THE PREDICTABLE DEGREE PROPERTY AND A PARAMETRIZATION OF ANNIHILATORS OF A BEHAVIOR OVER A FINITE RING

Margreta Kuijper\textsuperscript{1}  Raquel Pinto\textsuperscript{2}  Jan Willem Polderman\textsuperscript{3}

\textsuperscript{1}Department of Electrical and Electronic Engineering  
University of Melbourne

\textsuperscript{2}Department of Mathematics  
University of Aveiro

\textsuperscript{3}Department of Applied Mathematics  
University of Twente

LinSys 2007, Canberra
SYSTEMS OVER FINITE ALGEBRAS—WHY?

- ↔ coding theory:
  - convolutional codes as linear systems over a finite algebra
    - Rosenthal a.o. ’96; Gluesing a.o. ’06; Fornasini & Pinto ’04
    - Massey a.o. ’89; Johannesson a.o. ’98
  - decoding of Reed-Solomon codes = iterative modeling of behaviors over a finite algebra, see Kuijper & Willems ’97; Kuijper & Polderman ’04

- ↔ sequence theory:
  - complexity of sequences of elements from a finite algebra ↔ minimal partial realization of impulse response
SYSTEMS OVER FINITE ALGEBRAS—WHY?

- \( \leftrightarrow \) coding theory:
  - convolutional codes as linear systems over a finite algebra
    - Rosenthal a.o. '96; Gluesing a.o. '06; Fornasini & Pinto '04
    - Massey a.o. '89; Johannesson a.o. '98
  - decoding of Reed-Solomon codes = iterative modeling of behaviors over a finite algebra, see Kuijper & Willems '97; Kuijper & Polderman '04

- \( \leftrightarrow \) sequence theory:
  - complexity of sequences of elements from a finite algebra \( \leftrightarrow \) minimal partial realization of impulse response
SYSTEMS OVER FINITE ALGEBRAS—WHY?

• \(\leftrightarrow\) coding theory:
  
  • convolutional codes as linear systems over a finite algebra
    
    • Rosenthal a.o. ’96; Gluesing a.o. ’06; Fornasini & Pinto ’04
    
    • Massey a.o. ’89; Johannesson a.o. ’98

  • decoding of Reed-Solomon codes = iterative modeling of behaviors over a finite algebra, see Kuijper & Willems ’97; Kuijper & Polderman ’04

• \(\leftrightarrow\) sequence theory:

  • complexity of sequences of elements from a finite algebra\(\leftrightarrow\) minimal partial realization of impulse response
SYSTEMS OVER FINITE ALGEBRAS—WHY?

• $\leftrightarrow$ coding theory:
  
  • **convolutional codes** as linear systems over a finite algebra
    
    • *Rosenthal a.o. ’96; Gluesing a.o. ’06; Fornasini & Pinto ’04*
    
    • *Massey a.o. ’89; Johannesson a.o. ’98*

  • decoding of Reed-Solomon codes = iterative modeling of behaviors over a finite algebra, see *Kuijper & Willems ’97; Kuijper & Polderman ’04*

• $\leftrightarrow$ sequence theory:
  
  • complexity of sequences of elements from a finite algebra $\leftrightarrow$ minimal partial realization of impulse response
SYSTEMS OVER FINITE ALGEBRAS—WHY?

• $\leftrightarrow$ coding theory:
  
  • **convolutional codes** as linear systems over a finite algebra
    • *Rosenthal a.o.* ’96; *Gluesing a.o.* ’06; *Fornasini & Pinto* ’04
    • *Massey a.o.* ’89; *Johannesson a.o.* ’98
  
  • **decoding** of Reed-Solomon codes = iterative modeling of behaviors over a finite algebra, see *Kuijper & Willems* ’97; *Kuijper & Polderman* ’04

• $\leftrightarrow$ sequence theory:
  
  • **complexity** of sequences of elements from a finite algebra$\leftrightarrow$ minimal partial realization of impulse response
SYSTEMS OVER FINITE ALGEBRAS—WHY?

- **<--> coding theory:**
  - **convolutional codes** as linear systems over a finite algebra
    - Rosenthal a.o. ’96; Gluesing a.o. ’06; Fornasini & Pinto ’04
    - Massey a.o. ’89; Johannesson a.o. ’98
  - **decoding** of Reed-Solomon codes = iterative modeling of behaviors over a finite algebra, see Kuijper & Willems ’97; Kuijper & Polderman ’04

- **<--> sequence theory:**
  - **complexity** of sequences of elements from a finite algebra <-> minimal partial realization of impulse response
• Example over field \( \mathbb{Z}_{11} \): \( B = \text{span} \left\{ \left[ \begin{array}{c} 9 \\ 0 \end{array} \right], \left[ \begin{array}{c} 0 \\ 1 \end{array} \right], \left[ \begin{array}{c} 0 \\ 0 \end{array} \right], \ldots \right\} \)

• has kernel representation \( A(\sigma)w = 0 \) with

\[
A(\xi) = \begin{bmatrix} 0 & \xi^2 \\ 1 & 2\xi \end{bmatrix}
\]

• \( A \) is not row reduced since leading row coefficient matrix

\[
A^{\text{lrc}} = \begin{bmatrix} 0 & 1 \\ 0 & 2 \end{bmatrix}
\]

• Any other representation \( R(\sigma)w = 0 \) of \( B \) with \( R(\xi) \) of full row rank is given by \( R(\xi) = U(\xi)A(\xi) \) with \( U(\xi) \) unimodular

• Row reduction procedure of Wedderburn ’34; Wolovich ’74 yields

\[
U(\xi)A(\xi) = \begin{bmatrix} \xi & 0 \\ 1 & 2\xi \end{bmatrix} \text{ for } U(\xi) = \begin{bmatrix} 9 & \xi \\ 0 & 1 \end{bmatrix}
\]

• Thus minimal row degrees are 1, 1.
• Example over field \( \mathbb{Z}_{11} \): \( \mathcal{B} = \text{span} \{ \begin{bmatrix} 9 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \ldots \} \)

• has kernel representation \( A(\sigma)w = 0 \) with

\[
A(\xi) = \begin{bmatrix} 0 & \xi^2 \\ 1 & 2\xi \end{bmatrix}
\]

• \( A \) is not row reduced since leading row coefficient matrix \( A^{\text{lrc}} = \begin{bmatrix} 0 & 1 \\ 0 & 2 \end{bmatrix} \)

• Any other representation \( R(\sigma)w = 0 \) of \( \mathcal{B} \) with \( R(\xi) \) of full row rank is given by \( R(\xi) = U(\xi)A(\xi) \) with \( U(\xi) \) unimodular

• Row reduction procedure of Wedderburn ’34; Wolovich ’74 yields

\[
U(\xi)A(\xi) = \begin{bmatrix} \xi & 0 \\ 1 & 2\xi \end{bmatrix}
\]

for \( U(\xi) = \begin{bmatrix} 9 & \xi \\ 0 & 1 \end{bmatrix} \)

• Thus minimal row degrees are 1, 1.
• Example over field $\mathbb{Z}_{11}$: $B = \text{span}\left\{\left(\begin{array}{c} 9 \\ 0 \end{array}\right), \left(\begin{array}{c} 0 \\ 1 \end{array}\right), \left(\begin{array}{c} 0 \\ 0 \end{array}\right), \ldots\right\}$

• has kernel representation $A(\sigma)w = 0$ with

$$A(\xi) = \begin{bmatrix} 0 & \xi^2 \\ 1 & 2\xi \end{bmatrix}$$

• $A$ is not row reduced since leading row coefficient matrix

$$A^{\text{lrc}} = \begin{bmatrix} 0 & 1 \\ 0 & 2 \end{bmatrix}$$

• Any other representation $R(\sigma)w = 0$ of $B$ with $R(\xi)$ of full row rank is given by $R(\xi) = U(\xi)A(\xi)$ with $U(\xi)$ unimodular

• Row reduction procedure of Wedderburn ’34; Wolovich ’74 yields

$$U(\xi)A(\xi) = \begin{bmatrix} \xi & 0 \\ 1 & 2\xi \end{bmatrix} \text{ for } U(\xi) = \begin{bmatrix} 9 & \xi \\ 0 & 1 \end{bmatrix}$$

• Thus minimal row degrees are 1, 1.
• Example over field $\mathbb{Z}_{11}$: $\mathcal{B} = \text{span} \{ \left( \begin{array}{c} 9 \\ 0 \end{array} \right), \left( \begin{array}{c} 0 \\ 1 \end{array} \right), \left( \begin{array}{c} 0 \\ 0 \end{array} \right), \ldots \}$. 

• has kernel representation $A(\sigma)w = 0$ with 

$$A(\xi) = \left[ \begin{array}{cc} 0 & \xi^2 \\ 1 & 2\xi \end{array} \right]$$

• $A$ is not row reduced since leading row coefficient matrix 

$$A^{\text{lrc}} = \left[ \begin{array}{cc} 0 & 1 \\ 0 & 2 \end{array} \right]$$

• Any other representation $R(\sigma)w = 0$ of $\mathcal{B}$ with $R(\xi)$ of full row rank is given by $R(\xi) = U(\xi)A(\xi)$ with $U(\xi)$ unimodular 

• Row reduction procedure of Wedderburn '34; Wolovich '74 yields 

$$U(\xi)A(\xi) = \left[ \begin{array}{cc} \xi & 0 \\ 1 & 2\xi \end{array} \right]$$

for $U(\xi) = \left[ \begin{array}{cc} 9 & \xi \\ 0 & 1 \end{array} \right]$.

• Thus minimal row degrees are 1, 1.
• Example over field $\mathbb{Z}_{11}$: $\mathcal{B} = \text{span}\left\{ \left( \begin{array}{c} 9 \\ 0 \\ 0 \\ \vdots \end{array} \right), \left( \begin{array}{c} 0 \\ 1 \\ 0 \\ \vdots \end{array} \right), \left( \begin{array}{c} 0 \\ 0 \\ 0 \\ \vdots \end{array} \right), \ldots \right\}$

• has kernel representation $A(\sigma)w = 0$ with

$$A(\xi) = \begin{bmatrix} 0 & \xi^2 \\ 1 & 2\xi \end{bmatrix}$$

• $A$ is not row reduced since leading row coefficient matrix

$$A^{\text{lrc}} = \begin{bmatrix} 0 & 1 \\ 0 & 2 \end{bmatrix}$$

• Any other representation $R(\sigma)w = 0$ of $\mathcal{B}$ with $R(\xi)$ of full row rank is given by $R(\xi) = U(\xi)A(\xi)$ with $U(\xi)$ unimodular

• Row reduction procedure of Wedderburn ’34; Wolovich ’74 yields

$$U(\xi)A(\xi) = \begin{bmatrix} \xi & 0 \\ 1 & 2\xi \end{bmatrix} \quad \text{for} \quad U(\xi) = \begin{bmatrix} 9 & \xi \\ 0 & 1 \end{bmatrix}$$

• Thus minimal row degrees are 1, 1.
• Example over field \( \mathbb{Z}_{11} \): \( \mathcal{B} = \text{span} \left\{ \begin{bmatrix} 9 \\ 0 \\ 0 \\ \vdots \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \end{bmatrix}, \ldots \right\} \)

• has kernel representation \( A(\sigma)w = 0 \) with

\[
A(\xi) = \begin{bmatrix}
0 & \xi^2 \\
1 & 2\xi
\end{bmatrix}
\]

• \( A \) is not row reduced since leading row coefficient matrix

\[
A^{\text{lrc}} = \begin{bmatrix}
0 & 1 \\
0 & 2
\end{bmatrix}
\]

• Any other representation \( R(\sigma)w = 0 \) of \( \mathcal{B} \) with \( R(\xi) \) of full row rank is given by \( R(\xi) = U(\xi)A(\xi) \) with \( U(\xi) \) unimodular

• Row reduction procedure of Wedderburn ’34; Wolovich ’74 yields

\[
U(\xi)A(\xi) = \begin{bmatrix}
\xi & 0 \\
1 & 2\xi
\end{bmatrix} \quad \text{for} \quad U(\xi) = \begin{bmatrix}
9 & \xi \\
0 & 1
\end{bmatrix}
\]

• Thus minimal row degrees are 1, 1.
• Dropping rank constraint: any other representation $R(\sigma)w = 0$ of $B$ is given by $R(\xi) = U(\xi) \begin{bmatrix} A(\xi) \\ 0 \end{bmatrix}$ with $U(\xi)$ unimodular
Row reduced $R$ with row degrees $d_1, \ldots, d_k$ has

**PREDICTABLE DEGREE PROPERTY:**

$$\text{row degree of } a(\xi)R(\xi) = \max_{1 \leq i \leq k} (d_i + \deg a_i(\xi))$$

Then is key player in **parametrization** of annihilators of $B = \ker R(\sigma)$:

**THEOREM** A vector $V(\xi)$ of row degree $d$ is an annihilator of $B$ if and only if there exists $Q(\xi) = \begin{bmatrix} q_1(\xi) & \cdots & q_k(\xi) \end{bmatrix}$ such that
Row reduced $R$ with row degrees $d_1, \ldots, d_k$ has

**PREDICTABLE DEGREE PROPERTY:**

row degree of $a(\xi)R(\xi) = \max_{1 \leq i \leq k} (d_i + \deg a_i(\xi))$

Then is key player in **parametrization** of annihilators of $\mathcal{B} = \ker R(\sigma)$:

**Theorem** A vector $V(\xi)$ of row degree $d$ is an annihilator of $\mathcal{B}$ if and only if there exists $Q(\xi) = \begin{bmatrix} q_1(\xi) & \cdots & q_k(\xi) \end{bmatrix}$ such that

1. $V(\xi) = Q(\xi)R(\xi)$
2. $\deg q_i(\xi) \leq d_i$ for $i = 1, \ldots, k$

Furthermore, $Q(\xi)$ is unique.
Row reduced $R$ with row degrees $d_1, \ldots, d_k$ has

**PREDICTABLE DEGREE PROPERTY:**

row degree of $a(\xi)R(\xi) = \max_{1 \leq i \leq k} (d_i + \deg a_i(\xi))$

Then is key player in **parametrization** of annihilators of $\mathcal{B} = \ker R(\sigma)$:

**Theorem** A vector $V(\xi)$ of row degree $d$ is an annihilator of $\mathcal{B}$ if and only if there exists $Q(\xi) = \begin{bmatrix} q_1(\xi) & \cdots & q_k(\xi) \end{bmatrix}$ such that

1. $V(\xi) = Q(\xi)R(\xi)$
2. $\deg q_i(\xi) = d - d_i$, for $i = 1, \ldots, k$

Furthermore, $Q(\xi)$ is unique.
Row reduced $R$ with row degrees $d_1, \ldots, d_k$ has

**PREDICTABLE DEGREE PROPERTY:**

$$\text{row degree of } a(\xi)R(\xi) = \max_{1 \leq i \leq k} (d_i + \deg a_i(\xi))$$

Then is key player in **parametrization** of annihilators of $B = \ker R(\sigma)$:

**Theorem** A vector $V(\xi)$ of row degree $d$ is an annihilator of $B$ if and only if there exists $Q(\xi) = \begin{bmatrix} q_1(\xi) & \cdots & q_k(\xi) \end{bmatrix}$ such that

1. $V(\xi) = Q(\xi)R(\xi)$
2. $\deg q_i(\xi) \leq d - d_i$ for $i = 1, \ldots, k$.

Furthermore, $Q(\xi)$ is unique.
Row reduced $R$ with row degrees $d_1, \ldots, d_k$ has

**PREDICTABLE DEGREE PROPERTY:**

\[
\text{row degree of } a(\xi)R(\xi) = \max_{1 \leq i \leq k} (d_i + \deg a_i(\xi))
\]

Then is key player in parametrization of annihilators of $\mathcal{B} = \ker R(\sigma)$:

**THEOREM** A vector $V(\xi)$ of row degree $d$ is an annihilator of $\mathcal{B}$ if and only if there exists $Q(\xi) = \begin{bmatrix} q_1(\xi) & \cdots & q_k(\xi) \end{bmatrix}$ such that

1. $V(\xi) = Q(\xi)R(\xi)$
2. $\deg q_i(\xi) \leq d - d_i$ for $i = 1, \ldots, k$.

Furthermore, $Q(\xi)$ is unique.
Row reduced $R$ with row degrees $d_1, \ldots, d_k$ has

**PREDICTABLE DEGREE PROPERTY:**

\[
\text{row degree of } a(\xi)R(\xi) = \max_{1 \leq i \leq k} (d_i + \deg a_i(\xi))
\]

Then is key player in parametrization of annihilators of $\mathcal{B} = \ker R(\sigma)$:

**THEOREM** A vector $V(\xi)$ of row degree $d$ is an annihilator of $\mathcal{B}$ if and only if there exists $Q(\xi) = \left[ q_1(\xi) \ \cdots \ q_k(\xi) \right]$ such that

1. $V(\xi) = Q(\xi)R(\xi)$
2. $\deg q_i(\xi) \leq d - d_i$ for $i = 1, \ldots, k$.

Furthermore, $Q(\xi)$ is unique.
Row reduced $R$ with row degrees $d_1, \ldots, d_k$ has

PREDICTABLE DEGREE PROPERTY:

\[
\text{row degree of } a(\xi)R(\xi) = \max_{1 \leq i \leq k} (d_i + \deg a_i(\xi))
\]

Then is key player in parametrization of annihilators of $\mathcal{B} = \ker R(\sigma)$:

THEOREM A vector $V(\xi)$ of row degree $d$ is an annihilator of $\mathcal{B}$ if and only if there exists $Q(\xi) = \begin{bmatrix} q_1(\xi) & \cdots & q_k(\xi) \end{bmatrix}$ such that

1. $V(\xi) = Q(\xi)R(\xi)$
2. $\deg q_i(\xi) \leq d - d_i$ for $i = 1, \ldots, k$.

Furthermore, $Q(\xi)$ is unique.
- Same example over ring $\mathbb{Z}_{27}$: $\mathcal{B} = \text{span} \left\{ \left( \begin{array}{c} 9 \\ 0 \end{array} \right), \left( \begin{array}{c} 0 \\ 1 \end{array} \right), \left( \begin{array}{c} 0 \\ 0 \end{array} \right), \ldots \right\}$

- note that $\mathbb{Z}_{27}$ has zero divisors, such as 3, 9

- $\mathcal{B}$ has kernel representation $A(\sigma)w = 0$ with

$$A(\xi) = \begin{bmatrix} 0 & \xi^2 \\ 1 & 18\xi \end{bmatrix}$$

- Any other representation $R(\sigma)w = 0$ of $\mathcal{B}$ with $R(\xi)$ of full row rank is given by $R(\xi) = U(\xi)A(\xi)$ with $U(\xi)$ unimodular

- Attempt to make $R(\xi)$ row reduced: take $U(\xi) = \begin{bmatrix} -18 & \xi \\ 0 & 1 \end{bmatrix}$, yielding $R = \begin{bmatrix} \xi & 0 \\ 1 & 18\xi \end{bmatrix}$

- BUT... $U$ not unimodular, so does not yield correct $\mathcal{B}$. Indeed $R$ models $\left( \begin{array}{c} 0 \\ 1 \end{array} \right), \left( \begin{array}{c} 0 \\ 3 \end{array} \right), \left( \begin{array}{c} 0 \\ 3 \end{array} \right), \ldots$ which is not in $\mathcal{B}$
• Same example over ring $\mathbb{Z}_{27}$: $\mathcal{B} = \text{span}\left\{\left(\begin{array}{c} 9 \\ 0 \end{array}\right), \left(\begin{array}{c} 0 \\ 1 \end{array}\right), \left(\begin{array}{c} 0 \\ 0 \end{array}\right), \ldots\right\}$

• note that $\mathbb{Z}_{27}$ has zero divisors, such as 3 , 9

• $\mathcal{B}$ has kernel representation $A(\sigma)w = 0$ with

$$A(\xi) = \begin{bmatrix} 0 & \xi^2 \\ 1 & 18\xi \end{bmatrix}$$

• Any other representation $R(\sigma)w = 0$ of $\mathcal{B}$ with $R(\xi)$ of full row rank is given by $R(\xi) = U(\xi)A(\xi)$ with $U(\xi)$ unimodular

• Attempt to make $R(\xi)$ row reduced: take $U(\xi) = \begin{bmatrix} -18 & \xi \\ 0 & 1 \end{bmatrix}$, yielding $R = \begin{bmatrix} \xi & 0 \\ 1 & 18\xi \end{bmatrix}$

• BUT... $U$ not unimodular, so does not yield correct $\mathcal{B}$. Indeed $R$ models $\left(\begin{array}{c} 0 \\ 1 \end{array}\right), \left(\begin{array}{c} 0 \\ 3 \end{array}\right), \left(\begin{array}{c} 0 \\ 3 \end{array}\right), \ldots\right)$ which is not in $\mathcal{B}$
• Same example over ring $\mathbb{Z}_{27}$: $B = \text{span} \left\{ \left( \begin{array}{c} 9 \\ 0 \end{array} \right), \left( \begin{array}{c} 0 \\ 1 \end{array} \right), \left( \begin{array}{c} 0 \\ 0 \end{array} \right), \ldots \right\}$

• note that $\mathbb{Z}_{27}$ has zero divisors, such as $3, 9$

• $B$ has kernel representation $A(\sigma)w = 0$ with

$$A(\xi) = \begin{bmatrix} 0 & \xi^2 \\ 1 & 18\xi \end{bmatrix}$$

• Any other representation $R(\sigma)w = 0$ of $B$ with $R(\xi)$ of full row rank is given by $R(\xi) = U(\xi)A(\xi)$ with $U(\xi)$ unimodular

• Attempt to make $R(\xi)$ row reduced: take $U(\xi) = \begin{bmatrix} -18 & \xi \\ 0 & 1 \end{bmatrix}$, yielding $R = \begin{bmatrix} \xi & 0 \\ 1 & 18\xi \end{bmatrix}$

• BUT... $U$ not unimodular, so does not yield correct $B$. Indeed $R$ models $\left( \begin{array}{c} 0 \\ 1 \end{array} \right), \left( \begin{array}{c} 0 \\ 3 \end{array} \right), \left( \begin{array}{c} 0 \\ 3 \end{array} \right), \ldots$ which is not in $B$
- Same example over ring $\mathbb{Z}_{27}$: $B = \text{span}\left\{ \left( \begin{bmatrix} 9 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \ldots \right) \right\}$

- note that $\mathbb{Z}_{27}$ has zero divisors, such as 3 , 9

- $B$ has kernel representation $A(\sigma)w = 0$ with

  $$A(\xi) = \begin{bmatrix} 0 & \xi^2 \\ 1 & 18\xi \end{bmatrix}$$

- Any other representation $R(\sigma)w = 0$ of $B$ with $R(\xi)$ of full row rank is given by $R(\xi) = U(\xi)A(\xi)$ with $U(\xi)$ unimodular

  - Attempt to make $R(\xi)$ row reduced: take $U(\xi) = \begin{bmatrix} -18 & \xi \\ 0 & 1 \end{bmatrix}$, yielding $R = \begin{bmatrix} \xi & 0 \\ 1 & 18\xi \end{bmatrix}$

  - BUT... $U$ not unimodular, so does not yield correct $B$. Indeed $R$ models $\left( \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \end{bmatrix}, \ldots \right)$ which is not in $B$
• Same example over ring $\mathbb{Z}_{27}$: $\mathcal{B} = \text{span}\{\left(\begin{array}{c} 9 \\ 0 \end{array}\right), \left(\begin{array}{c} 0 \\ 1 \end{array}\right), \left(\begin{array}{c} 0 \\ 0 \end{array}\right), \ldots\}\}$

• note that $\mathbb{Z}_{27}$ has zero divisors, such as 3, 9

• $\mathcal{B}$ has kernel representation $A(\sigma)\mathbf{w} = 0$ with

$$A(\xi) = \begin{bmatrix} 0 & \xi^2 \\ 1 & 18\xi \end{bmatrix}$$

• Any other representation $R(\sigma)\mathbf{w} = 0$ of $\mathcal{B}$ with $R(\xi)$ of full row rank is given by $R(\xi) = U(\xi)A(\xi)$ with $U(\xi)$ unimodular

• Attempt to make $R(\xi)$ row reduced: take $U(\xi) = \begin{bmatrix} -18 & \xi \\ 0 & 1 \end{bmatrix}$,

yielding $R = \begin{bmatrix} \xi & 0 \\ 1 & 18\xi \end{bmatrix}$

• BUT... $U$ not unimodular, so does not yield correct $\mathcal{B}$. Indeed $R$ models $\left(\begin{array}{c} 0 \\ 1 \end{array}\right), \left(\begin{array}{c} 0 \\ 3 \end{array}\right), \left(\begin{array}{c} 0 \\ 3 \end{array}\right), \ldots\}$ which is not in $\mathcal{B}$
• Same example over ring $\mathbb{Z}_{27}$: $\mathcal{B} = \text{span} \left\{ \begin{pmatrix} 9 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \ldots \right\}$

• note that $\mathbb{Z}_{27}$ has zero divisors, such as 3, 9

• $\mathcal{B}$ has kernel representation $A(\sigma)w = 0$ with

\[
A(\xi) = \begin{bmatrix} 0 & \xi^2 \\ 1 & 18 \xi \end{bmatrix}
\]

• Any other representation $R(\sigma)w = 0$ of $\mathcal{B}$ with $R(\xi)$ of full row rank is given by $R(\xi) = U(\xi)A(\xi)$ with $U(\xi)$ unimodular

• Attempt to make $R(\xi)$ row reduced: take $U(\xi) = \begin{bmatrix} -18 & \xi \\ 0 & 1 \end{bmatrix}$, yielding $R = \begin{bmatrix} \xi & 0 \\ 1 & 18 \xi \end{bmatrix}$

• BUT... $U$ not unimodular, so does not yield correct $\mathcal{B}$. Indeed $R$ models $\left\{ \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \end{pmatrix}, \ldots \right\}$ which is not in $\mathcal{B}$
• Dropping rank constraint: any other representation $R(\sigma)w = 0$ of $\mathcal{B}$ is given by $R(\xi) = U(\xi) \begin{bmatrix} A(\xi) \\ 0 \end{bmatrix}$ with $U(\xi)$ unimodular

**WANTED:**
Theory of row reduced polynomial matrices over $\mathbb{Z}_p$

= OPEN PROBLEM, posed in e.g. $FZ'97$

We present a solution
• Dropping rank constraint: any other representation $R(\sigma)w = 0$ of $\mathcal{B}$ is given by $R(\xi) = U(\xi) \begin{bmatrix} A(\xi) & 0 \end{bmatrix}$ with $U(\xi)$ unimodular

WANTED:
Theory of row reduced polynomial matrices over $\mathbb{Z}_p^r$

= OPEN PROBLEM, posed in e.g. FZ’97

We present a solution
• Dropping rank constraint: any other representation \( R(\sigma)w = 0 \) of \( \mathcal{B} \) is given by \( R(\xi) = U(\xi) \begin{bmatrix} A(\xi) \\ 0 \end{bmatrix} \) with \( U(\xi) \) unimodular.

**WANTED:**
Theory of row reduced polynomial matrices over \( \mathbb{Z}_{p^r} \)

\[ = \text{OPEN PROBLEM, posed in e.g. } FZ'97 \]
• Dropping rank constraint: any other representation $R(\sigma)w = 0$ of $\mathcal{B}$ is given by $R(\xi) = U(\xi) \begin{bmatrix} A(\xi) \\ 0 \end{bmatrix}$ with $U(\xi)$ unimodular

WANTED:
Theory of row reduced polynomial matrices over $\mathbb{Z}_p^r$

= OPEN PROBLEM, posed in e.g. FZ’97

We present a solution
Outline of new theory:

- work with redundant kernel reps, obtained via

\[ R(\xi) = U(\xi) \begin{bmatrix} A(\xi) \\ 0 \end{bmatrix} \text{ with } U(\xi) \text{ unimodular} \]

- impose specific structure on \( R(\xi) \): the composed form
- composed form is less restrictive than “adapted form” from FZ’97
- impose rank condition on \( R^{lrc} \)

Inspired by theory of “\( p \)-generator sequences” for constant vectors in \( \mathbb{Z}_p^q \), as in Vazirani a.o. ’96
Outline of new theory:

- work with redundant kernel reps, obtained via

\[ R(\xi) = U(\xi) \begin{bmatrix} A(\xi) \\ 0 \end{bmatrix} \text{ with } U(\xi) \text{ unimodular} \]

- impose specific structure on \( R(\xi) \): the \textit{composed form}
- composed form is less restrictive than \textit{adapted form} from FZ’97
- impose rank condition on \( R^{\text{lrc}} \)

Inspired by theory of “\( p \)-generator sequences” for constant vectors in \( \mathbb{Z}_p^q \), as in Vazirani a.o. ’96
Outline of new theory:

- work with redundant kernel reps, obtained via

\[ R(\xi) = U(\xi) \begin{bmatrix} A(\xi) \\ 0 \end{bmatrix} \text{ with } U(\xi) \text{ unimodular} \]

- impose specific structure on \( R(\xi) \): the composed form
- composed form is less restrictive than “adapted form” from FZ’97
- impose rank condition on \( R_{\text{lrc}} \)

Inspired by theory of “\( p \)-generator sequences” for constant vectors in \( \mathbb{Z}_p^q \), as in Vazirani a.o. ’96
Outline of new theory:

- work with redundant kernel reps, obtained via

\[ R(\xi) = U(\xi) \begin{bmatrix} A(\xi) \\ 0 \end{bmatrix} \text{ with } U(\xi) \text{ unimodular} \]

- impose specific structure on \( R(\xi) \): the composed form
- composed form is less restrictive than “adapted form” from FZ’97
- impose rank condition on \( R^{lrc} \)

Inspired by theory of “\( p \)-generator sequences” for constant vectors in \( \mathbb{Z}_p^q \), as in Vazirani a.o. ’96
Outline of new theory:

- work with redundant kernel reps, obtained via

\[ R(\xi) = U(\xi) \begin{bmatrix} A(\xi) \\ 0 \end{bmatrix} \text{ with } U(\xi) \text{ unimodular} \]

- impose specific structure on \( R(\xi) \): the composed form
- composed form is less restrictive than “adapted form” from FZ’97
- impose rank condition on \( R^{\text{lrc}} \)

Inspired by theory of “\( p \)-generator sequences” for constant vectors in \( \mathbb{Z}_p^q \), as in Vazirani a.o. ’96
Outline of new theory:

- work with redundant kernel reps, obtained via
  
  \[ R(\xi) = U(\xi) \begin{bmatrix} A(\xi) \\ 0 \end{bmatrix} \mathrm{ with } \ U(\xi) \mathrm{ unimodular} \]

- impose specific structure on \( R(\xi) \): the composed form
- composed form is less restrictive than “adapted form” from FZ’97
- impose rank condition on \( R^{lrc} \)

Inspired by theory of “\( p \)-generator sequences” for constant vectors in \( \mathbb{Z}_p^q \), as in Vazirani a.o. ’96
Theory of $p$-generator sequences for $\mathbb{Z}_p^q[\xi]$

- Commutative algebra: concept of “generating system along a composition chain” Matsumura ’86
- Rephrased as “$p$-generator sequence” in Vazirani a.o. ’96 for constant vectors in $\mathbb{Z}_p^q$
- We now introduce same concepts for polynomial vectors in $\mathbb{Z}_p^q[\xi]$

**Definition** Let $v_1(\xi), \ldots, v_k(\xi)$ be vectors in $\mathbb{Z}_p^q[\xi]$ and let $a_j(\xi)$ be polynomials with coefficients in $\{0, 1, \ldots, p - 1\} \subset \mathbb{Z}_p$. Then the vector

$$\sum_{j=1}^{k} a_j(\xi)v_j(\xi)$$

is called a $p$-linear combination of $v_1(\xi), \ldots, v_k(\xi)$. The set of all $p$-linear combinations of $v_1(\xi), \ldots, v_k(\xi)$ is called the $p$-span of $\{v_1(\xi), \ldots, v_k(\xi)\}$.
Theory of $p$-generator sequences for $\mathbb{Z}_{q}^{r}[\xi]$

- **Commutative algebra:** concept of “generating system along a composition chain”  
  *Matsumura ’86*

- rephrased as “$p$-generator sequence” in Vazirani a.o. ’96 for constant vectors in $\mathbb{Z}_{q}^{r}$

- we now introduce same concepts for polynomial vectors in $\mathbb{Z}_{q}^{r}[\xi]$

**Definition** Let $v_1(\xi), \ldots, v_k(\xi)$ be vectors in $\mathbb{Z}_{q}^{r}[\xi]$ and let $a_j(\xi)$ be polynomials with coefficients in $\{0, 1, \ldots, p - 1\} \subset \mathbb{Z}_{p^r}$. Then the vector

$$
\sum_{j=1}^{k} a_j(\xi)v_j(\xi)
$$

is called a **$p$-linear combination** of $v_1(\xi), \ldots, v_k(\xi)$. The set of all $p$-linear combinations of $v_1(\xi), \ldots, v_k(\xi)$ is called the **$p$-span** of $\{v_1(\xi), \ldots, v_k(\xi)\}$. 
Theory of \( p \)-generator sequences for \( \mathbb{Z}_p^q [\xi] \)

- *Commutative algebra*: concept of “generating system along a composition chain”  
  *Matsumura ’86*

- rephrased as “\( p \)-generator sequence” in *Vazirani a.o. ’96* for constant vectors in \( \mathbb{Z}_p^q \)

- we now introduce same concepts for polynomial vectors in \( \mathbb{Z}_p^q [\xi] \)

**Definition** Let \( \nu_{1}(\xi), \ldots, \nu_{k}(\xi) \) be vectors in \( \mathbb{Z}_p^q [\xi] \) and let \( a_{j}(\xi) \) be polynomials with coefficients in \( \{0, 1, \ldots, p - 1\} \subset \mathbb{Z}_p^r \). Then the vector

\[
\sum_{j=1}^{k} a_{j}(\xi) \nu_{j}(\xi)
\]

is called a **\( p \)-linear combination** of \( \nu_{1}(\xi), \ldots, \nu_{k}(\xi) \). The set of all \( p \)-linear combinations of \( \nu_{1}(\xi), \ldots, \nu_{k}(\xi) \) is called the **\( p \)-span** of \( \{\nu_{1}(\xi), \ldots, \nu_{k}(\xi)\} \).
Theory of \( p \)-generator sequences for \( \mathbb{Z}_p^q[\xi] \)

- *Commutative algebra*: concept of “generating system along a composition chain” *Matsumura ’86*
- rephrased as “\( p \)-generator sequence” in *Vazirani a.o. ’96* for *constant* vectors in \( \mathbb{Z}_p^q \)
- we now introduce same concepts for *polynomial* vectors in \( \mathbb{Z}_p^q[\xi] \)

**Definition** Let \( v_1(\xi), \ldots, v_k(\xi) \) be vectors in \( \mathbb{Z}_p^q[\xi] \) and let \( a_j(\xi) \) be polynomials with coefficients in \( \{0, 1, \ldots, p - 1\} \subset \mathbb{Z}_p^r \). Then the vector

\[
\sum_{j=1}^{k} a_j(\xi)v_j(\xi)
\]

is called a *\( p \)-linear combination* of \( v_1(\xi), \ldots, v_k(\xi) \). The set of all \( p \)-linear combinations of \( v_1(\xi), \ldots, v_k(\xi) \) is called the *\( p \)-span* of \( \{v_1(\xi), \ldots, v_k(\xi)\} \).
Theory of $p$-generator sequences for $\mathbb{Z}_{pr}[\xi]$

- **Commutative algebra:** concept of “generating system along a composition chain” *Matsumura ’86*
- rephrased as “$p$-generator sequence” in *Vazirani a.o. ’96* for constant vectors in $\mathbb{Z}_{pr}^q$
- we now introduce same concepts for *polynomial* vectors in $\mathbb{Z}_{pr}^q [\xi]$

**Definition** Let $v_1(\xi), \ldots, v_k(\xi)$ be vectors in $\mathbb{Z}_{pr}^q [\xi]$ and let $a_j(\xi)$ be polynomials with coefficients in $\{0, 1, \ldots, p - 1\} \subset \mathbb{Z}_{pr}$. Then the vector

$$\sum_{j=1}^{k} a_j(\xi)v_j(\xi)$$

is called a **$p$-linear combination** of $v_1(\xi), \ldots, v_k(\xi)$. The set of all $p$-linear combinations of $v_1(\xi), \ldots, v_k(\xi)$ is called the **$p$-span** of $\{v_1(\xi), \ldots, v_k(\xi)\}$. 
**Definition** Let $v_1(\xi), \ldots, v_k(\xi)$ be vectors in $\mathbb{Z}_p^q[\xi]$. Then they are said to be **$p$-linearly independent** if there does not exist a nontrivial $p$-linear combination of $v_1(\xi), \ldots, v_k(\xi)$ that equals zero.
**Definition**  An ordered sequence of vectors $(v_1(\xi), v_2(\xi), \cdots, v_k(\xi))$, with $v_i(\xi) \in \mathbb{Z}_{p^r}^q [\xi]$, is said to be a \textbf{$p$-generator sequence} if

1) for $1 \leq i \leq k - 1$, the vector $pv_i(\xi)$ can be written as a $p$-linear combination of $v_{i+1}(\xi), \ldots, v_k(\xi)$ and

2) $pv_k(\xi)$ equals the zero vector.

**Important Property of $p$-Generator Sequence:**

$$p-\text{span} \,(v_1(\xi), v_2(\xi), \cdots, v_k(\xi)) = \text{span} \,(v_1(\xi), v_2(\xi), \cdots, v_k(\xi))$$

is a submodule of $\mathbb{Z}_{p^r}^q$. 
**Definition** An ordered sequence of vectors \((v_1(\xi), v_2(\xi), \cdots, v_k(\xi))\), with \(v_i(\xi) \in \mathbb{Z}_{p^r}[\xi]\), is said to be a \textit{p-generator sequence} if

1) for \(1 \leq i \leq k - 1\), the vector \(pv_i(\xi)\) can be written as a \textit{p}-linear combination of \(v_{i+1}(\xi), \ldots, v_k(\xi)\) and

2) \(pv_k(\xi)\) equals the zero vector.

**Important Property of \(p\)-Generator Sequence:**

\[p-\text{span} \ (v_1(\xi), v_2(\xi), \cdots, v_k(\xi)) = \text{span} \ (v_1(\xi), v_2(\xi), \cdots, v_k(\xi))\]

is a submodule of \(\mathbb{Z}_{p^r}^q\).
**DEFINITION** An ordered sequence of vectors 
$(v_1(\xi), v_2(\xi), \cdots, v_k(\xi))$, with $v_i(\xi) \in \mathbb{Z}_{p^r}^q[\xi]$, is said to be a $p$-generator sequence if

1) for $1 \leq i \leq k - 1$, the vector $pv_i(\xi)$ can be written as a $p$-linear combination of $v_{i+1}(\xi), \ldots, v_k(\xi)$ and

2) $pv_k(\xi)$ equals the zero vector.

**IMPORTANT PROPERTY OF $p$-GENERATOR SEQUENCE:**

$p$-span $(v_1(\xi), v_2(\xi), \cdots, v_k(\xi)) = \text{span} (v_1(\xi), v_2(\xi), \cdots, v_k(\xi))$

is a submodule of $\mathbb{Z}_{p^r}^q$. 

**DEFINITION** An ordered sequence of vectors \((v_1(\xi), v_2(\xi), \cdots, v_k(\xi))\), with \(v_i(\xi) \in \mathbb{Z}_{p^r}^q[\xi]\), is said to be a **\(p\)-generator sequence** if

1) for \(1 \leq i \leq k - 1\), the vector \(pv_i(\xi)\) can be written as a \(p\)-linear combination of \(v_{i+1}(\xi), \ldots, v_k(\xi)\) and

2) \(pv_k(\xi)\) equals the zero vector.

**IMPORTANT PROPERTY OF \(p\)-GENERATOR SEQUENCE:**

\[
p-\text{span} \ (v_1(\xi), v_2(\xi), \cdots, v_k(\xi)) = \text{span} \ (v_1(\xi), v_2(\xi), \cdots, v_k(\xi))
\]

is a submodule of \(\mathbb{Z}_{p^r}^q\).
**Definition** A kernel representation $R(\sigma)w = 0$ is in composed form if the rows of $R(\xi)$ are a $p$-generator sequence, up to row permutation.

Example as before in ring $\mathbb{Z}_{27}$:

- $A(\xi) = \begin{bmatrix} 0 & \xi^2 \\ 1 & 18\xi \end{bmatrix}$ is not in composed form.

- $\begin{bmatrix} A(\xi) \\ pA(\xi) \\ p^2A(\xi) \\ p^r-1A(\xi) \end{bmatrix} = \begin{bmatrix} 0 & \xi^2 \\ 1 & 18\xi \\ 0 & 3\xi^2 \\ 3 & 0 \end{bmatrix}$ is in composed form.

- Another composed rep. $R(\xi) = \begin{bmatrix} 0 & \xi^2 \\ 1 & 18\xi \\ 9 & 0 \end{bmatrix}$.
**Definition**  A kernel representation \( R(\sigma)w = 0 \) is in composed form if the rows of \( R(\xi) \) are a \( p \)-generator sequence, up to row permutation.

Example as before in ring \( \mathbb{Z}_{27} \):

- \( A(\xi) = \begin{bmatrix} 0 & \xi^2 \\ 1 & 18\xi \end{bmatrix} \) is not in composed form.

- \( \begin{bmatrix} A(\xi) \\ pA(\xi) \\ p^2A(\xi) \\ \vdots \\ p^{r-1}A(\xi) \end{bmatrix} = \begin{bmatrix} 0 & \xi^2 \\ 1 & 18\xi \\ 0 & 3\xi^2 \\ 3 & 0 \\ 9 & 9\xi^2 \end{bmatrix} \) is in composed form.

- Another composed rep: \( R(\xi) = \begin{bmatrix} 0 & \xi^2 \\ 0 & 3\xi^2 \\ 14 & 9\xi \\ \xi & 0 \\ 3 & 0 \\ 9 & 0 \end{bmatrix} \)
**Definition** A kernel representation $R(\sigma)w = 0$ is in composed form if the rows of $R(\xi)$ are a $p$-generator sequence, up to row permutation.

Example as before in ring $\mathbb{Z}_{27}$:

- $A(\xi) = \begin{bmatrix} 0 & \xi^2 \\ 1 & 18\xi \end{bmatrix}$ is not in composed form.

- $\begin{bmatrix} A(\xi) \\ pA(\xi) \\ p^2A(\xi) \\ \vdots \\ p^{r-1}A(\xi) \end{bmatrix} = \begin{bmatrix} 0 & \xi^2 \\ 1 & 18\xi \\ 0 & 3\xi^2 \\ 3 & 0 \\ 0 & 9\xi^2 \\ 9 & 0 \end{bmatrix}$ is in composed form.

- Another composed rep: $R(\xi) = \begin{bmatrix} 0 & \xi^2 \\ 0 & 3\xi^2 \\ 14 & 9\xi \\ \xi & 0 \\ 3 & 0 \\ 9 & 0 \end{bmatrix}$
**Definition** A kernel representation $R(\sigma)w = 0$ is in composed form if the rows of $R(\xi)$ are a $p$-generator sequence, up to row permutation.

Example as before in ring $\mathbb{Z}_27$:

- $A(\xi) = \begin{bmatrix} 0 & \xi^2 \\ 1 & 18\xi \end{bmatrix}$ is not in composed form.

- $\begin{bmatrix} A(\xi) \\ pA(\xi) \\ p^2A(\xi) \\ \vdots \\ p^{r-1}A(\xi) \end{bmatrix} = \begin{bmatrix} 0 & \xi^2 \\ 1 & 18\xi \\ 0 & 3\xi^2 \\ 3 & 0 \\ 0 & 9\xi^2 \\ 9 & 0 \end{bmatrix}$ is in composed form.

- Another composed rep: $R(\xi) = \begin{bmatrix} 0 & \xi^2 \\ 0 & 3\xi^2 \\ 14 & 9\xi \\ \xi & 0 \\ 3 & 0 \\ 9 & 0 \end{bmatrix}$
**Definition (KPP '07)** Let $M$ be a submodule of $\mathbb{Z}_p^q[\xi]$, written as a $p$-span of a $p$-generator sequence $(v_1(\xi), v_2(\xi), \ldots, v_k(\xi))$. Then $(v_1(\xi), v_2(\xi), \ldots, v_k(\xi))$ is called a **reduced $p$-basis** for $M$ if the vectors $v_1^{\lrc}, v_2^{\lrc}, \ldots, v_k^{\lrc}$ are $p$-linearly independent in $\mathbb{Z}_p^q$.

Leads to concepts of

- $p$-dimension of $M$: $p-\dim (M) = k$
- $p$-degrees of $M$: given by $\deg v_1(\xi), \deg v_2(\xi), \ldots, \deg v_k(\xi)$

**Algorithm (KPP '07)**

*Input data:* module $M := \text{span} (w_1(\xi), \ldots, w_g(\xi))$ with $w_i(\xi) \in \mathbb{Z}_p^q[\xi]$

*Output data:* reduced $p$-basis $(v_1(\xi), \ldots, v_k(\xi))$
**Definition** (KPP '07) Let $M$ be a submodule of $\mathbb{Z}_{p^r}^q[\xi]$, written as a $p$-span of a $p$-generator sequence $(v_1(\xi), v_2(\xi), \ldots, v_k(\xi))$. Then $(v_1(\xi), v_2(\xi), \ldots, v_k(\xi))$ is called a **reduced $p$-basis** for $M$ if the vectors $v_1^{lrc}, v_2^{lrc}, \ldots, v_k^{lrc}$ are $p$-linearly independent in $\mathbb{Z}_{p^r}^q$.

Leads to concepts of

- $p$-dimension of $M$: $p-$dim $(M) = k$
- $p$-degrees of $M$: given by $\deg v_1(\xi), \deg v_2(\xi), \ldots, \deg v_k(\xi)$

**Algorithm** (KPP '07)

*Input data:* module $M := \text{span} (w_1(\xi), \ldots, w_g(\xi))$ with $w_i(\xi) \in \mathbb{Z}_{p^r}^q[\xi]$

*Output data:* reduced $p$-basis $(v_1(\xi), \ldots, v_k(\xi))$
**Definition** *(KPP ’07)* Let $M$ be a submodule of $\mathbb{Z}_q^{\mathbb{P}_r}[\xi]$, written as a $p$-span of a $p$-generator sequence $(v_1(\xi), v_2(\xi), \ldots, v_k(\xi))$. Then $(v_1(\xi), v_2(\xi), \ldots, v_k(\xi))$ is called a **reduced $p$-basis** for $M$ if the vectors $v_1^{\text{lrc}}, v_2^{\text{lrc}}, \ldots, v_k^{\text{lrc}}$ are $p$-linearly independent in $\mathbb{Z}_q^{\mathbb{P}_r}$.

Leads to concepts of

- **$p$-dimension of $M$**: $p-$dim $(M) = k$
- **$p$-degrees of $M$**: given by $\deg v_1(\xi), \deg v_2(\xi), \ldots, \deg v_k(\xi)$

**Algorithm** *(KPP ’07)*

*Input data:* module $M := \text{span} (w_1(\xi), \ldots, w_g(\xi))$ with $w_i(\xi) \in \mathbb{Z}_q^{\mathbb{P}_r}[\xi]$

*Output data:* reduced $p$-basis $(v_1(\xi), \ldots, v_k(\xi))$
**Definition** (KPP ’07) Let $M$ be a submodule of $\mathbb{Z}_q^r[\xi]$, written as a $p$-span of a $p$-generator sequence $(v_1(\xi), v_2(\xi), \cdots, v_k(\xi))$. Then $(v_1(\xi), v_2(\xi), \cdots, v_k(\xi))$ is called a **reduced $p$-basis** for $M$ if the vectors $v_1^{\text{lrc}}, v_2^{\text{lrc}}, \ldots, v_k^{\text{lrc}}$ are $p$-linearly independent in $\mathbb{Z}_q^r$.

Leads to concepts of

- **$p$-dimension of $M$**: $p-\dim (M) = k$
- **$p$-degrees of $M$**: given by $\deg v_1(\xi), \deg v_2(\xi), \ldots, \deg v_k(\xi)$

**Algorithm** (KPP ’07)

*Input data:* module $M := \text{span} (w_1(\xi), \ldots, w_g(\xi))$ with $w_i(\xi) \in \mathbb{Z}_q^r[\xi]$

*Output data:* reduced $p$-basis $(v_1(\xi), \ldots, v_k(\xi))$
**Definition (KPP ’07)** Let $R(\xi)$ be a matrix in $\mathbb{Z}_{p^r}^{k \times q}[\xi]$ with row degrees $d_1, \ldots, d_k$. Let

$$a(\xi) = \begin{bmatrix} a_1(\xi) & \cdots & a_k(\xi) \end{bmatrix}$$

be a nonzero polynomial vector with coefficients in

$\{0, 1, \ldots, p - 1\} \subset \mathbb{Z}_{p^r}$ for $i = 1, \ldots, k$. Then $R(\xi)$ is said to have the **$p$-predictable-degree property** if the row degree of $a(\xi)R(\xi)$ equals

$$\max_{1 \leq i \leq k} (d_i + \deg a_i)$$

**Theorem (KPP ’07)** Let $R(\xi)$ be a matrix in $\mathbb{Z}_{p^r}^{k \times q}[\xi]$. Then $R(\xi)$ has the $p$-predictable-degree property iff the rows of $R^{lrc}$ are $p$-linearly independent.
**Definition (KPP '07)** Let $R(\xi)$ be a matrix in $\mathbb{Z}_{p^r}^{k \times q}[\xi]$ with row degrees $d_1, \ldots, d_k$. Let

$$a(\xi) = \begin{bmatrix} a_1(\xi) & \cdots & a_k(\xi) \end{bmatrix}$$

be a nonzero polynomial vector with coefficients in $\{0, 1, \ldots, p - 1\} \subset \mathbb{Z}_{p^r}$ for $i = 1, \ldots, k$. Then $R(\xi)$ is said to have the **$p$-predictable-degree property** if the row degree of $a(\xi)R(\xi)$ equals

$$\max_{1 \leq i \leq k} \left( d_i + \deg a_i \right)$$

**Theorem (KPP '07)** Let $R(\xi)$ be a matrix in $\mathbb{Z}_{p^r}^{k \times q}[\xi]$. Then $R(\xi)$ has the $p$-predictable-degree property iff the rows of $R^{\text{lrc}}$ are $p$-linearly independent.
Example as before in ring $\mathbb{Z}_{27}$:

\[
A(\xi) = \begin{bmatrix}
0 & \xi^2 \\
1 & 18\xi
\end{bmatrix} \rightarrow \text{Algorithm} \quad R(\xi) = \\
\begin{bmatrix}
0 & \xi^2 \\
0 & 3\xi^2 \\
14 & 9\xi \\
\xi & 0 \\
3 & 0 \\
9 & 0
\end{bmatrix}
\]
**Theorem** *(PARAMETRIZATION; KPP ’07)* Let $\mathcal{B} = \ker R(\sigma)$ with row degrees $d_1, \ldots, d_k$ and

- $R(\xi)$ in composed form
- $R(\xi)$ has $p$-predictable-degree property

Then vector $V(\xi)$ is an annihilator of $\mathcal{B}$ of row degree $d$ if and only if there exists a vector $Q(\xi) = \begin{bmatrix} q_1(\xi) & \cdots & q_k(\xi) \end{bmatrix}$ in $\mathbb{Z}_p^k[\xi]$ such that

1. $V(\xi) = Q(\xi)R(\xi)$
2. $\deg q_i(\xi) \leq d - d_i$ for $i = 1, \ldots, k$
3. the coefficients of $q_i(\xi)$ are restricted to $
\{0, 1, \ldots, p - 1\} \subset \mathbb{Z}_p$ for $i = 1, \ldots, k$.

Furthermore, $Q(\xi)$ is unique.
**Theorem (Parametrization; KPP '07)** Let \( B = \ker R(\sigma) \) with row degrees \( d_1, \ldots, d_k \) and

- \( R(\xi) \) in composed form
- \( R(\xi) \) has \( p \)-predictable-degree property

Then vector \( V(\xi) \) is an annihilator of \( B \) of row degree \( d \) if and only if there exists a vector \( Q(\xi) = \begin{bmatrix} q_1(\xi) & \cdots & q_k(\xi) \end{bmatrix} \) in \( \mathbb{Z}_{p^r}[\xi] \) such that

1. \( V(\xi) = Q(\xi)R(\xi) \)
2. \( \deg q_i(\xi) \leq d - d_i \) for \( i = 1, \ldots, k \)
3. the coefficients of \( q_i(\xi) \) are restricted to \( \{0, 1, \ldots, p - 1\} \subseteq \mathbb{Z}_{p^r} \) for \( i = 1, \ldots, k \).

Furthermore, \( Q(\xi) \) is unique.
**Theorem** *(PARAMETRIZATION; KPP ’07)* Let $\mathcal{B} = \ker R(\sigma)$ with row degrees $d_1, \ldots, d_k$ and

- $R(\xi)$ in composed form
- $R(\xi)$ has $p$-predictable-degree property

Then vector $V(\xi)$ is an annihilator of $\mathcal{B}$ of row degree $d$ if and only if there exists a vector $Q(\xi) = \left[ q_1(\xi) \cdots q_k(\xi) \right]$ in $\mathbb{Z}_{p^r}^k[\xi]$ such that

1. $V(\xi) = Q(\xi)R(\xi)$
2. $\deg q_i(\xi) \leq d - d_i$ for $i = 1, \ldots, k$
3. the coefficients of $q_i(\xi)$ are restricted to $\{0, 1, \ldots, p - 1\} \subset \mathbb{Z}_{p^r}$ for $i = 1, \ldots, k$.

Furthermore, $Q(\xi)$ is unique.
**Theorem** *(Parametrization; KPP ’07)* Let $\mathcal{B} = \ker R(\sigma)$ with row degrees $d_1, \ldots, d_k$ and

- $R(\xi)$ in composed form
- $R(\xi)$ has $p$-predictable-degree property

Then vector $V(\xi)$ is an annihilator of $\mathcal{B}$ of row degree $d$ if and only if there exists a vector $Q(\xi) = \left[ q_1(\xi) \cdots q_k(\xi) \right]$ in $\mathbb{Z}_{p^r}[\xi]$ such that

1. $V(\xi) = Q(\xi)R(\xi)$
2. $\deg q_i(\xi) \leq d - d_i$ for $i = 1, \ldots, k$
3. the coefficients of $q_i(\xi)$ are restricted to $\{0, 1, \ldots, p - 1\} \subset \mathbb{Z}_{p^r}$ for $i = 1, \ldots, k$.

Furthermore, $Q(\xi)$ is unique.
**Theorem** *(PARAMETRIZATION; KPP ’07)* Let $\mathcal{B} = \ker R(\sigma)$ with row degrees $d_1, \ldots, d_k$ and

- $R(\xi)$ in composed form
- $R(\xi)$ has $p$-predictable-degree property

Then vector $V(\xi)$ is an annihilator of $\mathcal{B}$ of row degree $d$ if and only if there exists a vector $Q(\xi) = \left[ q_1(\xi) \cdots q_k(\xi) \right]$ in $\mathbb{Z}_p^k[\xi]$ such that

1. $V(\xi) = Q(\xi)R(\xi)$
2. $\deg q_i(\xi) \leq d - d_i$ for $i = 1, \ldots, k$
3. the coefficients of $q_i(\xi)$ are restricted to $\{0, 1, \ldots, p - 1\} \subset \mathbb{Z}_p$ for $i = 1, \ldots, k$.

Furthermore, $Q(\xi)$ is unique
CONCLUSIONS:

- Row reducedness defined for $k \times q$ polynomial matrices $R(\xi)$ with coefficients in $\mathbb{Z}_p^r$, as
  - in composed form AND
  - $p$-dim (rows of $R^{\text{lrc}}$) = $k$
- solves open problem
- gives parametrization result that extends field result

FUTURE WORK:

- apply to minimal polynomial interpolation problems over $\mathbb{Z}_p^r$
- develop dual theory for image representations $w = G(\sigma)u$ of systems over $\mathbb{Z}_p^r$
- apply to convolutional codes over $\mathbb{Z}_p^r$ given by encoder $w = G(\sigma)u$ or syndrome former $H(\sigma)w = 0$. 
CONCLUSIONS:

- Row reducedness defined for $k \times q$ polynomial matrices $R(\xi)$ with coefficients in $\mathbb{Z}_{p^r}$, as
  - in composed form AND
  - $p$-dim (rows of $R^{lrc}$) = $k$

- solves open problem
- gives parametrization result that extends field result

FUTURE WORK:

- apply to minimal polynomial interpolation problems over $\mathbb{Z}_{p^r}$
- develop dual theory for image representations $w = G(\sigma)u$ of systems over $\mathbb{Z}_{p^r}$
- apply to convolutional codes over $\mathbb{Z}_{p^r}$ given by encoder $w = G(\sigma)u$ or syndrome former $H(\sigma)w = 0$. 
**Conclusions:**

- Row reducedness defined for \( k \times q \) polynomial matrices \( R(\xi) \) with coefficients in \( \mathbb{Z}_{p^r} \), as
  - in composed form AND
  - \( p\)-dim (rows of \( R^{\text{lrc}} \)) = \( k \)
- solves open problem
- gives parametrization result that extends field result

**Future Work:**

- apply to minimal polynomial interpolation problems over \( \mathbb{Z}_{p^r} \)
- develop dual theory for image representations \( w = G(\sigma)u \) of systems over \( \mathbb{Z}_{p^r} \)
- apply to convolutional codes over \( \mathbb{Z}_{p^r} \) given by encoder \( w = G(\sigma)u \) or syndrome former \( H(\sigma)w = 0 \).
**Conclusions:**

- Row reducedness defined for $k \times q$ polynomial matrices $R(\xi)$ with coefficients in $\mathbb{Z}_{p^r}$, as
  - in composed form AND
  - $p$-dim (rows of $R_{lrc}$) = $k$
- solves open problem
- gives parametrization result that extends field result

**Future Work:**

- apply to minimal polynomial interpolation problems over $\mathbb{Z}_{p^r}$
- develop dual theory for image representations $w = G(\sigma)u$ of systems over $\mathbb{Z}_{p^r}$
- apply to convolutional codes over $\mathbb{Z}_{p^r}$ given by encoder $w = G(\sigma)u$ or syndrome former $H(\sigma)w = 0$. 
CONCLUSIONS:

• Row reducedness defined for $k \times q$ polynomial matrices $R(\xi)$ with coefficients in $\mathbb{Z}_{p^r}$, as
  • in composed form AND
  • $p$-dim (rows of $R_{\text{lrc}}$) = $k$
• solves open problem
• gives parametrization result that extends field result

FUTURE WORK:

• apply to minimal polynomial interpolation problems over $\mathbb{Z}_{p^r}$
• develop dual theory for image representations $w = G(\sigma)u$ of systems over $\mathbb{Z}_{p^r}$
• apply to convolutional codes over $\mathbb{Z}_{p^r}$ given by encoder $w = G(\sigma)u$ or syndrome former $H(\sigma)w = 0$. 
CONCLUSIONS:

- Row reducedness defined for $k \times q$ polynomial matrices $R(\xi)$ with coefficients in $\mathbb{Z}_{p^r}$, as
  - in composed form AND
  - $p$-dim (rows of $R^{lrc}$) = $k$
- solves open problem
- gives parametrization result that extends field result

FUTURE WORK:

- apply to minimal polynomial interpolation problems over $\mathbb{Z}_{p^r}$
- develop dual theory for image representations $w = G(\sigma)u$ of systems over $\mathbb{Z}_{p^r}$
  - apply to convolutional codes over $\mathbb{Z}_{p^r}$ given by encoder $w = G(\sigma)u$ or syndrome former $H(\sigma)w = 0$. 
CONCLUSIONS:

- Row reducedness defined for $k \times q$ polynomial matrices $R(\xi)$ with coefficients in $\mathbb{Z}_p^r$, as
  - in composed form AND
  - $p$-dim (rows of $R^{\text{lrc}}$) = $k$
- solves open problem
- gives parametrization result that extends field result

FUTURE WORK:

- apply to minimal polynomial interpolation problems over $\mathbb{Z}_p^r$
- develop dual theory for image representations $w = G(\sigma)u$ of systems over $\mathbb{Z}_p^r$
- apply to convolutional codes over $\mathbb{Z}_p^r$ given by encoder $w = G(\sigma)u$ or syndrome former $H(\sigma)w = 0$. 