Lecture 5: Minimality of Representation

Given a kernel representation matrix $R(\xi) \in \mathbb{R}^{g\times q}[\xi]$ we try to reduce the number of equations by creating zero-rows by means of left unimodular transformations (premultiplying $R(\xi)$ by unimodular matrices). This leads to the notion of *full row rank* representation.
A representation is called *minimal* if the number of rows is minimal among all possible equivalent representations i.e. the number of rows cannot be reduced any further.

We have already seen that various different kernel representation matrices can give rise to the same behavior. Recall that we have seen in the last lecture that if two kernel representation matrices, say $R_1(\xi)$ and $R_2(\xi)$ are related by $R_2(\xi) = U(\xi)R_1(\xi)$, where $U(\xi)$ is unimodular, then the two behaviors, $\mathfrak{B}_1 = \ker R_1(\frac{d}{dt})$ and $\mathfrak{B}_2 = \ker R_2(\frac{d}{dt})$ are equal. Now, notice that if $R_2(\xi) = U(\xi)R_1(\xi)$ then the rows of the two matrices span the same spce over $\mathbb{R}[\xi]$! Let us make this idea precise. We first define the *row-span* of a polynomial matrix. The *row-span* of a polynomial matrix $R(\xi)$ is the collestion of all polynomial row vectors that can be obtained as polynomial linear combinations of the rows of $R(\xi)$. This set is denoted by $\mathcal{R}$. The set $\mathcal{R}$ has the structure of a *module* over the ring $\mathbb{R}[\xi]$.

Definition 1. Module: *Let $\mathcal{A}$ be a ring. An $\mathcal{A}$-module (or a module over $\mathcal{A}$) is a non-empty set $\mathcal{M}$ with the operations $+$ and $.$ such that*

1. *$\mathcal{M}$ is an abelian group with respect to $(+)$ addition.*
2. *For $m \in \mathcal{M}$ and $a \in \mathcal{A}$, $a.m \in \mathcal{M}$.*
3. *For $x, y \in \mathcal{M}$ and $a, b \in \mathcal{A}$ the following relations hold,*
   - *(a) $.$ distributes over $+$ i.e. $a.(x + y) = a.x + a.y$*
   - *(b) $+$ distributes over $.$ i.e. $(a + b).x = a.x + b.x$*
   - *(c) $(a.b).x = a.(b.x)$*
   - *(d) If there exists an identity element 1, such that $1.x = x$ for all $x \in \mathcal{M}$, then $\mathcal{M}$ is said to be a* unitary *module.*

Note that the row-span of $R(\xi) \in \mathbb{R}^{g\times q}[\xi]$ is a subset of $\mathbb{R}^{1\times q}[\xi]$. It can be easily checked that $\mathbb{R}^{1\times q}[\xi]$, too, is a module over $\mathbb{R}[\xi]$. Thus, $\mathcal{R}$, the row-span of $R(\xi)$, is actually a *sub-module* of the bigger module $\mathbb{R}^{1\times q}[\xi]$. (A submodule is a subset of a module that is a module in its own right.) Since the submodule $\mathcal{R}$ comes from a set of differential equations it is called an *equation module.*

Example 1: Consider the kernel representation matrix given by

$$R(\xi) = \begin{bmatrix} p_{11}(\xi) & p_{12}(\xi) & p_{13}(\xi) & p_{14}(\xi) \\ p_{21}(\xi) & p_{22}(\xi) & p_{23}(\xi) & p_{24}(\xi) \\ p_{31}(\xi) & p_{32}(\xi) & p_{33}(\xi) & p_{34}(\xi) \end{bmatrix} = \begin{bmatrix} r_1(\xi) \\ r_2(\xi) \\ r_3(\xi) \end{bmatrix}$$

The equation module for this situation is

$$\mathcal{R} = \left\{ r(\xi) \in \mathbb{R}^{1\times q}[\xi] \mid r(\xi) = \sum_{i=1}^{q} a_i(\xi) r_i(\xi), \text{ where } a_i(\xi) \in \mathbb{R}[\xi] \text{ for all } i = 1, 2, \ldots, q \right\}.$$

Example 2: Consider the kernel representation of a scalar behavior given by the differential equations

$$\begin{aligned} \frac{dw}{dt} + w &= 0 \\ \frac{d^2w}{dt^2} + w &= 0 \\ \Rightarrow R(\xi) &= \begin{bmatrix} \xi + 1 \\ \xi^2 + 1 \end{bmatrix} \end{aligned} \tag{1}$$

The rowspan of $R(\xi)$ is a module over $\mathbb{R}[\xi]$. The equation module $\mathcal{R}$ is given by the polynomial combination of the rows as

$$\mathcal{R} = \left\{ a(\xi)(\xi+1) + b(\xi)(\xi^2+1) | a(\xi), b(\xi) \in \mathbb{R}[\xi] \right\} \subseteq \mathbb{R}[\xi]$$

Note that this is the *ideal* generated by $(\xi + 1)$ and $(\xi^2 + 1)$. This ideal is often represented as $\langle (\xi + 1) \ , \ (\xi^2 + 1) \rangle$.

Definition 2. Ideal: *Let $\mathcal{A}$ be a ring. An ideal in $\mathcal{A}$ is a non-empty subset $\mathfrak{a}$ of $\mathcal{A}$ with the operations $+$ and $.$ such that*

1. *If $a_1, a_2 \in \mathfrak{a}$ then, $a_1 + a_2 \in \mathfrak{a}$*
2. *If $a \in \mathfrak{a}$ and $c \in \mathcal{A}$ then, $c.a \in \mathfrak{a}$*

An ideal in $\mathcal{A}$ is clearly an $\mathcal{A}$-module.

Knowing the concept of modules enables us to restate Theorem 1 of Lecture 4 in the language of modules.

Theorem 3. *Consider two behaviors given in kernel representations as*

$$\mathfrak{B}_1 = \ker \ R_1(\frac{d}{dt}), \quad \mathfrak{B}_2 = \ker \ R_2(\frac{d}{dt}).$$

Suppose the two equation modules $\mathcal{R}_1$ and $\mathcal{R}_2$ are equal, that is, $\mathcal{R}_1 = \mathcal{R}_2$. Then $\mathfrak{B}_1 = \mathfrak{B}_2$.

Proof: First note that $\mathcal{R}_1 \subseteq \mathcal{R}_2$. This means every row of $R_1(\xi)$ is a polynomial linear combination of the rows of $R_2(\xi)$. Hence, there exists a matrix $F(\xi)$ of proper size such that $R_1(\xi) = F(\xi)R_2(\xi)$. It then easily follows that $w \in \ker \ R_2(\frac{d}{dt})$ implies $w \in \ker \ R_1(\frac{d}{dt})$. In other words, $\mathfrak{B}_2 \subseteq \mathfrak{B}_1$.

Now noting that $\mathcal{R}_2 \subseteq \mathcal{R}_1$ and running the exactly same chain of arguments with roles of $\mathcal{R}_1$ and $\mathcal{R}_2$ reversed, we get that there exists $\widetilde{F}(\xi)$ such that $R_2(\xi) = \widetilde{F}(\xi)R_1(\xi)$. It then follows that $\mathfrak{B}_1 \subseteq \mathfrak{B}_2$. Hence, $\mathfrak{B}_1 = \mathfrak{B}_2$. □

To understand the strength of the module theoretic description of equations, consider the behavior given by equation (1) in Example 2. Here the equation ideal is generated by $\xi + 1$ and $\xi^2 + 1$. Notice that

$$\xi^2 + 1 - (\xi - 1)(\xi + 1) = 2.$$

Now every $w \in \mathfrak{B}$ satisfies $(\frac{d}{dt} + 1)w = 0$ and $\frac{d^2}{dt^2}w + 1 = 0$. Therefore, for every $w \in \mathfrak{B}$ we must have

$$\begin{aligned} (\frac{d^2}{dt^2} + 1)w - (\frac{d}{dt} - 1)(\frac{d}{dt} + 1)w &= 2w \\ \Rightarrow \ 0.w &= 2w \\ \Rightarrow \ w &= 0. \end{aligned}$$

Since $w \in \mathfrak{B}$ was arbtrary, it means that $\mathfrak{B} = \{0\}$. The important thing to notice in this example is that here the equation ideal contains 2 and therefore it contains the ideal generated by 2. But, 2 generates the whole ring as an ideal. Therefore, the equation ideal here is the whole ring $\mathbb{R}[\xi]$. Therefore, the behavior must be equal to the behavior corresponding to the whole ring, which is the zero behavior.

The next theorem is a well-known result from commutative algebra. It shows that if there is an ideal that is generated by two polynomials then the same ideal is generated by a single polynomial, namely, the gcd of the two generating polynomials.

Theorem 4. *Let $p(\xi)$, $q(\xi) \in \mathbb{R}[\xi]$. Then the ideal generated by $p(\xi)$ and $q(\xi)$ is equal to the ideal generated by $g(\xi)$ where $g = g.c.d(p, q)$*

Proof: To show $< g > \subseteq < p, q >$
Since $g(\xi)$ is the g.c.d of $p(\xi)$ and $q(\xi)$ we have by *Aryabhatta identity* that there exists polynomials $a(\xi)$ and $b(\xi) \in \mathbb{R}[\xi]$ such that $g = a(\xi)p(\xi) + b(\xi)q(\xi)$. Thus $g(\xi) \in < p(\xi), q(\xi) >$. Any multiple of $g(\xi)$ is also generated by $< p(\xi), q(\xi) >$. Therefore, $< g > \subseteq < p, q >$.
To show $< p, q > \subseteq < g >$
Ideals generated by $p(\xi)$ will be of the form $c(\xi)p(\xi)$ where $c(\xi) \in \mathbb{R}[\xi]$. Since g is the g.c.d of p, p is some polynomial multiple of g, i.e. $p(\xi) = p_1(\xi)g(\xi)$. Similarly, $q(\xi) = q_1(\xi)g(\xi)$. Therefore $a(\xi)p(\xi) + b(\xi)q(\xi) = (a(\xi)p_1(\xi) + b(\xi)q_1(\xi))g(\xi)$.
Since both sides inclusion holds, $< p(\xi), q(\xi) > = < g(\xi) >$. □

Example: Let the describing equations of a dynamical system be

$$\frac{d^2w}{dt^2} + 3\frac{dw}{dt} + 2w = 0$$
$$\frac{d^3w}{dt^3} + 6\frac{d^2w}{dt^2} + 11\frac{dw}{dt} + 6w = 0$$

The kernel representation matrix is given by $R(\xi) = \begin{bmatrix} \xi^2 + 3\xi + 2 \\ \xi^3 + 6\xi^2 + 11\xi + 6 \end{bmatrix} w = 0$. The rows $r_1(\xi)$ and $r_2(\xi)$ are not coprime. They can be factored as $r_1(\xi) = (\xi + 1)(\xi + 2)$ and $r_2(\xi) = (\xi + 1)(\xi + 2)(\xi + 3)$. Thus the behavior of this system will be given by (the g.c.d of the two polynomials) $(\xi^2 + 3\xi + 2)w = 0$.

Thus we have found a systematic procedure of calculating the minimal representation of a system with one variable.
When the number of variables are q, i.e. the signal space $\mathbb{W} = \mathbb{R}^q$, the kernel representation matrix $R(\xi)$ is a matrix with q columns and the g.c.d condition is not applicable for that case. To get a zero row we could have used the algorithm for upper-triangularization but that would be too cumbersome and computationally expensive. The following theorem gives a better approach for producing a zero row if the matrix has dependent rows.

Theorem 5. *Let $a_1(\xi), a_2(\xi), \ldots, a_k(\xi) \in \mathbb{R}[\xi]$ and assume that $a_1(\xi), a_2(\xi), \ldots, a_k(\xi)$ are coprime (have no common factors). Then there exists a unimodular matrix $U(\xi) \in \mathbb{R}^{k \times k}[\xi]$ such that the last row of $U(\xi) = \begin{bmatrix} a_1(\xi) & a_2(\xi) & \ldots & a_k(\xi) \end{bmatrix}$*

If

$$R(\xi) = \begin{bmatrix} r_1(\xi) \\ r_2(\xi) \\ \vdots \\ r_k(\xi) \end{bmatrix} \qquad R(\xi) \in \mathbb{R}^{k \times q}[\xi]$$

and the rows are dependent then from the definition of dependence, there exists polynomials $a_i(\xi) \in \mathbb{R}[\xi]$ not all zero, such that $\sum_{i=1}^{k} a_i(\xi) r_i(\xi) = 0$. We can safely say that $a_i(\xi)$ are coprime because if they are not then we can pull out the gcd of the $a_i(\xi)$ and have

$$\begin{aligned} g(\xi) \sum_{i=1}^{k} \widetilde{a}_i(\xi) r_i(\xi) &= 0 \\ \Rightarrow \sum_{i=1}^{k} \widetilde{a}_i(\xi) r_i(\xi) &= 0. \end{aligned}$$

Since $g(\xi)$ was the gcd of $a_i(\xi)$, the polynomials $\widetilde{a}_i(\xi)$'s must be coprime.

Therefore, pre-multiplying $R(\xi)$ with $U(\xi)$ ensures $U(\xi)R(\xi) = \begin{bmatrix} \tilde{R}(\xi) \\ 0 \end{bmatrix}$ where $\tilde{R}(\xi) \in \mathbb{R}^{k-1 \times q}[\xi]$. We have succeeded in creating a zero row in the kernel representation matrix by assuming that the unimodular matrix has $a_1(\xi)a_2(\xi)\dots a_k(\xi)$ as the last row. Now the aim is to complete the matrix $U(\xi)$ such that $U(\xi)$ is unimodular. This is known as the *Matrix Completion Problem.*

Proof: Let $a(\xi) = \begin{bmatrix} a_1(\xi) & a_2(\xi) & \dots & a_k(\xi) \end{bmatrix}$. Take the minimal degree polynomial of $a(\xi)$. Using this polynomial divide the other polynomials using long division. This is equivalent to right multiplication by a unimodular matrix $V_1(\xi)$. Now take the polynomial of minimal degree from $a(\xi)V_1(\xi)$ and repeat the procedure. This is again a postmultiplication by a unimodular matrix $V_2(\xi)$. After repeating this procedure a finite number of times, we get $a(\xi)V_1(\xi)V_2(\xi)\dots V_{n-1}(\xi) = \begin{bmatrix} m(\xi) & 0 & \dots & 0 \end{bmatrix}$. By postmultiplying by a permutation matrix V_n we finally get $a(\xi)V_1(\xi)V_2(\xi)\dots V_{n-1}(\xi)V_n(\xi) = \begin{bmatrix} 0 & 0 & \dots & m(\xi) \end{bmatrix}$. Since all $a_i(\xi)$ were coprime $m(\xi)$ must be a non-zero constant polynomial. Defining $V(\xi) = V_1(\xi)V_2(\xi)\dots V_{n-1}(\xi)V_n(\xi)$, $a(\xi)V(\xi) = \begin{bmatrix} 0 & 0 & \dots & m(\xi) \end{bmatrix}$. Since the inverse of a unimodular matrix is unimodular, let $V^{-1}(\xi) = U(\xi)$ therefore $r(\xi) = \begin{bmatrix} 0 & 0 & \dots & 1 \end{bmatrix} U(\xi)$. This implies that the last row of $U(\xi)$ is $r(\xi)$ and all other entries are also calculated using $V^{-1}(\xi)$. □

So far we have seen two methods of converting a row dependent kernel representation matrix into full row rank matrices by i) upper-triangularization and ii) making zero rows at the bottom which can easily be discarded. Both the methods involve premultiplication by unimodular matrices. Combining this with postmultiplication one can reduce a polynomial matrix into a diagonal matrix. This would be quite helpful in solving polynomial differential equations because the equations would then be decoupled and easier to solve.

However, since this would involve column operations, such a reduction would change the solution set, and we cannot say that the behavior of the reduced set of equations would be the same. This issue will be addressed later. First we give a constructive proof for the diagonal representation form which is known as the *Smith canonical form* (in short, SCF), where $U(\xi)R(\xi)V(\xi) =$ diag $(d_1(\xi), d_2(\xi), \dots, d_r(\xi)$ where r is the rank of the kernel representation matrix $R(\xi)$.

Theorem 6. *Let $R(\xi) \in \mathbb{R}^{g \times q}[\xi]$ be the kernel representation matrix. There exists unimodular matrices $U(\xi) \in \mathbb{R}^{g \times g}[\xi]$ and $V(\xi) \in \mathbb{R}^{q \times q}[\xi]$ such that*

$$U(\xi)R(\xi)V(\xi) = \left[\begin{array}{ccc|c} d_1(\xi) & & & \\ & d_2(\xi) & & \\ & & \ddots & \mathbf{0_{r \times (q-r)}} \\ & & d_r(\xi) & \\ \hline & \mathbf{0_{(g-r) \times r}} & & \mathbf{0_{(g-r) \times (q-r)}} \end{array}\right]$$

where r is the number of linearly independent rows of the matrix (which is equal to the rank of the matrix).

Proof: Choose the element of least degree from $R(\xi)$. Apply row and column permutations to bring this element at the (1, 1) position. This involves pre and postmultiplication by unimodular matrices. Use the element of minimal degree to divide the entries along the first column of $R(\xi)$. This involves premultiplication by unimodular matrices. Similarly carry out divisions of the elements in the first row (postmultiplying by unimodular matrices). In the first pass the degree of the elements in the first row and column is reduced by atleast one. Select the element of least degree among the entries of the first row and column and bring it to the (1,1) position by column and(or) row permutaions. Divide the remaining entries both column wise and row wise with this element. Again the degree of the elements is reduced by atleast one. This process continues when there are two nonzero elements in the first row or column. Since the degrees are nonnegative after a finite number of steps the first row and the first column becomes zero as

$$\begin{bmatrix} d_1(\xi) & 0 & \dots & 0 \\ 0 & a_{22}(\xi) & \dots & a_{2q}(\xi) \\ \vdots & \vdots & \ddots & \\ 0 & a_{g2}(\xi) & \dots & a_{gq}(\xi) \end{bmatrix}$$

with the (1,1) element being nonzero and minimal.
Apply the procedure iteratively for the $(g-1) \times (q-1)$ submatrix. By submatrix we mean the matrix excluding the reduced rows and columns (here only the first row and column is excluded). The minimal degree is now placed at (2,2) position with the other entries of the second row and second column brought to zero. Applying the procedure for subsequent submatrices we get a diagonal form as

$$\begin{bmatrix} d_1(\xi) & 0 & \dots & \dots & \\ 0 & d_2(\xi) & 0 & \dots & \\ \vdots & 0 & d_r(\xi) & 0 & \\ \vdots & \vdots & 0 & \ddots & \\ 0 & 0 & 0 & \dots & 0 \end{bmatrix}$$

□

As mentioned previously since the reduction of the kernel representation matrix to the Smith canonical form involves column operations the solution set (behavior) does not remain the same, unlike upper-triangularization which involved only row operations. The question now is how does the behavior change? The claim is the behavior is isomorphic which is proved in the following theorem.

Theorem 7. *Given a behavior $\mathfrak{B}$ represented by $R(\frac{d}{dt})w = 0$. The kernel representation matrix is transformed to the diagonal form $D(\xi)$ by left and right unimodular matrices as $U(\xi)R(\xi)V(\xi) = D(\xi)$. If the behavior given by $D(\xi)$ is $\tilde{\mathfrak{B}}$, then the behaviors $\mathfrak{B}$ and $\tilde{\mathfrak{B}}$ are isomorphic.*

Proof: Considering the original kernel representation

$$R(\frac{d}{dt})w = 0$$

After transformation the behaviour changes, $\tilde{w}$ represented the new behavior. Therefore,

$$D(\frac{d}{dt})\tilde{w} = 0$$
$$U(\xi)R(\xi)V(\xi)\tilde{w} = 0$$

Premultiplication doesnot change the behavior, thus

$$\bar{R}(\xi)V(\xi)\tilde{w} = 0$$

where $\bar{R}(\xi) = U(\xi)R(\xi)$. By a slight abuse of notation we write $R(\xi) = \bar{R}(\xi)$. By defining $\tilde{w} := V^{-1}(\xi)w$ we get

$$R(\xi)V(\xi)V^{-1}(\xi)w = 0$$
$$R(\xi)w = 0$$

Therefore to show that the behaviors are isomorphic we need to show the map

$$V^{-1}(\frac{d}{dt}) : \mathfrak{B} \to \tilde{\mathfrak{B}} \tag{2}$$

is bijective, i.e. both injective (one-to-one) and surjective(onto) where $\tilde{\mathfrak{B}} := \ker R(\frac{d}{dt})V(\frac{d}{dt})$. To show the map is surjective means for every $\tilde{w} \in \tilde{\mathfrak{B}}$ there exists a $w \in \mathfrak{B}$.

$$w := V(\frac{d}{dt})\tilde{w}$$

or

$$V^{-1}(\frac{d}{dt})w = V^{-1}(\frac{d}{dt})V(\frac{d}{dt})\tilde{w} = \tilde{w}$$

This show the map is surjective.
To show the map is injective we use the method of contradiction.
Suppose the map is not injective, implies there exists $w_1, w_2 \in \mathfrak{B}$ and $w_1 \neq w_2$ such that

$$V^{-1}(\frac{d}{dt})w_1 = V^{-1}(\frac{d}{dt})w_2$$
$$V^{-1}(\frac{d}{dt})(w_1 - w_2) = 0$$

Premultiplying by a unimodular matrix $V(\frac{d}{dt})$ we get $w_1 = w_2$ which is a contradiction to the assumed fact that $w_1 \neq w_2$. Thus the assumption is false and the map is indeed injective.
Since both injectivity and surjectivity holds the map is known as a bijective map and hence an isomorphism. □