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

Margreta Kuijper[1] Raquel Pinto[2] Jan Willem Polderman[3]

[1]Department of Electrical and Electronic Engineering
University of Melbourne

[2]Department of Mathematics
University of Aveiro

[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. '69; 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?

- <—> 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?

- <—> 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?

- <—> 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?

- <—> 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?

- <—> 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 $\mathbb{Z}_{11}$: $\mathcal{B} = \text{span}\left\{\left(\begin{bmatrix} 9 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \ldots\right)\right.$
- 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

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

- Thus minimal row degrees are $1, 1$.

- Example over field $\mathbb{Z}_{11}$: $\mathcal{B} = \text{span}\left\{\left(\begin{bmatrix} 9 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \dots\right)\right.$
- 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

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

- Thus minimal row degrees are $1, 1$.

- Example over field $\mathbb{Z}_{11}$: $\mathcal{B} = \text{span}\left\{\left(\begin{bmatrix} 9 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \ldots\right)\right.$
- 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

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

- Thus minimal row degrees are 1, 1.

- Example over field $\mathbb{Z}_{11}$: $\mathcal{B} = \text{span}\left\{\left(\begin{bmatrix} 9 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \ldots\right)\right.$
- has kernel representation $A(\sigma)\boldsymbol{w} = 0$ 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 $R(\sigma)\boldsymbol{w} = 0$ 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

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

- Thus minimal row degrees are $1, 1$.

- Example over field $\mathbb{Z}_{11}$: $\mathcal{B} = \text{span}\left\{\left(\begin{bmatrix} 9 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \dots\right)\right.$
- has kernel representation $A(\sigma)\boldsymbol{w} = 0$ 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 $R(\sigma)\boldsymbol{w} = 0$ 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 $\mathbb{Z}_{11}$: $\mathcal{B} = \text{span}\left\{\left(\begin{bmatrix} 9 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \ldots\right)\right.$
- has kernel representation $A(\sigma)\boldsymbol{w} = 0$ 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 $R(\sigma)\boldsymbol{w} = 0$ 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 $1, 1$.

- Dropping rank constraint: any other representation $R(\sigma)\boldsymbol{w} = 0$ of $\mathcal{B}$ 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:

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

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

Row reduced R with row degrees $d_1, \ldots, d_k$ has

PREDICTABLE DEGREE PROPERTY:

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

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

Row reduced R with row degrees $d_1, \ldots, d_k$ has

PREDICTABLE DEGREE PROPERTY:

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

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. $\max_{1 \le i \le k} (\deg q_i(\xi) + d_i) \le d$
3. $Q(\xi)$ is unique

Row reduced R with row degrees $d_1, \ldots, d_k$ has

PREDICTABLE DEGREE PROPERTY:

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

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. $\deg q_i(\xi) \le d - d_i \quad$ 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:

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

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. $\deg q_i(\xi) \le d - d_i \quad$ 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:

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

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. $\deg q_i(\xi) \le d - d_i \quad$ 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:

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

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. $\deg q_i(\xi) \le d - d_i \quad$ for $i = 1, \ldots, k$.

Furthermore, $Q(\xi)$ is unique.

- Same example over ring $\mathbb{Z}_{27}$: $\mathcal{B} = \text{span}\left\{\left(\begin{bmatrix} 9 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \ldots\right)\right.$
- note that $\mathbb{Z}_{27}$ has zero divisors, such as 3 , 9
- $\mathcal{B}$ 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 $\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \end{bmatrix}, \ldots\right)$ which is not in $\mathcal{B}$

- Same example over ring $\mathbb{Z}_{27}$: $\mathcal{B} = \text{span}\left\{\left(\begin{bmatrix} 9 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \dots\right)\right.$
- 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 $\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \end{bmatrix}, \dots\right)$ which is not in $\mathcal{B}$

- Same example over ring $\mathbb{Z}_{27}$: $\mathcal{B} = \text{span}\left\{\left(\begin{bmatrix} 9 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \dots\right)\right.$
- 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 $\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \end{bmatrix}, \dots\right)$ which is not in $\mathcal{B}$

- Same example over ring $\mathbb{Z}_{27}$: $\mathcal{B} = \text{span}\left\{\left(\begin{bmatrix} 9 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \dots\right)\right.$
- note that $\mathbb{Z}_{27}$ has zero divisors, such as 3 , 9
- $\mathcal{B}$ has kernel representation $A(\sigma)\boldsymbol{w} = 0$ with

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

- Any other representation $R(\sigma)\boldsymbol{w} = 0$ 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 $\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \end{bmatrix}, \dots\right)$ which is not in $\mathcal{B}$

- Same example over ring $\mathbb{Z}_{27}$: $\mathcal{B} = \text{span}\left\{\left(\begin{bmatrix} 9 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \dots\right)\right.$
- note that $\mathbb{Z}_{27}$ has zero divisors, such as 3 , 9
- $\mathcal{B}$ has kernel representation $A(\sigma)\boldsymbol{w} = 0$ with

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

- Any other representation $R(\sigma)\boldsymbol{w} = 0$ 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 $\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \end{bmatrix}, \dots\right)$ which is not in $\mathcal{B}$

- Same example over ring $\mathbb{Z}_{27}$: $\mathcal{B} = \text{span}\left\{\left(\begin{bmatrix} 9 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \dots\right)\right.$
- 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 $\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \end{bmatrix}, \dots\right)$ which is not in $\mathcal{B}$

- Dropping rank constraint: any other representation $R(\sigma)\boldsymbol{w} = 0$ 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 $\mathbb{Z}_{p^r}$

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

We present a solution

- Dropping rank constraint: any other representation $R(\sigma)\boldsymbol{w} = 0$ 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 $\mathbb{Z}_{p^r}$

= 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 $\mathbb{Z}_{p^r}^q$, 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 $\mathbb{Z}_{p^r}^q$, 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 $\mathbb{Z}_{p^r}^q$, 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 $\mathbb{Z}_{p^r}^q$, 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 $\mathbb{Z}_{p^r}^q$, 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 $\mathbb{Z}_{p^r}^q$, as in *Vazirani a.o. '96*

Theory of p-generator sequences for $\mathbb{Z}_{p^r}^q[\xi]$

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

DEFINITION Let $v_1(\xi), \ldots, v_k(\xi)$ be vectors in $\mathbb{Z}_{p^r}^q[\xi]$ 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 $\{v_1(\xi), \cdots, v_k(\xi)\}$.

Theory of p-generator sequences for $\mathbb{Z}_{p^r}^q[\xi]$

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

DEFINITION Let $v_1(\xi), \ldots, v_k(\xi)$ be vectors in $\mathbb{Z}_{p^r}^q[\xi]$ 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 $\{v_1(\xi), \cdots, v_k(\xi)\}$.

Theory of p-generator sequences for $\mathbb{Z}_{p^r}^q[\xi]$

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

DEFINITION Let $v_1(\xi), \ldots, v_k(\xi)$ be vectors in $\mathbb{Z}_{p^r}^q[\xi]$ 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 $\{v_1(\xi), \cdots, v_k(\xi)\}$.

Theory of p-generator sequences for $\mathbb{Z}_{p^r}^q[\xi]$

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

DEFINITION Let $v_1(\xi), \ldots, v_k(\xi)$ be vectors in $\mathbb{Z}_{p^r}^q[\xi]$ 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 $\{v_1(\xi), \cdots, v_k(\xi)\}$.

Theory of p-generator sequences for $\mathbb{Z}_{p^r}^q[\xi]$

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

DEFINITION Let $v_1(\xi), \ldots, v_k(\xi)$ be vectors in $\mathbb{Z}_{p^r}^q[\xi]$ 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 $\{v_1(\xi), \cdots, v_k(\xi)\}$.

DEFINITION Let $v_1(\xi), \ldots, v_k(\xi)$ be vectors in $\mathbb{Z}_{p^r}^q[\xi]$. 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 ***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 $v_i(\xi) \in \mathbb{Z}_{p^r}^q[\xi]$, 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 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 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 $R(\sigma)\boldsymbol{w} = 0$ 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. $R(\xi) = \begin{bmatrix} 0 & \xi^2 \\ 0 & 9\xi^2 \\ 1 & 9\xi \\ 0 & 3\xi^2 \\ 3 & 0 \\ 0 & 9\xi^2 \\ 9 & 0 \end{bmatrix}$

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 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 $\mathbb{Z}_{p^r}^q[\xi]$, 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 $\mathbb{Z}_{p^r}^q$.

Leads to concepts of

- p-dimension of M: $p\text{-dim}(M) = k$
- 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 $\mathbb{Z}_{p^r}^q[\xi]$, 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 $\mathbb{Z}_{p^r}^q$.

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 $\mathbb{Z}_{p^r}^q[\xi]$, 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 $\mathbb{Z}_{p^r}^q$.

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 $\mathbb{Z}_{p^r}^q[\xi]$, 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 $\mathbb{Z}_{p^r}^q$.

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 $R(\xi)$ 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

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

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

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

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

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

$$A(\xi) = \begin{bmatrix} 0 & \xi^2 \\ 1 & 18\xi \end{bmatrix} \quad \rightarrow^{Algorithm} \quad R(\xi) = \begin{bmatrix} 0 & \xi^2 \\ 0 & 3\xi^2 \\ 14 & 9\xi \\ \xi & 0 \\ 3 & 0 \\ 9 & 0 \end{bmatrix}$$

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 $\mathbb{Z}_{p^r}^k[\xi]$ such that

1. $V(\xi) = Q(\xi)R(\xi)$
2. $\deg q_i(\xi) \leq d - d_i \quad$ 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 $Q(\xi) = \begin{bmatrix} q_1(\xi) & \cdots & q_k(\xi) \end{bmatrix}$ in $\mathbb{Z}_{p^r}^k[\xi]$ such that

1. $V(\xi) = Q(\xi)R(\xi)$
2. $\deg q_i(\xi) \leq d - d_i \quad$ 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 $Q(\xi) = \begin{bmatrix} q_1(\xi) & \cdots & q_k(\xi) \end{bmatrix}$ in $\mathbb{Z}_{p^r}^k[\xi]$ such that

1. $V(\xi) = Q(\xi)R(\xi)$
2. $\deg q_i(\xi) \leq d - d_i \quad$ 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 $Q(\xi) = \begin{bmatrix} q_1(\xi) & \cdots & q_k(\xi) \end{bmatrix}$ in $\mathbb{Z}_{p^r}^k[\xi]$ such that

1. $V(\xi) = Q(\xi)R(\xi)$
2. $\deg q_i(\xi) \leq d - d_i \quad$ 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 $Q(\xi) = \begin{bmatrix} q_1(\xi) & \cdots & q_k(\xi) \end{bmatrix}$ in $\mathbb{Z}_{p^r}^k[\xi]$ such that

1. $V(\xi) = Q(\xi)R(\xi)$
2. $\deg q_i(\xi) \leq d - d_i \quad$ 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

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 $\boldsymbol{w} = G(\sigma)\boldsymbol{u}$ of systems over $\mathbb{Z}_{p^r}$
- apply to *convolutional codes* over $\mathbb{Z}_{p^r}$ given by encoder $\boldsymbol{w} = G(\sigma)\boldsymbol{u}$ or syndrome former $H(\sigma)\boldsymbol{w} = 0$.

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^{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^{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 $\boldsymbol{w} = G(\sigma)\boldsymbol{u}$ of systems over $\mathbb{Z}_{p^r}$
- apply to *convolutional codes* over $\mathbb{Z}_{p^r}$ given by encoder $\boldsymbol{w} = G(\sigma)\boldsymbol{u}$ or syndrome former $H(\sigma)\boldsymbol{w} = 0$.

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 $\boldsymbol{w} = G(\sigma)\boldsymbol{u}$ of systems over $\mathbb{Z}_{p^r}$
- apply to *convolutional codes* over $\mathbb{Z}_{p^r}$ given by encoder $\boldsymbol{w} = G(\sigma)\boldsymbol{u}$ or syndrome former $H(\sigma)\boldsymbol{w} = 0$.

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 $\boldsymbol{w} = G(\sigma)\boldsymbol{u}$ of systems over $\mathbb{Z}_{p^r}$
- apply to *convolutional codes* over $\mathbb{Z}_{p^r}$ given by encoder $\boldsymbol{w} = G(\sigma)\boldsymbol{u}$ or syndrome former $H(\sigma)\boldsymbol{w} = 0$.