Strongly autonomous behaviors over finite rings

Eva Zerz
RWTH Aachen University

NDS 2009
$\Theta\varepsilon\sigma\sigma\alpha\lambda o\nu\acute{\iota}\kappa\eta$

Discrete linear systems: History

$\sim$ 1200 Fibonacci: $\sigma^2 y = \sigma y + y$

Discrete linear systems: History

$\sim$ 1200 Fibonacci: $\sigma^2 y = \sigma y + y$

$\sim$ 1960s Kalman et al: $\sigma x = Ax + Bu$

Discrete linear systems: History

$\sim$ 1200 Fibonacci: $\sigma^2 y = \sigma y + y$

$\sim$ 1960s Kalman et al: $\sigma x = Ax + Bu$

$\sim$ 1970s Sontag et al: $\sigma x = Ax + Bu$ over rings
Roesser, Fornasini et al: 2D state models

Discrete linear systems: History

$\sim$ 1200 Fibonacci: $\sigma^2 y = \sigma y + y$

$\sim$ 1960s Kalman et al: $\sigma x = Ax + Bu$

$\sim$ 1970s Sontag et al: $\sigma x = Ax + Bu$ over rings
Roesser, Fornasini et al: 2D state models

$\sim$ 1980s Willems et al: $R(\sigma)w = 0$

Discrete linear systems: History

$\sim$ 1200 Fibonacci: $\sigma^2 y = \sigma y + y$

$\sim$ 1960s Kalman et al: $\sigma x = Ax + Bu$

$\sim$ 1970s Sontag et al: $\sigma x = Ax + Bu$ over rings
Roesser, Fornasini et al: 2D state models

$\sim$ 1980s Willems et al: $R(\sigma)w = 0$

$\sim$ 1990s Oberst, Rocha et al: $R(\sigma_1, \ldots, \sigma_n)w = 0$

Discrete linear systems: History

$\sim$ 1200 Fibonacci: $\sigma^2 y = \sigma y + y$

$\sim$ 1960s Kalman et al: $\sigma x = Ax + Bu$

$\sim$ 1970s Sontag et al: $\sigma x = Ax + Bu$ over rings
Roesser, Fornasini et al: 2D state models

$\sim$ 1980s Willems et al: $R(\sigma)w = 0$

$\sim$ 1990s Oberst, Rocha et al: $R(\sigma_1, \dots, \sigma_n)w = 0$

$\sim$ 2000s Kuijper et al: $R(\sigma)w = 0$ over rings
Lu, Nechaev et al: $R(\sigma_1, \dots, \sigma_n)w = 0$ over rings

Discrete linear systems: Framework

Signals: Sequences $a : T \to C$

T . . . time / index set, here: $\mathbb{N}^n$
C . . . signal alphabet, coefficient set

Signal set: $\mathcal{A} = C^T$

Discrete linear systems: Framework

Signals: Sequences $a : T \to C$

T . . . time / index set, here: $\mathbb{N}^n$
C . . . signal alphabet, coefficient set

Signal set: $\mathcal{A} = C^T$

Operators: Shifts $\sigma_i : \mathcal{A} \to \mathcal{A}$ for $i = 1, \ldots, n$

$$(\sigma_i a)(t_1, \ldots, t_n) = a(t_1, \ldots, t_i + 1, \ldots, t_n)$$

Operator set: $\mathcal{D} = C[\sigma_1, \ldots, \sigma_n]$

Signal set: $\mathcal{A}$ . . . sequences $\mathbb{N}^n \to C$

Operator set: $\mathcal{D}$ . . . linear shift operators with coeff. in C

Linear system:

vector of signals $w \in \mathcal{A}^q$

matrix of operators $R \in \mathcal{D}^{g \times q}$

$$\boxed{Rw = 0}$$

linear system of partial difference equations with coeff. in C

Signal set: $\mathcal{A}$ . . . sequences $\mathbb{N}^n \to C$

Operator set: $\mathcal{D}$ . . . linear shift operators with coeff. in C

Linear system:

vector of signals $w \in \mathcal{A}^q$

matrix of operators $R \in \mathcal{D}^{g \times q}$

$$\boxed{Rw = 0}$$

linear system of partial difference equations with coeff. in C

Behave!

$$\mathcal{B} = \{w \in \mathcal{A}^q \mid Rw = 0\}$$

What do we know?

Signals $a : \mathbb{N}^n \to C$

Operators $d = \sum_{t \in \mathbb{N}^n} c_t \sigma^t, \; c_t \in C$

What do we know?

Signals $a : \mathbb{N}^n \to C$
Operators $d = \sum_{t \in \mathbb{N}^n} c_t \sigma^t,\ c_t \in C$

Well known case: C is a field
Oberst, Rocha, Valcher, Wood, Z, . . .

Continuous counterpart:
Oberst, Pillai & Shankar, Pommaret, Quadrat, . . .

What do we know?

Signals $a : \mathbb{N}^n \to C$
Operators $d = \sum_{t \in \mathbb{N}^n} c_t \sigma^t$, $c_t \in C$

Well known case: C is a field
Oberst, Rocha, Valcher, Wood, Z, . . .

Continuous counterpart:
Oberst, Pillai & Shankar, Pommaret, Quadrat, . . .

Not so well known case: C is a (nice) ring
here: $C = \mathbb{Z}_m$, $m > 1$
Sontag, Rouchalau & Wyman, Perdon, Kuijper et al., . . .

Why? E.g. Coding theory
Fagnani & Zampieri, Nechaev et al., Rosenthal et al., . . .

Overview

- 1. Discrete linear systems: History, mathematical framework
- 2. Autonomy in the field case: Short review
- 3. Autonomy in the ring case: Known and new results
- 4. Open problems: Conclusion

Autonomy: Field case

F . . . field, $\mathcal{A} = \{a \mid a : \mathbb{N}^n \to F\}$
$\mathcal{D} = F[\sigma_1, \ldots, \sigma_n]$, $R \in \mathcal{D}^{g \times q}$

Linear system $\mathcal{B} = \{w \in \mathcal{A}^q \mid Rw = 0\}$

Autonomy: Field case

F . . . field, $\mathcal{A} = \{a \mid a : \mathbb{N}^n \to F\}$
$\mathcal{D} = F[\sigma_1, \ldots, \sigma_n]$, $R \in \mathcal{D}^{g \times q}$

Linear system $\mathcal{B} = \{w \in \mathcal{A}^q \mid Rw = 0\}$

Projection on i-th component $\quad \pi_i : \mathcal{B} \to \mathcal{A}, \quad w \mapsto w_i$

$\mathcal{B}$ autonomous $\Leftrightarrow$ none of the π_i is surjective
i.e., there are no free variables (inputs)

Theorem: $\mathcal{B}$ is autonomous $\Leftrightarrow$ R has full column rank

Autonomy: Field case

F . . . field, $\mathcal{A} = \{a \mid a : \mathbb{N}^n \to F\}$
$\mathcal{D} = F[\sigma_1, \ldots, \sigma_n]$, $R \in \mathcal{D}^{g \times q}$

Linear system $\mathcal{B} = \{w \in \mathcal{A}^q \mid Rw = 0\}$

Projection on i-th component $\quad \pi_i : \mathcal{B} \to \mathcal{A}, \quad w \mapsto w_i$

$\mathcal{B}$ autonomous $\Leftrightarrow$ none of the π_i is surjective
i.e., there are no free variables (inputs)

Theorem: $\mathcal{B}$ is autonomous $\Leftrightarrow$ R has full column rank

Rank: $\mathcal{D}$ domain $\Rightarrow$ $\mathcal{D} \hookrightarrow \mathcal{Q}$ quotient field

Interpretation in terms of trajectories

$\mathcal{B} = \{w \in \mathcal{A}^q \mid Rw = 0\}$

Theorem: [Rocha, Valcher, Wood, Z, . . .] Equivalent:

- $\mathcal{B}$ autonomous (has no free variables)
- R has full column rank

Interpretation in terms of trajectories

$\mathcal{B} = \{w \in \mathcal{A}^q \mid Rw = 0\}$

Theorem: [Rocha, Valcher, Wood, Z, . . .] Equivalent:

- $\mathcal{B}$ autonomous (has no free variables)
- R has full column rank
- $\exists N \in \mathbb{N}^n$:
  $w \in \mathcal{B}$ has finite support in $N + \mathbb{N}^n \;\Rightarrow\; w = 0$
- $\mathcal{B}$ past-determined, that is, $\exists N \in \mathbb{N}^n$:
  $w \in \mathcal{B}$ vanishes on $\mathbb{N}^n \setminus (N + \mathbb{N}^n) \;\Rightarrow\; w = 0$

Autonomy: Ring case

$\mathcal{A} = \{a \mid a : \mathbb{N}^n \to \mathbb{Z}_m\}$
$\mathcal{D} = \mathbb{Z}_m[\sigma_1, \ldots, \sigma_n]$, $m > 1$

Autonomy: Ring case

$\mathcal{A} = \{a \mid a : \mathbb{N}^n \to \mathbb{Z}_m\}$
$\mathcal{D} = \mathbb{Z}_m[\sigma_1, \ldots, \sigma_n]$, $m > 1$

Problem: $\mathcal{D}$ is not a domain (unless m is prime)

i.e., there are zero-divisors, there is no quotient field . . .

$\rightsquigarrow$ theory developed so far not directly applicable

Polynomial ring $\mathcal{D} = \mathbb{Z}_m[\sigma_1, \ldots, \sigma_n]$

$$\mathcal{D} \ni d = \sum_{t \in \mathbb{N}^n} d_t \, \sigma_1^{t_1} \cdots \sigma_n^{t_n}$$

- d nilpotent $\Leftrightarrow$ all d_t nilpotent
- d zero-divisor $\Leftrightarrow$ $\exists 0 \neq c \in \mathbb{Z}_m$: $c\, d_t = 0$ for all t
- d unit $\Leftrightarrow$ d_0 unit and all d_t for $t \neq 0$ nilpotent

Degrees of autonomy of $\mathcal{B} = \{w \in \mathcal{A}^q \mid Rw = 0\}$

Theorem [NDS 07]:

- $\exists N \in \mathbb{N}^n$: $[w \in \mathcal{B}$ has finite support in $N + \mathbb{N}^n \;\Rightarrow\; w = 0]$

$$\Downarrow$$

- R has full column rank

$$\Downarrow$$

- $\mathcal{B}$ has no free variables

But: converse of $\Downarrow$ no longer true, in general!

“Counter”-Examples

$$R = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \in \mathbb{Z}_4^{2\times 2}$$

$\mathcal{B} = \{w : \mathbb{N} \to (\mathbb{Z}_4)^2 \mid 2w = 0\}$
has no free variables
but $\text{rank}(R) < 2$

"Counter"-Examples

$$R = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \in \mathbb{Z}_4^{2\times 2}$$

$\mathcal{B} = \{w : \mathbb{N} \to (\mathbb{Z}_4)^2 \mid 2w = 0\}$
has no free variables
but rank$(R) < 2$

$$R = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \in \mathbb{Z}_4^{2\times 2}$$

$\mathcal{B} = \{w : \mathbb{N} \to (\mathbb{Z}_4)^2 \mid w_1 = 0,\ 2w_2 = 0\}$
rank$(R) = 2$
but $\exists$ non-zero trajectories with finite support in any $[N, \infty)$

The concept of rank

Clear for domains (embed into quotient field)
For arbitrary commutative rings $\mathcal{D} \neq \{0\}$ two notions of rank:
determinantal ideals

$$\mathcal{D} =: J_0(R) \supseteq J_1(R) \supseteq J_2(R) \supseteq \dots$$

The concept of rank

Clear for domains (embed into quotient field)
For arbitrary commutative rings $\mathcal{D} \neq \{0\}$ two notions of rank:
determinantal ideals

$$\mathcal{D} =: J_0(R) \supseteq J_1(R) \supseteq J_2(R) \supseteq \dots$$

- rank(R) ... largest r such that $J_r(R) \neq 0$
- red-rank(R) ... largest r such that ann($J_r(R)$) $= 0$

The concept of rank

Clear for domains (embed into quotient field)
For arbitrary commutative rings $\mathcal{D} \neq \{0\}$ two notions of rank:
determinantal ideals

$$\mathcal{D} =: J_0(R) \supseteq J_1(R) \supseteq J_2(R) \supseteq \dots$$

- rank(R) ... largest r such that $J_r(R) \neq 0$
- red-rank(R) ... largest r such that ann($J_r(R)$) $= 0$

Examples: $R = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \in \mathbb{Z}_4^{2\times 2}$ rank(R) $= 1$ red-rank(R) $= 0$

$R = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \in \mathbb{Z}_4^{2\times 2}$ rank(R) $= 2$ red-rank(R) $= 1$

Always: red-rank$(R) \leq$ rank(R)

Over domains: red-rank$(R) =$ rank(R)

Always: red-rank(R) $\leq$ rank(R)

Over domains: red-rank(R) $=$ rank(R)

Significance of reduced rank

McCoy's **Theorem:**

$\mathcal{D} \neq \{0\}$ commutative ring
$R \in \mathcal{D}^{g \times q}$

Then

$$\exists 0 \neq x \in \mathcal{D}^q : Rx = 0 \quad \Leftrightarrow \quad \text{red-rank}(R) < q$$

Theorem: Equivalent:

- $\exists N \in \mathbb{N}^n$: [$w \in \mathcal{B}$ has finite support in $N + \mathbb{N}^n \;\Rightarrow\; w = 0$]
- R has reduced full column rank
- $\exists X$ and non-zero-divisor d: $XR = dI_q$

Theorem: Equivalent:

- $\exists N \in \mathbb{N}^n$: [$w \in \mathcal{B}$ has finite support in $N + \mathbb{N}^n \;\; \Rightarrow \;\; w = 0$]
- R has reduced full column rank
- $\exists X$ and non-zero-divisor d: $XR = dI_q$

$$\Downarrow$$

R has full column rank

$$\Downarrow$$

$\exists X$ and $0 \neq d : XR = dI_q$

$$\Downarrow$$

Theorem: Equivalent:

- $\exists N \in \mathbb{N}^n$: $[w \in \mathcal{B}$ has finite support in $N + \mathbb{N}^n \;\; \Rightarrow \;\; w = 0]$
- R has reduced full column rank
- $\exists X$ and non-zero-divisor d: $XR = dI_q$

$$\Downarrow$$

$$R \text{ has full column rank}$$

$$\Downarrow$$

$$\exists X \text{ and } 0 \neq d : XR = dI_q$$

$$\Downarrow$$

Theorem: Equivalent:

- $\mathcal{B}$ has no free variables
- $\exists X$ and $0 \neq d_i$: $XR = \mathrm{diag}(d_1, \ldots, d_q)$

Past-determinedness

Theorem: Equivalent:

1. $\exists N \in \mathbb{N}^n$: $[w \in \mathcal{B}$ has finite support in $N + \mathbb{N}^n \;\Rightarrow\; w = 0]$
2. R has reduced full column rank
3. $\exists X$ and non-zero-divisor d: $XR = dI$

Past-determinedness

Theorem: Equivalent:

1. $\exists N \in \mathbb{N}^n$: $[w \in \mathcal{B}$ has finite support in $N + \mathbb{N}^n \;\Rightarrow\; w = 0]$
2. R has reduced full column rank
3. $\exists X$ and non-zero-divisor d: $XR = dI$
4. $\exists N \in \mathbb{N}^n$: $[w \in \mathcal{B}$ vanishes on $\mathbb{N}^n \setminus (N + \mathbb{N}^n) \;\Rightarrow\; w = 0]$

[NDS 07]: $1 \Leftrightarrow 2 \Leftrightarrow 3$

Clearly: $4 \Rightarrow 1$

Crucial part: $3 \Rightarrow 4$

Past-determinedness

Theorem: Equivalent:

1. $\exists N \in \mathbb{N}^n$: $[w \in \mathcal{B}$ has finite support in $N + \mathbb{N}^n \;\; \Rightarrow \;\; w = 0]$
2. R has reduced full column rank
3. $\exists X$ and non-zero-divisor d: $XR = dI$
4. $\exists N \in \mathbb{N}^n$: $[w \in \mathcal{B}$ vanishes on $\mathbb{N}^n \setminus (N + \mathbb{N}^n) \;\; \Rightarrow \;\; w = 0]$

[NDS 07]: 1 $\Leftrightarrow$ 2 $\Leftrightarrow$ 3

Clearly: 4 $\Rightarrow$ 1

Crucial part: 3 $\Rightarrow$ 4

Lemma: $d \in \mathcal{D} = \mathbb{Z}_m[\sigma_1, \ldots, \sigma_n]$ non-zero-divisor $\Rightarrow$ some multiple of d is monic (w.r.t. a chosen term order)

Open problems

- Constructive aspects: effective Gröbner basis theory over $\mathbb{Z}_m$
  (recent release of Singular 3-1-0 admits GB computation)

Open problems

- Constructive aspects: effective Gröbner basis theory over $\mathbb{Z}_m$
  (recent release of Singular 3-1-0 admits GB computation)

- Well-posed initial value problems for past-determined systems

Open problems

- Constructive aspects: effective Gröbner basis theory over $\mathbb{Z}_m$
  (recent release of Singular 3-1-0 admits GB computation)

- Well-posed initial value problems for past-determined systems

- $\mathbb{Z}_m$-module structure of $\mathcal{B}$, e.g., finitely generated?

Open problems

- Constructive aspects: effective Gröbner basis theory over $\mathbb{Z}_m$
  (recent release of Singular 3-1-0 admits GB computation)

- Well-posed initial value problems for past-determined systems

- $\mathbb{Z}_m$-module structure of $\mathcal{B}$, e.g., finitely generated?

- Generalization of finite-dim. behaviors over fields

Conclusion

- Reasonably well understood:

$$\mathcal{D} = F[\sigma_1, \ldots, \sigma_n] \quad \text{and} \quad \mathcal{A} = \{a \mid a : \mathbb{N}^n \to F\}$$

  where F is a field

Conclusion

- Reasonably well understood:

$$\mathcal{D} = F[\sigma_1, \ldots, \sigma_n] \quad \text{and} \quad \mathcal{A} = \{a \mid a : \mathbb{N}^n \to F\}$$

  where F is a field

- Autonomy:
  no free variables $\Leftrightarrow$ fcr $\Leftrightarrow$ past-determined

Conclusion

- Reasonably well understood:

$$\mathcal{D} = F[\sigma_1, \ldots, \sigma_n] \quad \text{and} \quad \mathcal{A} = \{a \mid a : \mathbb{N}^n \to F\}$$

  where F is a field

- Autonomy:
  no free variables $\Leftrightarrow$ fcr $\Leftrightarrow$ past-determined

- Applications in coding $\rightsquigarrow$
  replace field F by more general rings, here: $\mathbb{Z}_m$

$\boxed{\text{Conclusion}}$

- Reasonably well understood:

$$\mathcal{D} = F[\sigma_1, \ldots, \sigma_n] \quad \text{and} \quad \mathcal{A} = \{a \mid a : \mathbb{N}^n \to F\}$$

  where F is a field

- Autonomy:
  no free variables $\Leftrightarrow$ fcr $\Leftrightarrow$ past-determined

- Applications in coding $\leadsto$
  replace field F by more general rings, here: $\mathbb{Z}_m$

- Autonomy:
  no free variables $\Leftarrow$ fcr $\Leftarrow$ past-determined $\Leftrightarrow$ red-fcr