Algebraic study of Discrete Multidimensional Signal processing

Naval Saini
SIT, GGS Indraprastha University,
Kashmere Gate, New Delhi 110096, India
Email: navalsaini@rediffmail.com

Abstract—**An abstract study of discrete multidimensional (MD) signal processing has been done by proving the theorems using results of group theory. We have covered some basic theorems of discrete MD signal processing, the perfect reconstruction (PR) property for MD delay chain systems and resulting periodicity upon decimation of periodic signals.**
Discrete MD signals are defined on domain of Z^d. Up-samplers and down-samplers form the ring of endomorphisms over Z^d. Many proofs also use the property that the ring of endomorphisms over Z^d is principally generated for the right and left ideals. Therefore, we have given interesting proofs the important properties.

Index terms—**algebra, discrete multidimensional signal processing, coprime integer matrices, multi-dimensional delay chains, periodicity.**

I. INTRODUCTION

Multidimensional signal processing is useful in processing complex data that are functions over domain having two or more dimensions, such as image and video data. Altering the sampling rate of data is done by are down-samplers (decimator matrix) and up-samplers (expander matrix) which endomorphic mappings on the domain space.
Many results of 1-D signal processing cannot be borrowed into multi-dimensional signal processing. This is due to the fact that MD is not commutative as compared to 1-D case, particularly the up-sampling and down-sampling. But, it also makes MD, a more interesting case for a study of algebraic structures.
MD sampling matrices appears in the paper as a ring of endomorphisms over an additive group of d-dimensional integers. When we limit to the center of this ring, commutatively holds among elements of sub-ring and many results of 1-d signal processing would apply. In the paper, we have discussed results which applicable to all elements, throughout the non-commutative ring (and in which the commutative center is embedded/sub-ring).
While the paper focuses on the properties of mathematical structures, the proofs of theorems are useful in addressing to problems, such as development of polyphase representation for rational sampling alterations, the prefect reconstruction properties of MD delay chain systems and the periodicity properties of decimated periodic signals. More is mentioned in [1],[2] possibly from a better engineering point of view. In comparison, the paper has exposed the mathematical structures that are underlying these theorems. It reviews the fundamental concepts of MD signal processing from point of view of algebra involved.
Section wise the contents are as follows. Section II focuses on understanding the basics involved, such as that the up-samplers and down-samplers form an un-commutative ring. Section III introduces properties of the ring mentioned before, which are useful in getting many results. The section IV is some basic theorems of MD signal processing, which needed to be redone to prove the efficacy of algebraically studying MD signal processing. Section V and section VI is about MD delay chain systems and decimation of periodic MD signals. There we have proved some theorems using results of group theory.
Appendix contains some more proofs. Appendix I illustrates the G-sets and conjugate class structures formed by left associates in the ring. Appendix II.gives the proof of property of the ring $End_Z(\eta)$ that it is principally generated for right ideals.

II. PRELIMINARIES

A. Domain of discrete MD signals

A non-periodic discrete MD function z varies over η.

$$z : \eta \rightarrow C \qquad \text{where } z \in F^*$$

F^* is the space of MD Signals and η is the chosen symbolic representation of $d \times 1$ integer matrices Z^d.

The properties of η are easily grasped.
1) η forms an abelian group under addition
2) Scalar multiplication is defines for η over the ring of integer Z

$Z \times \eta \rightarrow \eta$

This is sufficient to state that η forms module over Z.

A.1. Free Module η

Let $e_1 = [\ 1\ 0\ 0\ \ldots\ldots 0]^{T}_{d\times 1}$. Following the usual notations, define any e_i as a $d \times 1$ matrix where i^{th} element is 1 and all others are 0.

The set $\{ e_i \}_{i \in 1..d}$ forms a linearly independent set.

$\sum_{i=1..d} a_i e_i = 0$ where $a_i \in Z$

$\Rightarrow\ a_i = 0 \quad \forall\ i = 1..d$

Each of the e_i 's can generate over addition, disjoint groups which are isomorphic to Z. ∴Their linear combination is isomorphic to Z^d or η.

$$\oplus \sum_{i=1..d} a_i e_i \cong \eta$$

So, η is finitely generated free module. And the basis of η is the set $\{ e_i \}_{i=1..d}$.

The Endomorphism's over η and quotient spaces are of much use in the paper. Say **m** is an endomorphism on η, then **m(η)** forms a sub-module of η. The periodic MD signals are defined over quotient submodules of η. The diagram below shows the mappings of a periodic function to the image space C.

Free module → Quotient space → Field

η η(*m*) C

In this case, an MD periodic function defined over the quotient space is **m-periodic** (where m is the endomorphism). 'm-periodic' simply means that the function is defined over the domain η/*m*(η) or η(*m*) in short. If $z \in F^*_m$ is m-periodic then,

$$z(n) = z(m(\eta) + n) \quad \text{where } n \in \eta$$

The order of the quotient module η(*m*) is same as the dimensionality of vector space of periodic MD signals. An arbitrary basis element is of the latter is,

$$\delta_k(\eta) = \begin{cases} 1 & \text{where } \mathbf{k} - \mathbf{n} \in \mathbf{m}(\eta) \\ 0 & \text{otherwise} \end{cases}$$

B. Endomorphism's over η

All $End_Z(\eta)$ form a non-commutative ring. This is given in greater detail in [3].

i. It is an abelian group under addition.
ii. It is closed under multiplication. The multiplication is the composition of mappings of two endomorphisms and is a non abelian operation.
iii. Obeys the distributive properties.

Basically all $End_Z(\eta)$ are either 1-1 or ONTO or both.

i. Not 1-1 endomorphisms: Since these are not 1-1, Ø is proper subset of the kernel space. Say we take $f, g \in End_Z(\eta)$ such that,
   Image $g \subset$ kernel f
   Then $f \circ g\ (n) = 0 \quad \forall\ n \in \eta$
   $\Rightarrow\ f \cdot g = 0$
   Thus f & g are zero divisions in $End_Z(\eta)$. Similarly all endomorphisms which are not 1-1 zero divisors.
ii. 1-1 / not ONTO endomorphisms: These are 1 – 1 and not onto, so their multiplication inverse does not exist in $End_Z(\eta)$ as these mappings are non-isomorphic. These are non-zero, non–unit elements which do not have multiplicative inverses.
iii. 1–1 / ONTO endomorphisms: Since these endomorphisms are 1–1 and onto, they are isomorphic. Therefore, they have inverses, and are unity in the ring $End_Z(\eta)$.

These units (iii) form a non-commutative group of Aut (η) over multiplication (composition of mappings).

III. STRUCTURE OF THE RING

The proofs in this section have been provided for completeness of content and better understanding of the methods that we have used. We discuss principality of right and left ideals & anti-isomorphism, which arise from the structure of ring of endomorphisms (over the domain of MD signals). They come useful to us when we discuss and prove theorems related to polyphase implementations, MD delay chain systems, etc.

For instance since the ring is principally generated, we find that using co-prime elements from ring as expanders and decimators allows us to interchange their positions and use the noble identities as mentioned in [1]; this allows us to do processing at lowest rates (maximize parallel processing of MD signals).

A. Proof The ring $End_z(\eta)$ has all principally generated right ideals [2]

Let the ring $End_z(\eta)$ be given by R. For arbitrary f, $g \in R$; there exists an $h \in R$, s.t

$h R = f R + g R$

Thus $End_z(\eta)$ is principally generated for right

ideals.•

The proof for above theorem is given in Appendix I. The result will come useful many times in the paper. Some lemma's we can get from the proof above are.

Lemma 1 All right associates of h generate the same right ideal. If any $hr \in u\mathrm{R}$,

$h\,\mathrm{r} = (hu)(u^{-1}r)$ where u is a unit

$\Rightarrow h\,\mathrm{R} = hu\,\mathrm{R}$ for any unit $u \in \mathrm{R}$

Lemma 2 For any $f, g \in \mathrm{R}$, there $\exists$s an $h \in \mathrm{R}$, such that,

$h.\mathrm{R} = f.\mathrm{R} + g.\mathrm{R} \Leftrightarrow (h) = (f) + (g)$

Lemma 3 And if f & g are right co-prime in the ring R,

$\mathrm{R} = f.\mathrm{R} + g.\mathrm{R} \Leftrightarrow \eta = (f) + (g)$

B. The ring End$_z(\eta)$ is anti-isomorphic to itself.

Let, the **anti-isomorphism** on R be given by,

$$^{t}: \mathbf{R} \rightarrow \mathbf{R}$$

Integer Matrices is another representation for the ring $\mathrm{End}_z(\eta)$, which has mention in algebra books [3, 4]. Thus analogous to the transpose operation in Matrices, the ring of $\mathrm{End}_z(\eta)$ also has such anti-isomorphic mapping. •

C. <u>Proof</u> The ring End$_z(\eta)$ has all <u>principally generated right ideals</u>

For any arb. $f, g \in \mathrm{R}$, there exist its transpose $f^t, g^t \in \mathrm{R}$. Using the result from section A, that all right ideals are principally generated, $\exists$s some $h^t \in \mathrm{R}$,

$$h^t\mathrm{R} = f^t\mathrm{R} + g^t\mathrm{R}$$

Now, apply transpose (anti-isomorphism) to above,

$(h^t\mathrm{R})^t = (f^t\mathrm{R} + g^t\mathrm{R})^t$

$\Rightarrow \mathrm{R}h = \mathrm{R}f + \mathrm{R}g$ (as $\mathrm{R}^t = \mathrm{R}$)

ie, $\forall f, g \in \mathrm{R}$, $\exists$s $h \in \mathrm{R}$, such that

$$\mathrm{R}h = \mathrm{R}f + \mathrm{R}g$$

This proves $\mathrm{End}_z(\eta)$ is principally generated for left ideals. •

An independent proof of above (which does not use transpose and/or result in section A) is given on my website at www.freewebs.com/navalsaini [4]. It is posted for anyone to take a look, if interested in a proof for above (left ideal case) which does not use the ring being principally generated for right ideals or anti-isomorphism (transpose) as premise.

IV. MD PROCESSING THEOREMS

The theorems below are also a different approach to the theorems given in [1]. As we proceed with the proofs, we observe that the latter proofs which depend on initial ones seem to have become less complex. We also attempt to see if they reveal more about MD signal processing, than the original theorems have done.

Theorem 1 Images of anti-isomorphic elements in ring $\mathrm{End}_z(\eta)$ generate isomorphic quotient modules on η.

For any, $a \in \mathrm{R}$:-

$$\frac{\eta}{(a)} \cong \frac{\eta}{(a^t)}$$

Since, $(a) \cong (a^t)$, the proof follows.

The FPD generated by integer matrix and its transpose in η has the same elements, in [2].

Theorem 2 For any $a, x \in \mathrm{R}$,

$$\frac{\eta}{(a)} \cong \frac{(x)}{(xa)}$$

We get this from,

$$x: \eta \rightarrow (x)$$

also, $x: (a) \rightarrow (xa)$

If there is a certain element $n_1 \in \eta$, st.,

$n_1 + (\boldsymbol{a}) = (\boldsymbol{a}) \Leftrightarrow n_1 \in (\boldsymbol{a})$

$\Leftrightarrow x(n_1) \in (\boldsymbol{xa})$

$\Leftrightarrow x(n_1) + (\boldsymbol{xa}) = (\boldsymbol{xa})$

An isomorphism between the kernels proves that the isomorphism mentioned in the theorem holds. •

Theorem 3 When $m.p = l.q$ then,

$$\frac{(m)+(l)}{(m)\cap(l)} \cong \frac{(p^t)+(q^t)}{(p^t)\cap(q^t)}$$

Proof: Say,

$(m) + (l) = (x)$ and $(p^t) + (q^t) = (y^t)$

$\Rightarrow mp = lq = xay$

(We get above expression, as follows,

$\Rightarrow x\,m'\,p'\,y = x\,l'\,q'\,y$

for some $m', p', l', q' \in \mathrm{R}$

$\Rightarrow m'\,p' = l'\,q' = a$

for some $a \in \mathrm{R}$)

Now,

$$\frac{(x)}{(xa)} \cong \frac{\eta}{(a)} \cong \frac{\eta}{(a^t)} \cong \frac{(y^t)}{(y^t a^t)}$$

$$\Rightarrow \frac{(m)+(l)}{(m)\cap(l)} \cong \frac{(p^t)+(q^t)}{(p^t)\cap(q^t)} \bullet$$

Theorem 4 When, $r = mp = lq$. Then r = lcrm (m,l) if and only if p & q are right co-prime.

Equivalently we prove the following,

$(r) = (m) \cap (l) \quad \Leftrightarrow \quad (p^t) + (q^t) = \eta$

We will be utilizing previous theorems here.

Part I Assuming $(r) = (m) \cap (l)$

$$\frac{(m)+(l)}{(m)\cap(l)} \cong \frac{(m)}{(m)\cap(l)} \times \frac{(l)}{(m)\cap(l)}$$

$$\cong \frac{(m)}{(r)} \times \frac{(l)}{(r)}$$

$$\cong \frac{\eta}{(p)} \times \frac{\eta}{(q)} \quad \textit{(Using T2 \& T3, r=mp)}$$

$$\cong \frac{\eta}{(p^t)} \times \frac{\eta}{(q^t)} \quad \textit{(Using T1)} \quad \textbf{... 1}$$

$$\cong \frac{(m)+(l)}{(m)\cap(l)}$$

$$\cong \frac{(p^t)+(q^t)}{(p^t)\cap(q^t)} \cong \frac{(p^t)+(q^t)}{(p^t)} \times \frac{(p^t)+(q^t)}{(q^t)} \quad \textbf{... 2}$$

From 1 and 2 :-

$$\frac{\eta}{(p^t)} \times \frac{\eta}{(q^t)} \cong \frac{(p^t)+(q^t)}{(p^t)} \times \frac{(p^t)+(q^t)}{(q^t)}$$

$$\Rightarrow \quad (p^t)+(q^t) = \eta$$

This proves part I.

Part II Assuming $(p^t) + (q^t) = \eta$

$$\frac{(p^t)+(q^t)}{(p^t)\cap(q^t)} \cong \frac{(p^t)+(q^t)}{(p^t)} \times \frac{(p^t)+(q^t)}{(q^t)}$$

$$\cong \frac{\eta}{(p^t)} \times \frac{\eta}{(q^t)}$$

$$\cong \frac{\eta}{(p)} \times \frac{\eta}{(q)} \cong \frac{(m)}{(r)} \times \frac{(l)}{(r)} \quad \textbf{... 3}$$

$$\frac{(p^t)+(q^t)}{(p^t)\cap(q^t)} \cong \frac{(m)+(l)}{(m)\cap(l)} \cong \frac{(m)}{(m)\cap(l)} \times \frac{(l)}{(m)\cap(l)}$$

... 4

From 3 & 4 :-

$$\frac{(m)}{(r)} \times \frac{(l)}{(r)} \cong \frac{(m)}{(m)\cap(l)} \times \frac{(l)}{(m)\cap(l)}$$

$$\Rightarrow \quad (r) = (m) \cap (l)$$

This proves part II.

From part I and II we get theorem 4.

$(r) = (m)\cap(l) \quad \Leftrightarrow \quad (p^t) + (q^t) = \eta \qquad \bullet$

The next theorem is useful in extending the technique of rational polyphase decomposition (RPI) to MD signals, which finds applications in conversions of images or video data between sampling standards. In rational sampling rate alterations [1], the interchangeability of decimators and expanders allows us to perform each arithmetic operation at lowest rates using polyphase implementations. The following theorem gives us the conditions where such an interchange is allowed to be made, ie. l and m can be interchanged to achieve lowest rates. The premise in our theorem 5 (below) is the first condition that we require (for an interchange);

$$m.l^{-1} = l^{-1}.m \quad \Leftrightarrow \quad l.m = m.l$$

If it is given that they are interchangeable, then the premise ($l.m = m.l$) and the statements in the theorem below are implied, is given with proof in [1]. That is, interchangeability of expander and decimator (with no change) implies all of the mentioned in below theorem, ie. the premise and the four equivalent statements.

Theorem 5 When $m.l = l.m$, the following are equivalent,

1. $\mathbf{(l.m) = (l) \cap (m)}$
2. $(l^t) + (m^t) = \eta$
3. $\mathbf{(l) + (m) = \eta}$
4. $(l^t.m^t) = (l^t) \cap (m^t)$

Now we can take that, 1 $\Leftrightarrow$ 2 from the previous theorem 4 directly. The premise given matches the premise of theorem 4, (ie. $lm = ml$). Similarly, we can get 3 $\Leftrightarrow$ 4. The part to prove is that, 1 $\Leftrightarrow$ 3. First we are going to state a result from group theory, which we shall use.

$$\frac{(l)+(m)}{(l)} = \frac{(m)}{(l)\cap(m)} \quad \textbf{... 1}$$

The proof is simple,

$(l.m) = (m) \cap (l)$ (*Is 1 in above*)

$$\Leftrightarrow \frac{(l)+(m)}{(l)} = \frac{(m)}{(ml)}$$

(*substitute denominator RHS of 1,by above*)

$$\Leftrightarrow \frac{(l)+(m)}{(l)} = \frac{\eta}{(l)}$$

(*using Theorem 2*)

$\Leftrightarrow (l)+(m) = \eta$ (*Is 3 in above*)

Thus, 1 ⇔ 2 ⇔ 3 ⇔ 4. •

This also leads to the following result with more relaxed for commutativity (& interchangeability in RPI) than the above mentioned. Given m, $l \in$ R, we can always find m', $l' \in$ R, such that when interchanging the decimator l with expander m, we can get the same system by replacing the interchanged decimator with l' and expander with m' (that is, $l^{-1}.m = m'.l'^{-1}$) . Also for m', l' which are not right co-prime, we can always get right co-prime ones, by canceling their GCD's (or, the first principal ideal generator that contains of the right ideals generated by m' & l').

V. MD DELAY-CHAIN SYSYEMS

The figure 1 below is an MD delay chain system where input function is z and output function is z'. A perfect reconstruction MD delay chain is when the input function is replica of the output function, ie. (z = z' over all η).

The other components in parallel linear circuits are delays (where a line is delayed by same time magnitude with opposite signs, first when the signal is split and second when signal is concatenated) and decimators & upsamplers by a factor of $m \in \text{End}_z(\eta)$. The applications of MD delay chains are in designing of filter banks where the analysis and synthesis filters have certain symmetry; however these are not included in scope of presented work.

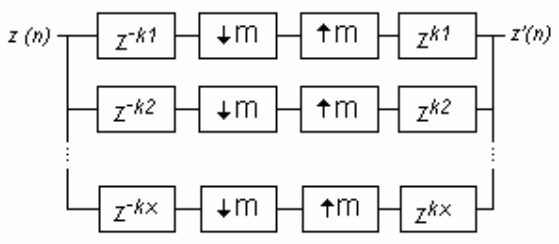

Figure 1 MD delay chain system with arbitrary delays

The MD delay chain system shown above is perfect reconstruction (PR) or z(n)=z'(n), for all n∈η; only when certain conditions are met about the choice of delays. For the above to be PR, we require that the set $\{k_i\}_{i=1..x}$ has a subset of which every element "k_i" belongs to every distinct coset in quotient space of $\eta /(m)$; where $m \in \text{End}_z(\eta)$. Thus the smallest of $\{k_i\}_{i=1..m}$, required for PR; is of cardinality $|\eta /(m)|$. For now, we shall assume that the set $\{k_i\}_{i=1..m}$ is such minimal set (which means $x = |\eta /(m)|$).

Now let us consider conditions for PR of an MD delay chain system, in which signal is delayed by an endomorphism (matrix) l (ie. $l \in \text{End}_z(\eta)$). Its drawing in Figure 2 is almost similar to figure 1. We will see that for PR, l may be chosen as the endomorphism which maps η to **group $\{k_i\}$** for k_i in **figure 1**, ie. (l) = group $\{k_i\}$.

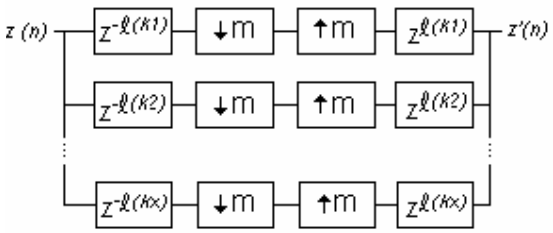

Figure 2 MD delay chain system with delay are by endomorphism; above $l \in \text{End}_z(\eta)$

Theorem 6 In an MD delay chain system such as given in figure 2, which is delayed by an $\boldsymbol{l} \in \text{End}_z(\eta)$ and sampled by $\boldsymbol{m} \in \text{End}_z(\eta)$, following conditions are equivalent;

P.R. ⇔ l & m are right co-prime

Proof:- Recall the result from group theory; G contains subgroups G_1 & G_2, then following are equivalent,

$G_1+G_2 = G \Leftrightarrow \{k + G_1 \mid k \in G_2\} = G_1/G$ **… 1**

We will use the above result, by exchanging a few symbols in 1. If l is the endomorphism which maps η to **group $\{k_i\}$**, ie. (l) = group $\{k_i\}$, where k_i are element from every distinct cosets of $\eta /(m)$, which is required for PR. Thus group (l) satisfies the conditions on RHS of 1 (above), so LHS is true. We prove below,

PR ⇔ $(l) + (m) = \eta$

We can further expand it,

⇔ $l.R + m.R = R$

⇔ ie. l & m are right co-prime •

VI. Decimation of Periodic Signals

An m-periodic signal is given as following:-

$z(n + (m)) = z (n)$

for all $n \in \eta$, where $m \in$ R

In case we decimate a periodic signal, we can expect to see a change in its periodicity. Suppose we decimate a periodic signal by l. Then let the new signal be given by z', where z' is now x-periodic.

$$z(l(n) + (m)) = z' (k + (x))$$
$$\text{for some } n, k \in \eta \text{ and } l, m, x \in R$$

Lets see how the periodicity is affected and how group theory can help us understand it better. Now G_1 and G_2 are groups in G on which our signal space can be defined. But lets stay focused on the fact that G_1 and G_2 are subgroups of G. Now consider the coset of G_1 in G.

$$\{ k + G_1 \mid k \in G \} = G / G_1$$

This is same as domain space of a periodic signal. Now, if we restrict the cosets to those being created from elements in G_2.

$$\{ k + G_1 \mid k \in G_2 \}$$

This is same as domain of the periodic signal formed by decimation of the signal periodic in G and defined on cosets of G_1 in G. Thus a further analysis shall be useful.

$$\{ k + G_1 \mid k \in G_2 \} = \frac{G_1+G_2}{G_1} = \frac{G_2}{G_1 \cap G_2}$$

Now in our case, finding existence of a group $X \subset G$; such that the new signal (z') is periodic in cosets of X in G as is in cosets of G_1 in G_1+G_2 (above).

$$\frac{G_1+G_2}{G_1} = \frac{G}{X}$$

A trivial case is when G_1 and G_2 are co-prime (*ie.* $G_1+G_2 = G$). In this case, X is same G_1 and there is no change in periodicity of our signal. In non-trivial cases, such an X may not exist in every group G; but in case of infinite abelian group η, such X will always exist. Let apply above to when our domain of MD-signal is η.

$$\frac{(m)+(l)}{(m)} = \frac{\eta}{X} \quad \text{, where } X = (x)$$

Let $(h) = (m)+(l)$. Then,

$$h: \eta \rightarrow (m)+(l)$$

also, $h: X \rightarrow (m)$ for some $X = (x)$

Thus, $x = h^{-1}.m$ which is the new periodicity for the m-periodic signal.

VII. APPENDIX I

A. Left Associates

Let N be the set of all subgroups of η and G be a set of all unit elements in R, ie. the group of automorphisms on η. The action of group G on the set N acts as a left G-set.

$u, v \in G$ and $A \in N$.

Say, $u * A = \{ u(a) \mid \forall a \in A \}$

Then, $u * v * A = u\ v * A$

For an arbitrary $u \in G$ and $A \in N$

i. $u.a_1 , u.a_2 \in u*A$ for some $a_1, a_2 \in A$
   $u\ a_1 + u\ a_2 = u (a_1+a_2) \in u*A$ because $a_1+a_2 \in A$
ii. $u.a \in u*A$ for some $a \in A$
   now, $a \in A \Rightarrow -a \in A$
   $\Rightarrow u(-a) = -u\ a \in u * A$

i and ii prove that $u*A \subset N$. So, there is a G-set action on N.

Proof A conjugate class formed in N is a set of all isomorphic subgroups of η.

Assume the $H \in N$ and H is isomorphic to A. Then we shall be proving that $H \sim A$ through the G-set action.

Since H & A are isomorphic subgroups of η. That is,

$$H \cong A \quad \& \quad \frac{\eta}{H} \cong \frac{\eta}{A}$$

Now, $$A \in N \Rightarrow \eta \cong A \times \frac{\eta}{A} \quad \dots \mathbf{1}$$

Similarly, $$H \in N \Rightarrow \eta \cong H \times \frac{\eta}{H} \quad \dots \mathbf{2}$$

From 1 and 2, we get the following mappings,

v_1: $A \rightarrow H$ is an isomorphism $\dots \mathbf{3}$

v_2: $\frac{\eta}{A} \rightarrow \frac{\eta}{H}$ is an isomorphism

We can combine $\mathbf{v_1}$ and $\mathbf{v_2}$, to get a mapping $\mathbf{v}$, such that,

$$\mathbf{v}: A \times \frac{\eta}{A} \rightarrow H \times \frac{\eta}{H} \quad \text{is an isomorphism}$$

$$\Rightarrow \quad v: \eta \rightarrow \eta$$

$\Rightarrow \quad v \in G \qquad \ldots \mathbf{4}$

$v: A \rightarrow H \quad \text{and} \quad v \in G$

$\Rightarrow \quad H = v * A$

$\Rightarrow \quad H \sim A$

Now we can make a statement that, for arbitrary $H \in N$ and is isomorphic to A, H and A belong to same conjugate class in the G-set on N. •

VIII. Appendix II

A. Proof The ring $End_z(\eta)$ has all principally generated right ideals [2]

Let the ring $End_z(\eta)$ be given by R. Take any $f, g \in R$

Also let (f) represent the image of endomorphism f. It is also a sub-module of η.

$f: \eta \rightarrow (f) \qquad \ldots \mathbf{1}$

(g) is defined similarly.

f.R is principally generated right ideal in R. Then $f.r \in$ f.R.

$f.r : \eta \rightarrow (f\,r) \quad \text{for any } r \in R \qquad \ldots \mathbf{2}$

$$\eta \xrightarrow{r} (r) \xrightarrow{f} (f.r)$$

$f : (r) \rightarrow (f.r) \in \text{End}(\eta) \qquad \ldots \mathbf{3}$

The image in *2* & *3* ie, $(f.r)$ is a submodule of η.

From mappings of 'f' is in *1* & *3* we get,

$\text{Dom}(1) \supset \text{Dom}(2) \Leftrightarrow \text{Img}(1) \supset \text{Img}(2)$

i.e., $\eta \supset (r) \Leftrightarrow (f) \supset (f\,r)$

Since $r \in R$ was arbitrary in the above equation's, we get :-

$(f\,R) \subset (f) \qquad \ldots \mathbf{4}$

$(g\,R) \subset (g) \qquad \ldots \mathbf{5}$

$(f) + (g)$ is a sub-module formed by the sum of sub-modules (elementary theorem).

$(f) + (g) \subset \eta$

Then there must exist an endomorphism η to $(f)+(g)$. Let it be given by $h \in R$

$h: \eta \rightarrow (f) + (g) = (h) \qquad \ldots \mathbf{6}$

We have assembled all that we will need to prove the theorem. In short, we will prove the result, $h.R = f.R + g.R$ (for the ring R to have principally generated right ideals).

$fR + gR$ is right ideal in R, $fr_1 + gr_2 \in fR+gR$ for arbitrary $r_1, r_2 \in R$.

$fr_1 + gr_2 : \eta \rightarrow (fr_1 + gr_2)$

Using 4, 5, 6 it is easy to get,

$(h) \supset (fr_1 + gr_2)$

Since, $h : \eta \rightarrow (h)$ is onto, there must exist a submodule $(r_3) \subset \eta$, when considered as domain for the endomorphism h maps onto $(fr_1 + gr_2)$.

$h: (r_3) \rightarrow (fr_1 + gr_2)$

And also for the sub-module $(r_3) \subset \eta$ there must exist an endomorphism $r_3 \in R$ st,

$r_3: \eta \rightarrow (r_3)$

$$\eta \xrightarrow{r_3} (r_3) \xrightarrow{h} (fr_1 + gr_2)$$

$\Rightarrow \quad h\,r_3 = f\,r_1 + g\,r_2$ for arb. $r_1, r_2 \in R$

$\Rightarrow \quad hR \supset fR+gR \quad$ for arb. $f, g \in R \qquad \ldots \mathbf{7}$

It remains to show that,

$h = f\,r + g\,s \quad$ for some $r, s \in R$

$\Rightarrow \quad h\,R \subset f\,R+g\,R \quad$ (we prove it next)

We know,

$(h) = (f) + (g)$

$\therefore\ h(e_i) = f(n_i) + g(m_i)$

where $e_i, n_i, m_i \in \eta \ \forall\ i = 1..d$

It is possible to find $r_i, s_i \in R$ such that,

$r_i(e_i) = n_i \quad \text{and} \quad s_i(e_i) = m_i$

If each of the r_i and s_i is an extension of the mapping r and s respectively, over the disjoint sub-modules $Z_i = gp(e_i)$ of η. The mappings r and s are defined over the domain η, ie. $r, s \in \text{End}(\eta)$.

$h(e_i) = f\,r(e_i) + g\,s(e_i) \quad \forall\ i = 1\ldots d$

$\Rightarrow \quad h = f\,r + g\,s$

$\Rightarrow \quad h\,R \subset f\,R + g\,R \qquad \ldots \mathbf{8}$

Together *7* and *8* imply,

$h\,R = f\,R + g\,R \quad$ for arb. $f, g \in R$

Thus $End_z(\eta)$ is principally generated for right ideals. •

VI. Conclusion

In this paper, we have formulated and solved various theorems related to discrete MD signal processing. We have attempted to demonstrate that algebraic structures formed are useful in solving these theorems. Many of our proofs use the property that the ring of endomorphisms over Z^d are principal left/right ideal rings.

Acknowledgement

I am extremely grateful to Professor S.D.Joshi (ECE, IIT Delhi) for guiding me through the study project. He is among the most motivated teachers, I have observed.

REFERENCES

[1] Chen, T. and Vaidyanathan, P. P., "The role of integer matrices in multidimensional multirate systems", *IEEE Trans. on Signal Processing*, vol. 41, no. 3, March 1993, pp. 1035-1047

[2] Chen, T. and Vaidyanathan, P. P., "Least common right/left multiples of integer matrices and applications to multidimensional multirate systems", *Proc. IEEE Int. Symp. on Circuits and Systems*, San Diego, May 1992, pp. 935-938.

[3] Basic Abstract Algebra, Cambridge University Press, (ISBN-10: 0521466296, ISBN-13: 9780521466295)

[4] www.freewebs.com/navalsaini *Proof that ring $End_z(\eta)$ has principally generated left ideals*

Naval Saini has completed Masters in Computer Applications (MCA) at the School of Information Technology (SIT), Main Campus of Guru Gobind Singh Indraprashta University, New Delhi in 2006.