E_2 \end{bmatrix}_t$$

This is a linear system over the ring K with state "space" (module) equal to $K \oplus K$. The formulation is directly analogous to the usual field formulation.

One of the main points of interest here is the fact that K is (isomorphic to) the group ring (or algebra) $R[J_n]$ where R = the real numbers and J_n = the integers modulo n. This is interesting because K and $K \oplus K$ are semisimple and finite Fourier techniques are applicable. In particular, the Fast Fourier Transform algorithm may be used to implement the various multiplications of elements in the group ring. Furthermore, it is to be hoped that the techniques of semisimple system decomposition developed in the last chapter can be specialized to this commutative situation. In some sense, this formulation is even "richer" in structure than the usual field-type linear system; this richness is a result of imposing a multiplicative structure on the basis elements of the state space.

A serious omission in the discussion so far is the question of boundary conditions. Only some general comments can be made here. However, a preliminary investigation suggests that some boundary conditions can be met by (1) calculating the next state without constraint or control, (2) calculating a control that forces this next state to meet the boundary conditions, and (3) calculating the next state using this control. The control term so generated will probably have a physical interpretation such as an electronic charge or current, an addition of heat, or the reaction of a mechanical support. This general technique has been successfully applied to diffusion systems.

7. SUGGESTIONS AND SUMMARY

7.1 Suggestions for Further Work

The extensive structural knowledge of semisimple modules would justify further study of linear systems whose state modules are semisimple on theoretical grounds, at least. The connection between group algebras (which are semisimple) and group homomorphic machines suggests that such a study would be of more than intrinsic interest, however. Particular questions that could be asked are:

(1) When can an automorphism of a semisimple module be represented in block diagonal form, instead of just block triangular form?

(2) If the semisimple module is a group algebra and there exists a faithful matrix representation (over a field) of this algebra, what can be said about module endomorphisms?

(3) What simplifications occur when the state module is semisimple over a commutative ring? In this case, what are the connections with finite Fourier expansions?

A second area for further investigation might be the one introduced in Chapter 6, where probability distributions on an abelian group G were viewed as elements of the group algebra R[G], R = the real numbers. One goal in this direction would be to develop a state observer for a linear system whose state set is a finite abelian group, much like a Kalman filter. The object here would be to reconstruct the initial state of a linear system from noisy measurements on the output. If the initial state is viewed as an encoded message, such an observer would have a strong interpretation as a decoder.

A third area for potential investigation is the connection between the B.C.H. decoding algorithm and the theory of partial realizations in the case where the state set is a finite abelian group. It is known, for example, that the B.C.H. decoding algorithm over GF(q) is more or less equivalent to the problem of finding a minimal partial realization for a scalar sequence over GF(q). The question can be put: given that the B.C.H. decoding algorithm can be applied over various finite rings (other than fields), is the connection maintained with partial realization theory over these rings?

A fourth area for investigation concerns the problem of machine verification, or checking sequences. The partial realization problem for a linear system is to infer a complete description of a system given the first few turns of its impulse responses (Hankel sequence). In some cases, the partial Hankel sequence has a unique, minimal (in some sense) realization. One could think of this process as an experiment to determine the inner workings of a physical system: a 1 followed by some 0's is applied to an input port and the first few outputs are recorded. Suppose realization of this output sequence leads to a unique, minimal, canonical linear system. Then, either the physical system is accurately described by this realization, or it is non-minimal or non-linear (i.e., not in the class considered). It would be interesting to see if this technique could be applied to the problem of determining whether a physical system conforms to its design specifications.

Finally, a topic of theoretical interest is the further decomposition of linear systems over Noetherian Unique Factorization Domains and Principal Ideal Domains (where the output module is free). A major question might be: to what extent is the rational canonical decomposition over this field of quotients relevant to decomposition over the domain?

7.2 Summary

Chapter 2 presented the basic notion of a discrete-time, linear, time-invariant system over a ring R. The equivalent concept of a linear input/output map over R was discussed.

Chapter 3 established the importance of the ascending chain condition (A.C.C.) on the state module. It was shown that A.C.C. is fundamental to recovering familiar system-theoretic properties in this more general context. The result was a network of implications connecting A.C.C., reachability, distinguishability, controllability, realizability, the existence of transfer functions and the existence of monic annihilators. An effort was made to show that most of these results are valid even when the ring is noncommutative.

Chapter 3 also investigates systems over Noetherian rings, particularly integral domains. The results were similar to those of Rouchaleau, Kalman, and Wyman, but were approached in an entirely different way.

Chapter 4 discussed linear systems whose state sets were torsion modules over a P.I.D., e.g., finite abelian groups. Consideration of these systems was motivated by construction of a large class of error-correcting codes similar to the B.C.H. codes. It was shown that these codes could be conveniently implemented by using linear systems with finite abelian groups for state sets. This class of machines was then analyzed. Next state endomorphisms could always be put in a form reminiscent of rational canonical form, and thus be implemented rather easily with shift registers.

Chapter 5 continued to exploit A.C.C., but from the viewpoint of decomposition. Eventually, some effects of the descending chain condition (D.C.C.) and semisimplicity on decomposition were discussed. In particular, chapter 5 gave an automaton-theoretic cascade decomposition for systems with A.C.C., established the uniqueness of a parallel decomposition for systems with A.C.C. and D.C.C., and gave a detailed decomposition of linear systems whose state modules are semisimple.

Chapter 6 presented a diverse collection of dynamic systems, that could be formulated as "D.L.T.I. systems over a ring". Chapter 6 may contain the most important contributions of this thesis.

Finally, a summary of this thesis and suggestions for continuing the investigation were given in Chapter 7.

REFERENCES

1. J. Hartmanis, R. E. Stearns, "Algebraic Structure Theory of Sequential Machines", Prentice-Hall, Englewood Cliffs, N. J., 1966.

2. H. P. Zeiger, Chapter 4 in "Algebraic Theory of Machines, Languages, and Semigroups", M. A. Arbib, ed., Academic Press, New York, N. Y., 1968.

3. K. Krohn, J. L. Rhodes, and B. R. Tilson, Chapter 5 in"Algebraic Theory of Machines, Languages, and Semigroups", M. A. Arbib, ed., Academic Press, New York, N. Y., 1968.

4. R. W. Brockett, A. S. Willsky, "Finite Group Homomorphic Sequential Systems", IEEE Trans. A.C., Vol. AC-17, No. 4, August 1972, pp. 483-490.

5. M. A. Arbib, "Two Papers on Group Homomorphic Machines" Technical Report, Dept. of Electrical Engineering, University of Massachusetts, Amherst, Mass.

6. Y. Rouchaleau, "Linear, Discrete-Time, Finite Dimensional, Dynamical Systems Over Some Classes of Commutative Rings", Ph.D. dissertation, Department of Operations Research, Stanford University.

7. Y. Rouchaleau, R. E. Kalman, and B. F. Wyman, "Algebraic Structure of Linear Dynamical Systems III, Realization Theory over a Commutative Ring", Proc. Nat. Acad. Sciences, November 1972, 69, 11: 3404-3406.

8. E. R. Berlekamp, "Algebraic Coding Theory", McGraw-Hill Book Co., New York, N.Y., 1968.

9. R. G. Gallager, "Information Theory and Reliable Communication", John Wiley and Sons, Inc., New York, 1968.

10. R. E. Kalman, P. Falb, M. A. Arbib, "Topics in Mathematical System Theory", McGraw-Hill Book Co., New York, N.Y., 1969.

11. N. Jacobson, "Lectures in Abstract Algebra", Vol. 1, D. Van Nostrand Co. Inc., Princeton, N. J., 1951.

12. S. Lang, "Algebra", Addison-Wesley Publishing Co., Reading, Mass., 1971.

13. R. B. Ash, "Information Theory", John Wiley and Sons, Inc., New York, N.Y., 1965.

14. I. N. Herstein, "Topics in Algebra", Blaisdell, 1964.

15. M. A. Arbib, "Automata Theory", Part 3 of "Topics in Mathematical System Theory", McGraw-Hill Book Co., New York, N.Y. 1969.

16. I. N. Herstein, "Noncommutative Rings", Carus Mathematical Monograph No. 15, published by the Mathematical Assoc. of America, distributed by John Wiley and Sons, Inc., 1968.

17. B. L. van der Waerden, "Algebra", Vol. 2, Frederick Ungar Publishing Co., New York, N.Y., 1970.

18. D. T. Finkbeiner, "Introduction to Matrices and Linear Transformations", W. H. Freeman and Co., San Francisco, 1960.

Appendix 1. The Rings J_pm and $J_pm[x]$

In this section and the next the letter J denotes the ring of integers; p denotes a prime $\in$ J and J_pm denotes the ring of integers modulo p^m, $m > 0$ (i.e., $J_pm = J/<p^m>$, where $<p^m>$ denotes the ideal generated by p^m). An element of J_pm is denoted $[x]_pm$, and $<x_1, x_2, \ldots, x_n>$ denotes the ideal generated by $x_1, \ldots, x_n$ in some specified ring.

Definition A.1. A ring having a unique maximal ideal is said to be a local ring.

Lemma A.1. Let M be the maximal ideal of a local ring R. If $x \notin M$, then x is a unit of R (i.e., $\exists y \in R$ such that $sy = 1$)

Proof. Suppose $x \notin M$. If x is not a unit, then x generates a proper ideal I of R. Now I must be contained in some maximal ideal of R (provided R has an identity). But R has only one maximal ideal M, so $I \subseteq M$. Thus $x \in M$, contradiction. Hence $x \notin M$ implies x is a unit of R. Q.E.D.

Lemma A.2. J_pm is a local ring (for any prime p and integer $m > 0$) with maximal ideal $P = <[p]_pm>$.

Proof. Since p generates a maximal ideal of J, $[p]_pm$ certainly generates a maximal ideal of J_pm. Let M′ be another maximal ideal of J_pm. Then M′ is the image of a maximal ideal $<q> \subseteq J$, where q is some prime $q \neq p$. But then $<q>$ must contain $<p^m> \subseteq J$, i.e., p^m must be some multiple of q, which is impossible. Thus $P = <[p]_pm>$ is the unique maximal ideal of J_pm. Q.E.D

Notation: (1) with reference to the ring J_pm, P will denote $<[p]_pm>$.

(2) $U \subseteq J_p m$ is defined by

$$U = \{r \in J_p m \mid r \notin P\} = J_p m - P$$

Lemma A.3. $U \subseteq J_p m$ is an abelian group under multiplication of order $(p-1)p^{m-1}$.

Proof. by lemma 7.1, U is the group of units of $J_p m$, and since multiplication in $J_p m$ is commutative, U is indeed an abelian group under multiplication with identity $[1]_p m$.

To prove the second part, note that $J_p m/P$ is (isomorphic to) the field J_p, having p elements. Since $J_p m$ contains p^m elements, it follows that P contains $\#(J_p m)/\#(J_p) = p^{m-1}$ elements. Hence $U = J_p m - P$ contains $p^m - p^{m-1} = (p-1)\cdot p^{m-1}$ elements. Q.E.D.

Definition A.2. A coset of $P < [p]_p m > \subseteq J_p m$ will be called a primitive coset if it is a primitive element of the field $J_p m/P = J_p$. An element of $J_p m$ will be called P-primitive if it lies in some primitive coset of P. Note that if θ if P-primitive, then $\theta, \theta^2, \ldots, \theta^{p-2}, \theta^{p-1}$ all lie in distinct cosets of P and furthermore, $\forall\ x \notin P$, $x^{p-1} \equiv [1]_p m \bmod P$; i.e., x^{p-1} lies in that coset of P containing $[1]_p m$, namely $[1]_p m + P$.

Although the fact is not required here, it is useful to know that if $p \neq 2$, the group U of units in $J_p m$ is cyclic. This means that U is the direct product (as an abelian group) of a cyclic group of order (p-1) and a cyclic group of order p^{m-1} (which happens to be generated by $[1 + p]_p m$). If $p = 2$, and $m \geq 3$, U is the direct product of a group of order 2 and a cyclic group of order 2^{m-2}.

We now consider ways to extend the ring $J_p m$ by forming $J_p m[x]/<q(x)>$, where $<q(x)>$ is the ideal generated by a monic-polynomial $q(x) \in J_p m[x]$.

Lemma A.4. Let φ: $J_p m \to J_p$ be the canonical ring homomorphism mapping $J_p m$ onto J_p, where φ: $[x]_p m \mapsto [x]_p$. Then φ can be extended to a homomorphism mapping $J_p m[x]$ onto $J_p[x]$ by defining

$$\varphi \left(\sum_{i=0}^{n} [a_i]_p m\, x^i \right) = \sum_{i=0}^{n} [a_i]_p\, x^i \qquad (1)$$

The kernel of this homomorphism is the principal ideal P of $J_p m[x]$ generated by $[p]_p m$, and P is a prime ideal of $J_p m[x]$.

Proof. Obvious.

Lemma A 5. Every ideal of $R = J_p m[x]$ that properly contains $P = <[p]_p m>$ is generated by two elements, one of which is $[p]_p m$ and the other of which can be chosen as a monic polynomial.

Proof. Let φ be the canonical homomorphism mapping $J_p m[x]$ onto $J_p[x]$ as in equation 7.1. Let I be an ideal of R properly containing P. Then $\varphi(I)$ is a non-zero ideal of $J_p[x]$, and since $J_p[x]$ is a P.I.D., $\varphi(I) = <q'(x)>$ where $q'(x)$ can be taken as a monic polynomial $\in J_p[x]$. Clearly, we can find a monic-polynomial $q(x) \in I$ of the same degree as $q'(x)$ such that $\varphi(x) = q'(x)$. By assumption, I contains $<[p]_p m>$, so $<[p]_p m, q(x)> \subseteq I$.

Now let $f(x) \in I$. Since $q(x)$ is monic, we can write

$$f(x) = m(x)\ q(x) + r(x), \qquad (2)$$

where $\partial^0 r(x) < \partial^0 q(x) = \partial^0 q'(x)$. Since $f(x) \in I$, $\varphi(f(x)) \in \varphi(I) = <q'(x)>$. Since $\varphi(q(x)) = q'(x)$, $\varphi(m(x)\ q(x)) \in <q'(x)>$ as well. Hence $\varphi(r(x)) \in <q'(x)>$ where $\partial^0 r(x) < \partial^0 q'(x)$. But $q'(x)$ is a polynomial of least degree in $<q'(x)>$. Thus $\varphi(r(x)) = 0$, and $r(x) \in P$. So $r(x) = [p]_pm \cdot r'(x)$, some $r'(x) \in R$. Thus $f(x) = m(x)\ q(x) + [p]_pm \cdot r'(x)$. But this is equivalent to saying that $f(x) \in <[p]_pm,\ q(x)>$, and so we conclude that $I \subseteq <[p]_pm,\ q(x)>$. Hence $I = <[p]_pm,\ q(x)>$. Q.E.D.

Corollary A.5.1. Let M be a maximal ideal of the ring $J_pm[x]$. Then $M = <[p]_pm,\ q(x)>$ where $q(x)$ is a monic polynomial such that $\varphi(q(x))$ is irreducible in $J_p[x]$. Furthermore $J_pm[x]/M \simeq J_p[x]/<\varphi(q(x))>$.

Proof. we first show that any prime ideal I of $J_pm[x]$ must contain $P = <[p]_pm>$. Otherwise, there is some polynomial of the form $[p]_pm\cdot r(x)$ not contained in I, and must therefore be a non-zero element of $J_pm[x]/I$. Since I is a prime ideal, $J_pm[x]/I$ is a domain. However, $([p]_pm\cdot r(x))^m = [p^m]_pm\cdot r^m(x) = 0$, contradicting the fact that $J_pm[x]/I$ is a domain. Thus any prime ideal, and hence M, must contain P. By lemma 5, M is of the form $<[p]_pm,\ q(x)>$ where $q(x)$ is a monic polynomial of $J_pm[x]$. Since M is a maximal ideal of $J_pm[x]$, $\varphi(M) = <\varphi(q(x))>$ is a maximal ideal of $J_p[x]$. Hence $\varphi(q(x))$ is irreducible in $J_p[x]$.

It can be shown that $J_pm[x]/M \simeq J_p[x]/<\varphi(q(x))>$ in the usual manner.

Q.E.D.

Corollary A.5.2. (Converse to above corollary). Let $q(x)$ be a monic polynomial $\in J_pm[x]$ such that $\varphi(q(x))$ is irreducible in $J_p[x]$. Then $M =$

$<[p]_p m,\ q(x)>$ is a maximal ideal of $J_p m[x]$.

Proof. because $\varphi(M)$ is a maximal ideal of $J_p[x]$.

Lemma A.6. Let $q(x)$ be a monic polynomial $\in J_p m[x]$ such that $\varphi(q(x))$ is irreducible in $J_p[x]$. Then $R' = J_p m[x]/<q(x)>$ is a local ring with maximal ideal $P' = <[p]_p m>$.

Proof. Let $\psi: J_p m[x] \twoheadrightarrow J_p m[x]/<q(x)>$ be the canonical epimorphism. Since $M = <[p]_p m,\ q(x)>$ is a maximal ideal of $J_p m[x]$, $\psi(M)$ is a maximal ideal of $R' = J_p m[x]/<q(x)>$. But $\psi(M) = <\psi([p]_p m),\ \psi(q(x))> = <\psi([p]_p m)>$, since $\psi(q(x)) = 0$. But $\psi([p]_p m) = [p]_p m$ if we view $J_p m$ as embedded in R'. Thus $P' = <[p]_p m>$ is a maximal ideal of $R' = J_p m[x]/<q(x)>$, and $\psi^{-1}(P') = <[p]_p m,\ q(x)>$.

We must now show that P' is the unique maximal ideal of R'. Let I' be any maximal ideal of R. Then $\psi^{-1}(I')$ is a maximal ideal of $J_p m[x]$ containing $<q(x)>$. By corollary 7.5.1 $\psi^{-1}(I') = <[p]_p m,\ S(x)>$, where $S(x)$ is monic and $\varphi(S(x))$ is irreducible in $J_p[x]$. But $q(x) \in \psi^{-1}(I')$, so $\psi^{-1}(I')$ contains the ideal $<[p]_p m,\ q(x)>$ which is maximal by corollary 7.5.2. Therefore $\psi^{-1}(I') = <[p]_p m,\ q(x)>$ for otherwise $\psi^{-1}(I') = J_p m[x]$ contradicting fact that I' is a proper ideal of R'. But this means that $\psi^{-1}(I') = \psi^{-1}(P')$, and hence that $I' = P'$. Thus P' is the unique maximal ideal of $R' = J_p m[x]/<q(x)>$. Q.E.D.

Definition A.3. A monic polynomial $q(x) \in J_p m[x]$ will be called P-irreducible if the image $\varphi(q(x)) \in J_p[x]$ is irreducible.

Corollary A.6.1. Let $q(x) \in J_p m[x]$ be a P-irreducible polynomial of degree

d. Let P' be the maximal ideal of $R' = J_{p^m}[x]/\langle q(x)\rangle$, and let $U' = R' - P'$. Then U' is the group of units of R', and forms an abelian group (under polynomial multiplication modulo $q(x)$) of order $(p^d-1) \cdot p^{(m-1)d}$

Proof. that U' is the group of units of R' is clear from the fact that R' is local with maximal ideal P'.

Now $R' = J_{p^m}[x]/\langle q(x)\rangle$ consists of all polynomial residues under division by $q(x)$, i.e., polynomials of degree less than d. Since any one of p^m elements $\in J_{p^m}$ can appear at any of d coefficient positions, R' consists of p^{md} elements. Furthermore R'/P' is a field, and is isomorphic to $J_p[x]/\langle\varphi(q(x))\rangle$. Since $q(x)$ is monic, $\varphi(q(x))$ is of degree d as well, and $J_p[x]/\langle\varphi(q(x))\rangle$ therefore contains p^d elements. Thus P' contains $p^{md}/p^d = p^{(m-1)d}$ elements. Consequently, $U' = R' - P'$ contains $p^{md} - p^{(m-1)d} = (p^d-1) \cdot p^{(m-1)d}$ elements as claimed. Q.E.D.

Definition A.4: (extension of Def. 7.2.) Let $R' = J_{p^m}[x]/\langle q(x)\rangle$ where $q(x)$ is P-irreducible, and let P' be the maximal ideal of R'. A coset of P' will be called a primitive coset if it is a primitive lement of $R'/P' \simeq J_p[x]/\langle\varphi(q(x))\rangle$. An element of R' will be called P-primitive if it lies in some primitive coset of P'. Note that if θ is P-primitive and $\partial^0 q(x) = d$, then $\theta, \theta^2, \ldots, \theta^{p^d-1}$ all lie in distinct cosets of P'.

Discussion: The rings $J_{p^m}[x]/\langle q(x)\rangle$, $q(x)$ P-irreducible, have been developed to provide number systems with which to construct certain codes and their encoders/decoders. Study of these rings is a necessary preliminary to studying error-correcting codes over J_{p^m} (or J_n, n = any integer).

In the process of constructing error-correcting codes over J_pm, it is helpful to consider equations of the form:

$$\sum_{k=0}^{t} a_k(\theta^i)^k = 0 \qquad (3)$$

where θ is a p-primitive element of $R = J_pm[x]/\langle q(x)\rangle$, $q(x)$ = P-irreducible, and $a_k \in R$, $k = 0, 1, \ldots, t$. Solving equation 7.3 consists of finding those powers θ^i of θ that satisfy 7.3. Another way of looking at it is: given any polynomial $f(x) \in R[x]$ and a P-primitive element θ of $R = J_pm[x]/\langle q(x)\rangle$, for what values of i does $f(\theta^i) = 0$? These equations occur because we will represent each digit position i in a code of block length n by θ^i, where θ is a P-primitive element of some local ring $J_pm[x]/\langle q(x)\rangle$. Finding out at what positions errors occurred will then be equivalent to solving equations of the form 7.3. Note that 7.3 is really an equation for i, where $0 \leq i < p^d-1$ and d is the degree of q(x) in $R = J_pm[x]/\langle q(x)\rangle$.

The reason that we represent digit positions by θ^i is given by the lemma below. First, we have

Definition A.5. If q(x) is a P-irreducible polynomial (of degree d) in $J_pm[x]$, then $R = J_pm[x]/\langle q(x)\rangle$ will be called a local extension of J_pm (of degree d).

Lemma A.7. Let f(x) be any polynomial of degree t in R[x] where R is a local extension of J_pm (of degree d, say). Let θ be a P-primitive element of R. Then f(x) has at most t distinct roots of the form θ^i, $0 \leq i < p^d - 1$.

Proof. Suppose f(x) has more than r distinct roots, say θ^{k1}, θ^{k2}, ... θ^{k_r},

$\theta^{k_{r+1}}$, ... where $\theta^i \neq \theta^j$ if $i \neq j$. Then write

$$f(x) = m_1(x)\ (x - \theta^{k_1}) + r_1 \tag{4}$$

where $\partial^0 r_1 = 0$ and $\partial^0 m_1(x) = t - 1$. Since $f(\theta^{k_1}) = 0$, we must have $r_1 = 0$, and we can write

$$f(x) = M_i(x)\ (x - \theta^{k_1}) \tag{5}$$

Since θ^{k_2} is also a root of $f(x)$, we have

$$f(\theta^{k_2}) = m_1(\theta^{k_2})\ (\theta^{k_2} - \theta^{k_1}) = 0 \tag{6}$$

Now, since $\theta^{k_2} \neq \theta^{k_1}$, and $0 < k_1, k_2 < p^d - 1$, θ^{k_1} and θ^{k_2} must lie in different cosets of the maximal ideal P of R, because θ is P-primitive. This means that $\theta^{k_2} - \theta^{k_1} \notin P$. Because R is local, $\theta^{k_2} - \theta^{k_1}$ must be a unit. Then from 6 we obtain

$$m_1(\theta^{k_2}) = 0 \tag{7}$$

i.e., that θ^{k_2} is a root of $m_1(x)$.

Now write $\qquad m_1(x) = M_2(x)\ (x - \theta^{k_2}) + r_2, \qquad (8)$

and conclude that $m_1(x) = m_2(x)\ (x - \theta^{k_2})$, $\partial^0 m_2 = t - 2$.

Thus $\qquad f(x) = m_2(x)\ (x - \theta^{k_2})\ (x - \theta^{k_1}) \qquad (9)$

Continuing in this way t times, we find that

$$f(x) = m_t\ (x - \theta^{k_r})\ \dots\ (x - \theta^{k_2})\ (x - \theta^{k_1}), \tag{10}$$

where m_t is of degree 0, i.e., $m_t \in R$. We now use the fact that $f(\theta^{k_{r+1}}) = m_t(\theta^{k_{r+1}} - \theta^{k_r})\ \dots\ (\theta^{k_{r+1}} - \theta^{k_1}) = 0.$ (11)

We argue, as before, that since all the roots θ^{k_i} are distinct, $(\theta^{k_{r+1}} - \theta^{k_r}) \ldots (\theta^{k_{r+1}} - \theta^{k_1})$ is a unit. Equation 11 then forces $m_t = 0$, contradicting fact that f(x) is of degree t. Hence if f(x) is of degree t, f(x) has at most t distinct roots of the form θ^i, $0 \leq i < p^d - 1$, θ = P-primitive.

Q.E.D.

Thus if we have t distinct roots of a degree t polynomial $f(x) \in R[x]$ in the form θ^i, $0 \leq i < p^d - 1$, θ = P-primitive, we know that we have them all. Furthermore, we know that f(x) can be factored into a constant times t distinct linear factors of the form $(x - \theta^{k_i})$. What happens if f(x) has multiple roots, i.e., if f(x) can be written

$$f(x) = m_t(x - \theta^{k_1})^{e_1} \ldots (x - \theta^{k_j})^{e_j} \ ? \qquad (12)$$

The same arguments used above will show that we again have all the roots having the form θ^i, $0 \leq i < p^d - 1$.

The relevance of this result to coding is simply that, under certain conditions, we will be able to identify precisely the locations of errors in a transmitted word by finding the roots of polynomials having the form in 3. The significance of this result may be further brought by realizing that, in general, if $f(x) \in J_p m[x]$, $\partial^0 f = t$, f may have far more than t roots in some extension of $J_p m$. In the coding context this would had to unacceptable ambiguities in error locations with any scheme that tried to identify these locations by finding the roots of polynomials in $J_p m[x]$ or R[x].

There is one more facet of local extensions of $J_p m$ that we should consider; we will see later that it is rather crucial to the convenient implementation of encoders and decoders over J_pm. Specifically, the question is one of representing elements in an extension $R = J_pm[x]/\langle q(x)\rangle$. Suppose $R = J_pm[x]/\langle q(x)\rangle$ is a local extension of degree d. On one hand, R can be viewed as free module of dimension d over J_pm, generated by $\{1, x, x^2, \ldots x^{d-1}\}$. On the other hand, R is a commutative ring with multiplication modulo q(x). Thus R is an algebra over J_pm. In this sense, R, as a ring, operates on itself as a module. Thus, each element of R can be represented by a $d \times d$ matrix over J_pm as well. Hence we have a representation (homomorphism) mapping R into a commutative subalgebra of the algebra of endomorphisms $\mathrm{End}[(J_pm)^r]$.

It will be of particular interest to represent a P-primitive element θ in a degree d local extension $J_pm[x]/\langle q(x)\rangle$ by a $d \times d$ matrix. We will then be able to calculate powers θ^i by matrix multiplication. To see what the calculation of such a representation involves, let

$$q(x) = x^d + \sum_{i=0}^{d-1} q_i x^i \qquad (13)$$

and suppose that the P-primitive element θ is given by

$$\theta = \sum_{i=0}^{d-1} \theta_i x^i \qquad (14)$$

We know that θ can be represented by the column vector

$$\underline{\theta} = \begin{bmatrix}\theta_0\\ \theta_1\\ \cdot\\ \cdot\\ \cdot\\ \theta_{d-2}\\ \theta_{d-1}\end{bmatrix} \tag{15}$$

To represent θ as a matrix, we must calculate the effect of multiplying each basis element $\in \{1, x, x^2, \ldots, x^{d-1}\}$ by θ. We represemt x^{d-1}, x^{d-2}, x^{d-3}, ..., 1, by

$$\begin{bmatrix}0\\0\\ \cdot\\ \cdot\\ \cdot\\0\\0\\1\end{bmatrix}, \begin{bmatrix}0\\0\\ \cdot\\ \cdot\\ \cdot\\0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\ \cdot\\ \cdot\\ \cdot\\1\\0\\0\end{bmatrix}, \ldots\ldots, \begin{bmatrix}1\\0\\ \cdot\\ \cdot\\ \cdot\\0\\0\\0\end{bmatrix}, \text{ respectively} \tag{16}$$

These column vectors will be called $\underline{x}^{d-1}$, $\underline{x}^{d-2}$, ..., $\underline{1}$.

Clearly, $\theta\ 1 = \theta$ which can be represented by $\underline{\theta}$ as in equation 3. Now

$$\begin{aligned}\theta x &= \left(\sum_{i=0}^{d-1} \theta_i x^i\right)x\\ &= \sum_{i=0}^{d-1} \theta_i x^{i+1}\\ &= \theta_{d-1}x^d + \sum_{i=1}^{d-1} \theta_{i-1}\, x^i\end{aligned}$$

$$= \theta_{d-1} \left(\sum_{i=0}^{d-1} - q_i x^i \right) + \sum_{i=1}^{d-1} \theta_{i-1} x^i$$

$$= \sum_{i=1}^{d-1} (-\theta_{d-1} q_i + \theta_{i-1}) x^i + \theta_{d-1} q_0 \qquad (17)$$

θx can now be represented as the column vector

$$\underline{\theta x} = \begin{bmatrix} -\theta_{d-1} q_0 \\ -\theta_{d-1} q_1 + \theta_0 \\ \vdots \\ -\theta_{d-1} q_i + \theta_{i-1} \\ \vdots \\ -\theta_{d-1} q_{d-1} + \theta_{d-2} \end{bmatrix} \qquad (18)$$

Continuing in this way we can eventually represent θ as the $d \times d$ matrix

$$H = \underline{\theta}, \underline{\theta x}, \ldots, \underline{\theta x}^{d-1} \qquad (19)$$

where $\underline{\theta x}^i$ is the column vector representation of θx^i. (Note, in passing, that if we define the matrix α by

$$\begin{bmatrix} 0 & & & & -q_0 \\ 1 & & & & -q_1 \\ & 1 & & & -q_2 \\ & & \ddots & & \vdots \\ & & & 1 & -q_{d-1} \end{bmatrix} \qquad (20)$$

then we can calculate H as

$$H = \left[\underline{\theta}, \alpha\underline{\theta}, \ldots, \alpha^{d-1}\underline{\theta}\right] . \tag{21}$$

In any case, we obtain the matrix H as a representation of the action of θ on R. Note that we can obtain $\underline{\theta}^{i}$ by calculating $H^{i}\underline{1}$, and that since θ is a unit of R, H is invertible.

Appendix 2. Finitely-Generated Torsion Modules Satisfy Both Cháin Conditions.

Proof. (Of Proposition 4.3)

(a) Since J is a P.I.D., it is clear that every ideal of J is finitely generated. Hence J is Noetherian. Since X is F.G. over J, X is a Noetherian module; i.e., X satisfies the ascending chain condition on submodules.

(b) Since X is a F.G. torsion module over J, we know from Theorem 7.1 that X = $\underset{p}{\oplus} X[p]$, where for each ;, X[p] = $J_p{}^{m_1} \oplus \cdots \oplus J_p{}^{m_s}$, some $m_1, \ldots, m_s$. Suppose Y is a submodule of X. Then Y = $\underset{p}{\oplus} Y[p]$, and Y[p] = $J_p{}^{n_1} \oplus \cdots \oplus J_p{}^{n_t}$, for certain primes p and for some $n_1, \ldots, n_t$. It is easy to show that Y[p] ⊊ X [p] for each prime p. We first will show that if Y[p] ⊊ X[p], then there is only a finite number of modules having the form $\overset{t}{\underset{j=1}{\oplus}} J_p{}^{n_t}$ to which Y[p] can be isomorphic. In other words, every submodule of X[p] must fall in one of only a finite number of isomorphism classes (each class being characterized by an expression of the form $\overset{t}{\underset{j=1}{\oplus}} J_p{}^{n_t}$).

We will do this in two steps: the first step will show that if Y[p] ⊊ X[p], X[p] $\simeq \overset{s}{\underset{i=1}{\oplus}} J_p{}^{m_i}$, and Y[p] $\simeq \overset{t}{\underset{j=1}{\oplus}} J_p{}^{n_t}$, then $t \leq s$. The second step will show that if $m_1 \leq \cdots \leq m_s$ and $n_1 \leq \cdots \leq n_t$, then $n_t \leq m_s$. It will follow that

$$\sum_{j=1}^{t} n_j \leq t.n_t \leq s.m_s \qquad (22)$$

Since there are only a finite number of ways of choosing t and $\{n_j\}_{j=1}^{t}$ to satisfy (22), we will have the result: a submodule Y[p] of X[p] must belong to one of a finite number of isomorphism classes.

First step: let $X_p = \{x \in X[p] \mid px = 0\}$ and let $Y_p = \{y \in Y[p] \mid py = 0\}$. Clearly $Y_p \subseteq X_p$. Claim: $X_p \simeq (J_p)^s$ and $Y_p \simeq (J_p)^t$; Proof: Since $X[p] \simeq \bigoplus_{i=1}^{s} J_{p^{m_i}}$, $X[p]$ contains a submodule $X_1 \simeq (J_p)^s$, since each direct summand $J_{p^{m_i}}$ contains a submodule of the form J_p generated by $p^{m_i-1}.g_i$ where g_i is a generator of the cyclic module $J_{p^{m_i}}$. Similarly, $Y[p]$ contains a submodule $Y_1 \simeq (J_p)^t$. Clearly, $pX_1 = (0)$; hence $X_1 \subseteq X_p$. Now let $x \in X_p$, and write x as a direct sum

$$x = a_1g_1 + \ldots + a_sg_s \tag{23}$$

where $a_i \in J$ and g_i generates the $i^{\underline{th}}$ direct summand $J_{p^{m_i}}$. By definition of X_p, $px = 0$. Hence $pa_1g_1 + \ldots + pa_sg_s = 0$, which implies that $pa_ig_i = 0$, $i = 1, \ldots, s$ (otherwise would contradict the fact that $X[p] =$ <u>direct</u> sum of the cyclic submodules generated by the g_i). Hence $a_i \equiv 0 \pmod{p^{m_i-1}}$, $i = 1, \ldots, s$, and we can write $a_k = b_i\, p^{m_i-1}$ for all i. Thus, $x = b_1(p^{m_1-1}g_1) + \ldots + b_s(p^{m_s-1}g_s)$. But X_1 is the submodule of $X[p]$ generated by $\{p^{m_i-1}g_i\}_{i=1}^{s}$, and so $x \in X_1$. Hence $X_p \subseteq X_1$, and consequently $X_p = X_1$. Similarly, $Y[p]$ contains a submodule $Y_1 \simeq (J_p)^t$ where in fact $Y_1 = Y_p$.

In summary we have $Y_p \subseteq X_p$ where $Y_p \simeq (J_p)^t$ and $X_p \simeq (J_p)^s$. However, it is easy to show that Y_p and X_p are vector spaces over the field J_p of dimension t and s respectively. Hence Y_p is a subspace of X_p and must be of lower dimension. Thus $t \leq s$, as required.

Second step (to show that $n_t \leq m_s$): this is trivial, because if $X[p] = \bigoplus_{i=1}^{s} J_{p^{m_i}}$ and $m_1 \leq \cdots \leq m_s$, it follows that $p^{m_s}.X[p] = 0$.

Since $Y[p] \subseteq X[p]$, then obviously $p^{m_s}. Y[p] = (0)$. If $Y[p] = \bigoplus_{j=1}^{t} J_{p^{n_t}}$, where $n_1 \leq \ldots \leq n_t$, then if $r < n_t$, $p^r\ Y[p] \neq (0)$. Hence $m_s \geq n_t$.

Thus, $\sum_{j=1}^{t} n_j \leq t.n_t \leq s.m_s$, and we have proved that a submodule $Y[p]$ of $X[p]$ must fall in one or only a finite number of isomorphism classes. Taking into account the other p-modules in a direct sum decomposition of a F.G. torsion module X, we can prove the same result for submodules of X.

The last piece in establishing the descending chain conditions for F.G. torsion modules over P.I.D. consists of showing that: $Y \subseteq X$ and $Y \simeq X$ $\Rightarrow Y = X$. Thus if we have an infinite descending chain of submodules, then beyond a certain point in the chain all submodules must fall in the same isomorphism class. Applying the result that $Y \subseteq X$ and $Y \simeq X \Rightarrow Y = X$ will then establish our objective.

So assume that $Y \subseteq X$ and that both Y and X are isomorphic to $\bigoplus_p (\bigoplus_{i=1}^{m_p} J_{p^{m_i}})$. Choose any direct summand J_{p^m} and write $X \simeq Y \simeq J_{p^m} \oplus Z$. Let Y_z be the submodule of Y isomorphic to Z. Since $Y \subseteq X$, Y_z is also a submodule of X. Consider $X/Y_z \simeq Y/Y_z \simeq J_{p^m}$, and let β be the canonical epimorphism $\beta{:}X \to X/Y_z$. Now $\beta(Y) \subseteq \beta(X) = X/Y_z \simeq J_{p^m}$. But $\beta(Y) \simeq J_{p^m}$; in other words we have a module $\beta(X)$ isomorphic to J_{p^m} which contains a module $\beta(Y)$ also isomorphic to J_{p^m}.

We will show that $\beta(Y) = \beta(X)$. Both of these modules are cyclic since they are isomorphic to J_{p^m}: let g_1 generate $\beta(X)$ and let g_2 generate $\beta(Y)$. Since $\beta(Y) \subseteq \beta(X)$, we can write $g_2 = ng_1$ for some $n \in J$. Suppose p were a divisor of n, so that $n = kp$. Then $p^{m-1}g_2 = p^{m-1}ng_1 = p^{m-1}kpg_1 = kp^m g_1 = 0$, since $g_1 \in \beta(X) \simeq J_{p^m}$. But $p^{m-1}g_2 = 0$ implies that $p^{m-1}\beta(Y) = (0)$ contradicting the fact that $\beta(Y) \simeq J_{p^m}$. Hence p is not a divisor of n. Since p is prime, we have g.c.d.$\{n, p\} = 1$, and also we have g.c.d.$\{n, p^m\} = 1$. Since J is a P.I D., there exist $a, b \in J$ such that $an + bp^m = 1$. Now consider the equation $g_2 = ng_1$; we see that $ag_2 = ang_2 = (1-b.p^m)g_1 = g_1 - bp^m g_1 = g_1$. Thus $g_1 = ag_2$, some $a \in J$, and so $g_1 \in \beta(Y)$. Hence $\beta(X)$, which is generated by $g_{\cdot}$, is a submodule of $\beta(Y)$. Thus $\beta(Y) = \beta(X)$.

We now can show that $Y = X$, for otherwise (since $Y \subseteq X$) there exists $x \in X$ such that $x \notin Y$. Consider $\beta(x)$: $\beta(x) \in \beta(X) = \beta(Y)$, and so $\beta(x) = \beta(y)$ for some $y \in Y$. But then $\beta(x-y) = 0$, which implies that $x-y \in \ker \beta = Y_z$. But $Y_z \subseteq Y$, so $x-y \in Y$, and this implies that $x \in Y$, a contradiction. Hence $Y = X$.

In summary, we have just proved that for F.G. torsion modules over a P.I.D., if $Y \subseteq X$ and $Y \simeq X$, then $Y = X$. This last fact coupled with the result that the set of submodules of a given F G torsion module X over a P.I.D. J is partitioned into a finite number of isomorphism classes, yields the descending chain condition on such submodules. Q.E.D.

BIOGRAPHICAL NOTE

Robert deB Johnston was born on March 28, 1946, in Montreal, Quebec, Canada. He attended Bishop's College School in Lennoxville, Quebec, graduating in 1962. He entered McGill University on a University Scholarship and graduated from Electrical Engineering in 1968.

He started graduate studies in Electrical Engineering in the fall of 1968 at McGill University, where he was a research assistant until June 1970. At this point, having completed the research for the Master's degree, he left and resumed graduate work at the Massachusetts Institute of Technology. The Master's degree was awarded by McGill in June 1971.

In the time from September 1970 to June 1971, the author was a research assistant with Project MAC and with the Electronic Systems Laboratories.

In September 1967, he married the former Cathy Celeste Smith of Stuart, Florida. They have a daughter, Elise Rachel, born July 27, 1971.