Network coding theory via commutative algebra

李碩彥 (Bob Li)
The Chinese University of Hong Kong

Playing “*The Butterfly Lovers*” melody

Practical concern with CNC

Long-distance symbol-level synchronization is difficult, e.g.,

- when a symbol b misses the synchronization by a unit time (say, a μs), it becomes bD.

LNC	**Acyclic network**	**Data unit** $\in \mathbb{F}$
CNC	**Any network**	**Data unit** $\in \mathbb{F}[(D)]$
Abstract generalization	**Any network**	**Data unit** $\in$ **Some algebraic structure that shares the key property of** $\mathbb{F}[(D)]$

Algebraic properties of the ring $\mathbb{F}[(D)]$

Inside the ring $\mathbb{F}[(D)]$, the ideal $\langle D^t \rangle$ represents things that happen from the time t onward.

Key property: All ideals in the ring $\mathbb{F}[(D)]$ form a strictly descending chain

$$\langle D \rangle \supset \langle D^2 \rangle \supset \ldots \supset \langle D^t \rangle \supset \ldots \to \{0\}$$

// Anything infinitely delayed is null.

What algebraic structures share this key property?

Recall that CNC expands the polynomial ring $\mathbb{F}[D]$ into the ring $\mathbb{F}[(D)]$ of rational power series by making everything, except time, invertible.

This means localization of the ring $\mathbb{F}[D]$ at the ideal $\langle D \rangle$.

Algebraic properties of the ring $\mathbb{F}[(D)]$

Just ignore this slide if it contains foreign language to you. Relax!

$\mathbb{F}[D]$ is a PID, and $\langle D \rangle$ is a prime ideal. // In fact, a maximal ideal

Localization results in a local ring $\mathbb{F}[(D)]$,
which is also a PID.
A discrete valuation ring (DVR)

Terminology. When a local ring is a DVR, the generator z of the unique maximal ideal is called the uniformizer.

The key property of $\mathbb{F}[(D)]$ is typical for a DVR:

- All ideals in the DVR form a strictly descending chain

$$\langle z \rangle \supset \langle z^2 \rangle \supset \ldots \supset \langle z^t \rangle \supset \ldots \rightarrow \{0\}$$

// By, e.g., *Nakayama's Lemma*
// Unidirectional, just like time.

Algebraic structures

	+	–	*	/	Examples	Remarks
Field $\mathbb{F}$	√	√	√	√	$\mathbb{Q}$ = {rational #s}, $\mathbb{R}$ = {real #s}, $\mathbb{F}(x)$ = {rational functions}	
Ring (commutative ring with id)	√	√	√	×	$\mathbb{R}\times\mathbb{R}$, $\mathbb{Z}$ = {integers}	Zero divisor: $(2, 0)*(0, 5) = (0, 0)$

Ideals in a ring

- In a ring $\mathbb{R}$, the ideal generated by element a is

$$\{ax : x \in \mathbb{R}\} = \langle a \rangle = a \cdot \mathbb{R}$$

- Thus, $\langle a \rangle \supset \langle b \rangle$ means that $a \mid b$.

  // Then, a/b makes sense when $\mathbb{R}$ is an *integral domain*.

- The ideal generated by elements a, b, c is

$$\{ax+by+cz : x, y, z \in \mathbb{R}\} = \langle a, b, c \rangle$$

- The ring $\mathbb{F}[[D]] = \{$symbol pipelines starting at a time $\geq 0\}$.

  The ideal $D^3 \cdot \mathbb{F}[[D]] = \{$symbol pipelines starting at a time $\geq 3\}$.

- The ring $\mathbb{F}[(D)] = \{$"rational pipelines" starting at a time $\geq 0\}$.

  The ideal $D \cdot \mathbb{F}[(D)] = \{$"rational pipelines" starting at a time $\geq 1\}$.

Ring, field, integral domain, & PID

	$+-*$	/	Examples	Remarks
Ring (commutative ring with id)	√	✗	$\mathbb{R}\times\mathbb{R}$	Zero = (0, 0). ∃ zero divisor, which is not invertible: (2, 0)∗(0, 5) = zero
Integral domain	√	✗√	$\mathbb{Z}[x]$	∃ non-principal ideal: $\langle 2, x\rangle \neq \langle any\rangle$
Principal ideal domain (PID) $\mathbb{P}$	√	✗√	$\mathbb{Z}$, $\mathbb{F}[x]$	Ideal ↔ element up to invertible factor. Good enough for basic linear algebra. Ordering among ideals via inclusion is partial.
Discrete valuation ring (DVR) $\mathbb{D}$	√	✗√	$\mathbb{F}[(D)]$, $\mathbb{F}[[D]]$	All ideals form a linear chain.
Field $\mathbb{F}$	√	√	$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{F}(x)$	The only ideal is {0}.

Synchronization concern → general DVR

Long-distance symbol-level synchronization is difficult, e.g.,

- when a symbol b misses the synchronization by a unit time (say, a μs), it becomes bD.

LNC	**Acyclic network**	**data unit** $\in \mathbb{F}$
CNC	**Any network**	**data unit** $\in \mathbb{F}[(D)]$
Abstract NC	**Any network**	**data unit** $\in \mathbb{D}$**, a DVR**

Generality enhances applicability.

A DVR is not restricted to time-multiplexing of data symbols.

Example. When the uniformizer z of a DVR represents a unit shift in any domain other than time (e.g., space, phase, frequency, wavelength, or code), then the DVR-based NC is insensitive to imprecision in inter-node synchronization.

Generality. The uniformizer of a DVR is not necessarily a shift in any particular domain.

Open problem. Identify explicit application of NV based on a general DVR.

$\mathbb{F}[(D)] \rightarrow$ PID $\rightarrow$ DVR

$\mathbb{Z}$ = A handy example of PID

$\mathbb{F}[(D)]$ for CNC

DVR

PID suffices for linear algebra

Contents

- **PID-based network coding**
- **DVR-based causal network coding**

Based mainly on:

[Li-Sun, "Network coding theory via commutative algebra," IEEE Trans. IT., 1/2011]

Contents

- **PID-based network coding**
  - **Non-singular and normal network codes**
  - Existence of optimal code
- DVR-based causal network coding

$\mathbb{P}$-linear network code

Let $\mathbb{P}$ denote a PID.

Definition. A $\mathbb{P}$-linear network code assigns a coding coefficient $k_{d,e} \in \mathbb{P}$ to every adjacent pair (d, e) of channels.
Moreover, a $\mathbb{P}$-linear network code is normal if it is associated with a unique set of coding vectors f_e.

Normality is crucial for:

- Message propagation — The coding vector f_e unambiguously specifies a data unit $\in \mathbb{P}$ to be transmitted over a channel e.
- Message reception — A node decodes by its incoming coding vectors rather than by coding coefficients.

Rules over coding vectors

Terminology. A channel is called an *s*-channel or a link depending whether its originating end is the source *s*.

A set of coding vectors f_e satisfies the following w.r.t. the coding coefficients:

Initialization. Coding vectors of *s*-channels form the natural basis of $\mathbb{F}^{\omega}$, where ω is the message size. Thus,

$$[f_e]_{e:\ s\text{-channel}} = \text{the identity matrix } I_{\omega}$$

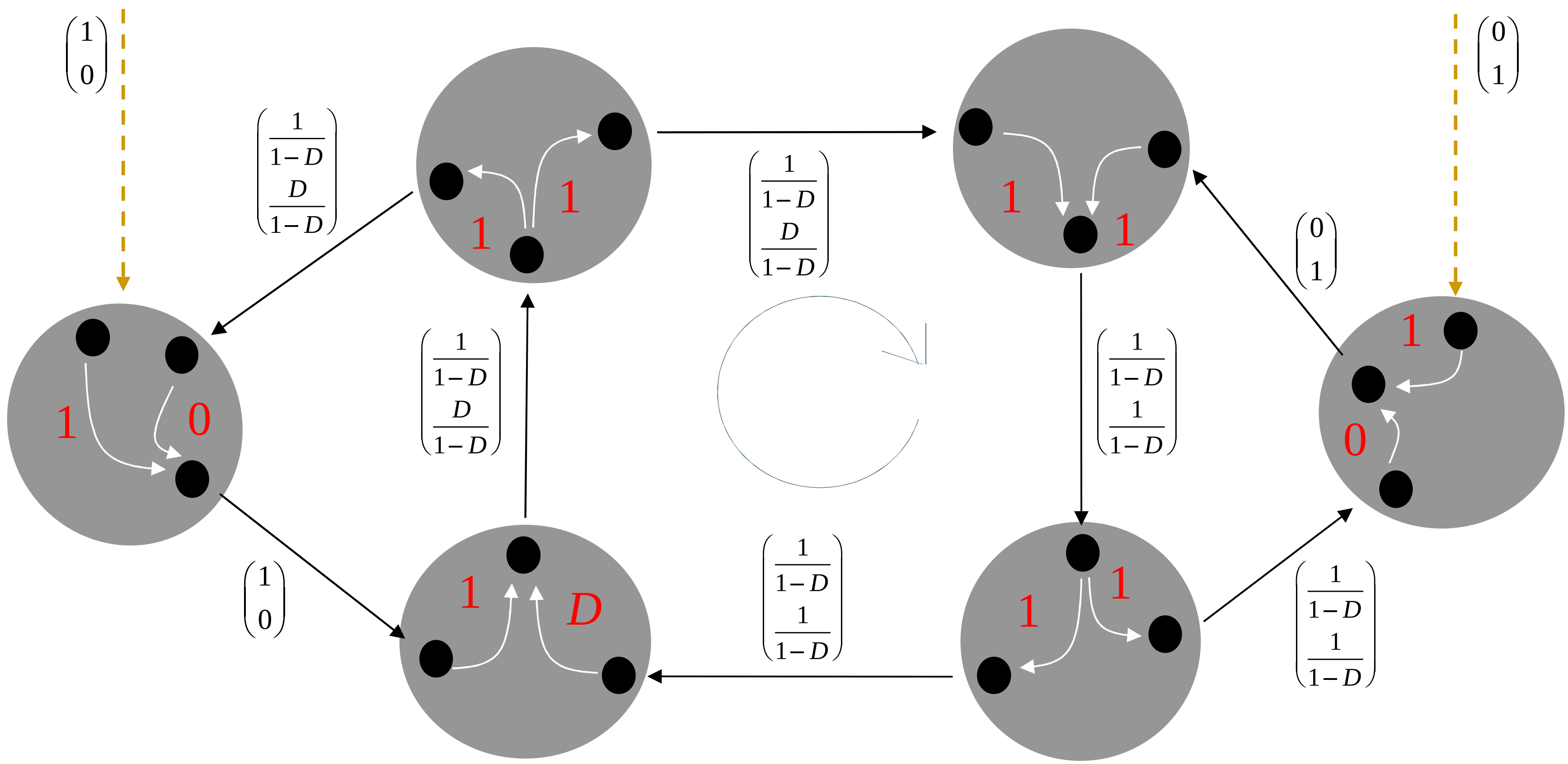
Recursion. For an outgoing link *e* from a node *v* ($\neq s$),

$$f_e = \sum_{d \in \mathrm{In}(v)} f_d\, k_{d,e}$$

Example of normal convolutional NC

Initialization. Coding vectors of *s*-channels form the natural basis of $\mathbb{P}^{\omega}$.

Recursion. For an outgoing link *e* from a node *v*, $f_e = \sum_{d\in \mathrm{In}(v)} f_d\, k_{d,e}$



Calculation of coding vectors

Initialization. Coding vectors of *s*-channels form the natural basis of $\mathbb{P}^{\omega}$.

$$[f_e]_{e:\ s\text{-channel}} = \text{the identity matrix } I_\omega$$

Recursion. For an outgoing link e from a node v, $f_e = \sum_{d\in \mathrm{In}(v)} f_d\, k_{d,e}$

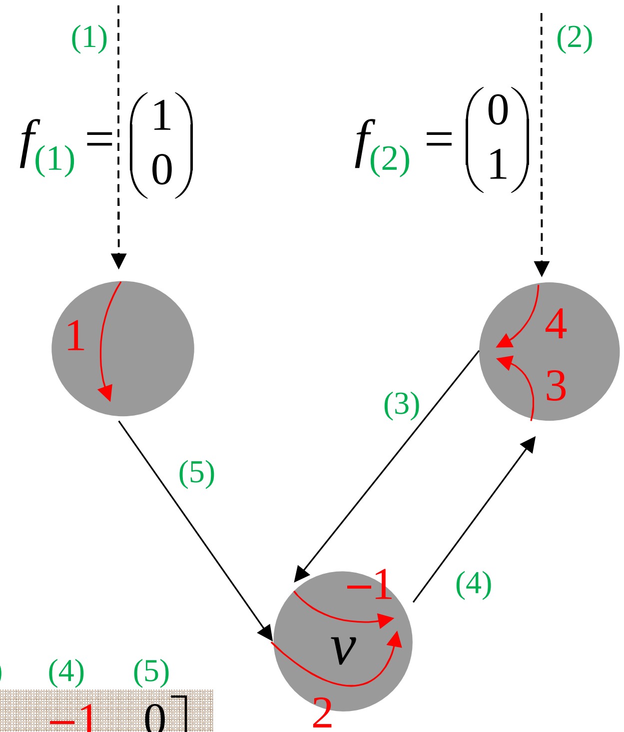
$$f_e = \sum_{d\in \mathrm{In}(v)} f_d\, k_{d,e}$$
$$= \sum_{s\text{-channel } d\in \mathrm{In}(v)} f_d\, k_{d,e} + \sum_{\text{link } d\in \mathrm{In}(v)} f_d\, k_{d,e}$$

$$= \begin{bmatrix} \vdots \\ k_{d,e} \\ \vdots \end{bmatrix}_{d:\ s\text{-channel}} + \sum_{\text{link } d\in \mathrm{In}(v)} f_d\, k_{d,e}$$

Coding vectors

Equation. For an outgoing link e from v,

$$f_e = \begin{bmatrix} \vdots \\ k_{d,e} \\ \vdots \end{bmatrix}_{d:\ s\text{-channel}} + \sum_{\text{link } d \in \mathrm{In}(v)} f_d\, k_{d,e}$$



Example. Take $f_e = f_{(3)}, f_{(4)}, f_{(5)}$ together.

$$\begin{bmatrix} f_{(3)} & f_{(4)} & f_{(5)} \end{bmatrix} = \begin{array}{c} \\ (1) \\ (2) \end{array} \!\!\begin{array}{c} \begin{array}{ccc} (3) & (4) & (5) \end{array} \\ \begin{bmatrix} 0 & 0 & 1 \\ 4 & 0 & 0 \end{bmatrix} \end{array} + \begin{bmatrix} f_{(3)} & f_{(4)} & f_{(5)} \end{bmatrix} \bullet \begin{array}{c} \\ (3) \\ (4) \\ (5) \end{array} \!\!\begin{array}{c} \begin{array}{ccc} (3) & (4) & (5) \end{array} \\ \begin{bmatrix} 0 & -1 & 0 \\ 3 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix} \end{array}$$

Notation. $F = A + F \bullet B$

Calculation for coding vectors

Try to solve *F* in terms of *A* and *B* from:

$$\boxed{F = A + F\,B}$$

$$F \cdot (I_l - B) = A$$ // Write l for the number of links.

$$\det(I_l - B)\, F = A \cdot \mathrm{Adj}(I_l - B)$$ // Adj = Adjugate matrix

The special case of an acyclic network:

The upstream-to-downstream order

$\Rightarrow$ B is a strictly triangular matrix

$\Rightarrow$ $\det(I_l - B) = 1$ & $\mathrm{Adj}(I_l - B) = (I_l - B)^{-1}$

$\Rightarrow$ **Unique solution**: $F = A \cdot (I_l - B)^{-1}$

Optimal Linear Network Codes on acyclic network

Definition. An $\mathbb{F}$-linear network code ($\mathbb{F}$-LNC) is said to be **optimal** when

- Incoming coding vectors to every receiver v generate a subspace of $\mathbb{F}^{\omega}$ with the full rank ω.

For each receiver v, create ω edge-disjoint paths starting from s-channels and ending at incoming links to v.

// if necessary append a new source node

Notation. Let C_v be an $(|E|-\omega)\times\omega$ index matrix in which

- rows are indexed by links;
- columns are indexed by s-channels;
- the $(e, d)^{\text{th}}$ entry in C_v is 1 when one of the ω paths starts with d and ends with the incoming link e to v and is 0 otherwise.

Existence of Optimal LNC on acyclic network

Corollary. An $\mathbb{F}$-LNC is optimal if, for each receiver v,

- the matrix $A\cdot(I-B)^{-1}\cdot C_v$ is nonsingular (and has the full rank ω)
- or, equivalently, the matrix $\begin{bmatrix} A & 0 \\ I-B & C_v \end{bmatrix}$ is nonsingular.

$$\begin{bmatrix} I_\omega & -A(I-B)^{-1} \\ 0 & (I-B)^{-1} \end{bmatrix} \begin{bmatrix} A & 0 \\ I-B & C_v \end{bmatrix} = \begin{bmatrix} 0 & A\cdot(I-B)^{-1}\cdot C_v \\ I & (I-B)^{-1}\cdot C_v \end{bmatrix}$$

Existence of Optimal LNC on acyclic network

Lemma. If $|\mathbb{F}|$ exceeds the degree of every x_i in a polynomial $g(x_1, \ldots, x_n)$ over $\mathbb{F}$, then there exist $a_1, \ldots, a_n \in \mathbb{F}$ such that $g(a_1, \ldots, a_n) \neq 0$.

Proof. By induction on n.

Theorem 1. An optimal $\mathbb{F}$-LNC exists when $|\mathbb{F}| > \delta$ (= number of receivers).

Proof. Regard every coding coefficient $k_{d,e}$ as an indeterminate. The degree of every indeterminate is at most 1 in $\det\begin{bmatrix} A & 0 \\ I-B & C_v \end{bmatrix}$ for every v and hence at most δ in $\prod_{v:\,\text{receiver}} \begin{bmatrix} A & 0 \\ I-B & C_v \end{bmatrix}$. The above Lemma now applies. ■

Task. Fill matrices A and B with coding coefficient $k_{d,e}$ and achieve nonsingularity of the δ matrices $\begin{bmatrix} A & 0 \\ I-B & C_v \end{bmatrix}$.

Schwartz-Zippel Lemma and an extension

Schwartz-Zippel Lemma. Let $g(x_1, \ldots, x_n)$ be a polynomial of degree $\delta > 0$ over $\mathbb{F}$, and $a_1, \ldots, a_n$ be independently and uniformly selected scalars from $\mathrm{F} \subseteq \mathbb{F}$. Then,

$$\Pr\{g(a_1, \ldots, a_n) = 0\} \le \delta / |\mathrm{F}|$$

Proof. By induction on n. // $\Pr\{g(a_1, \ldots, a_n) \neq 0\} \ge 1 - \delta / |\mathrm{F}|$

Extension. Consider a polynomial $g(x_1, \ldots, x_n)$ of a total degree δm over $\mathbb{F}$ such that the degree of each indeterminate is no more than δ. Let $a_1, \ldots, a_n$ be independently and uniformly selected scalars from $\mathrm{F} \subseteq \mathbb{F}$. Then,

$$\Pr\{g(a_1, \ldots, a_n) \neq 0\} \ge (1 - \delta / |\mathrm{F}|)^m$$

Proof. Refer to Lemma 4 in [Ho *et al*., "*A random linear network coding approach to multicast*"].

Optimality of Random LNCs

Theorem. Let $|\mathbb{F}| > \delta$. Construct an $\mathbb{F}$-LNC with coding coefficients independently and uniformly chosen from $\mathbb{F}$. Then, the probability for the $\mathbb{F}$-LNC to be optimal is at least $(1 - \delta / |\mathbb{F}|)^{|E|}$.

Proof. In the extended lemma, let $g(x_1, \ldots, x_n) = \prod_{v\text{: receiver}} \begin{bmatrix} A & 0 \\ I-B & C_v \end{bmatrix}$

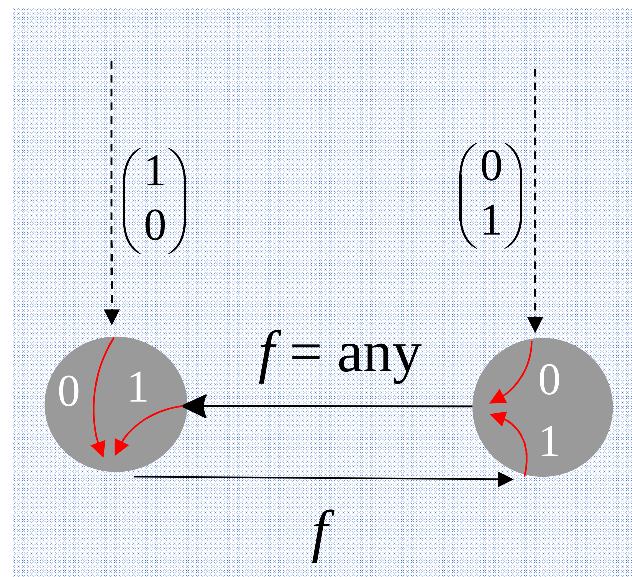
and $m = |E|$. ■

Nonsingularity and normality

For a $\mathbb{P}$-linear network code, $\det(I_l - B)\, F = A \cdot \mathrm{Adj}(I_l - B)$

$\det(I_l - B) = 0$ → None or multiple solutions for $[f_e]_{e \in E}$

$\det(I_l - B) \neq 0$ → Nonsingular code



Nonsingularity and normality

For a $\mathbb{P}$-linear network code, $\det(I_l - B)\, F = A \cdot \mathrm{Adj}(I_l - B)$

$\det(I_l - B) = 0$

None or multiple solutions for $[f_e]_{e \in E}$

$\det(I_l - B) \neq 0$

Nonsingular code

$\det(I_l - B)$ divides all entries in the matrix $A \cdot \mathrm{Adj}(I_l - B)$.
$\therefore$ Unique solution

Normal code

Otherwise

No solution

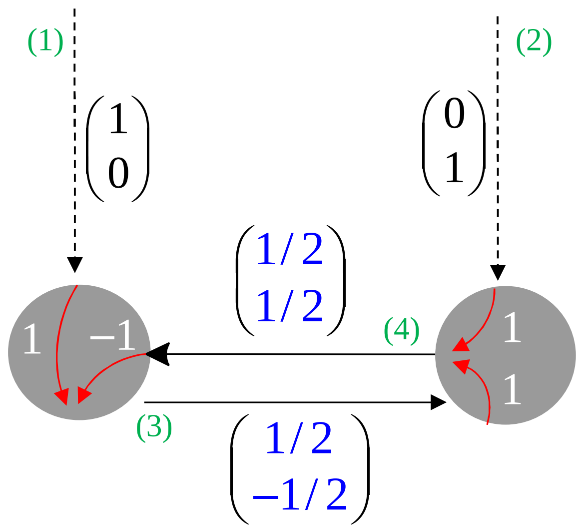
Nonsingularity $\not\Rightarrow$ normality over $\mathbb{P}$

Example. $\mathbb{P} = \mathbb{Z}$, $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $l = 2$

$\therefore\ I_l - B = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$ and $\mathrm{Adj}(I_l - B) = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$

This $\mathbb{Z}$-linear network code is nonsingular because $\det(I_l - B) = 2 \neq 0$.

But, it is not normal as 2 does not divide entries in $A \cdot \mathrm{Adj}(I_l - B) = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$



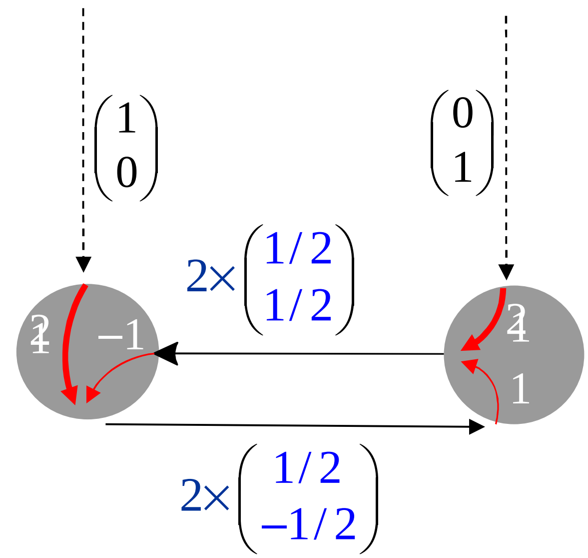
"Coding vectors" exist over $\mathbb{Q}$, the quotient field of $\mathbb{Z}$.

Normalization of a nonsingular code

When $\det(I_l - B) \neq 0$, we can force it to be a divisor of all entries in the matrix $A \cdot \mathrm{Adj}(I_l - B)$ by: // A contains $k_{d,e}$ with s-channel d.

- Simply multiply every entry in A with $\det(I_l - B)$.

$$\det(I_l - B) = 2$$

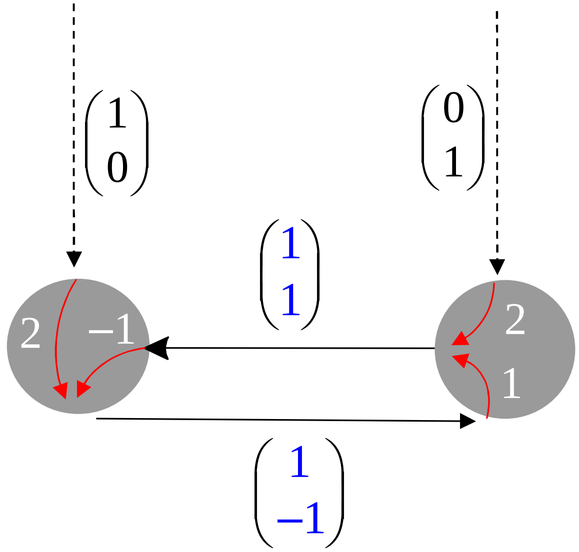


"Coding vectors" exist over $\mathbb{Q}$, the quotient field of $\mathbb{Z}$.

Normalization of a nonsingular code

When $\det(I_l - B) \neq 0$, we can force it to be a divisor of all entries in the matrix $A \cdot \mathrm{Adj}(I_l - B)$ by: // A contains $k_{d,e}$ with s-channel d.

- Simply multiply every entry in A with $\det(I_l - B)$.



The nonsingular code becomes normal.
Coding vectors now exist over $\mathbb{Z}$.

Contents

- **PID-based network coding**
  - **Non-singular and normal network codes**
  - **Existence of optimal code**
- **DVR-based causal network coding**

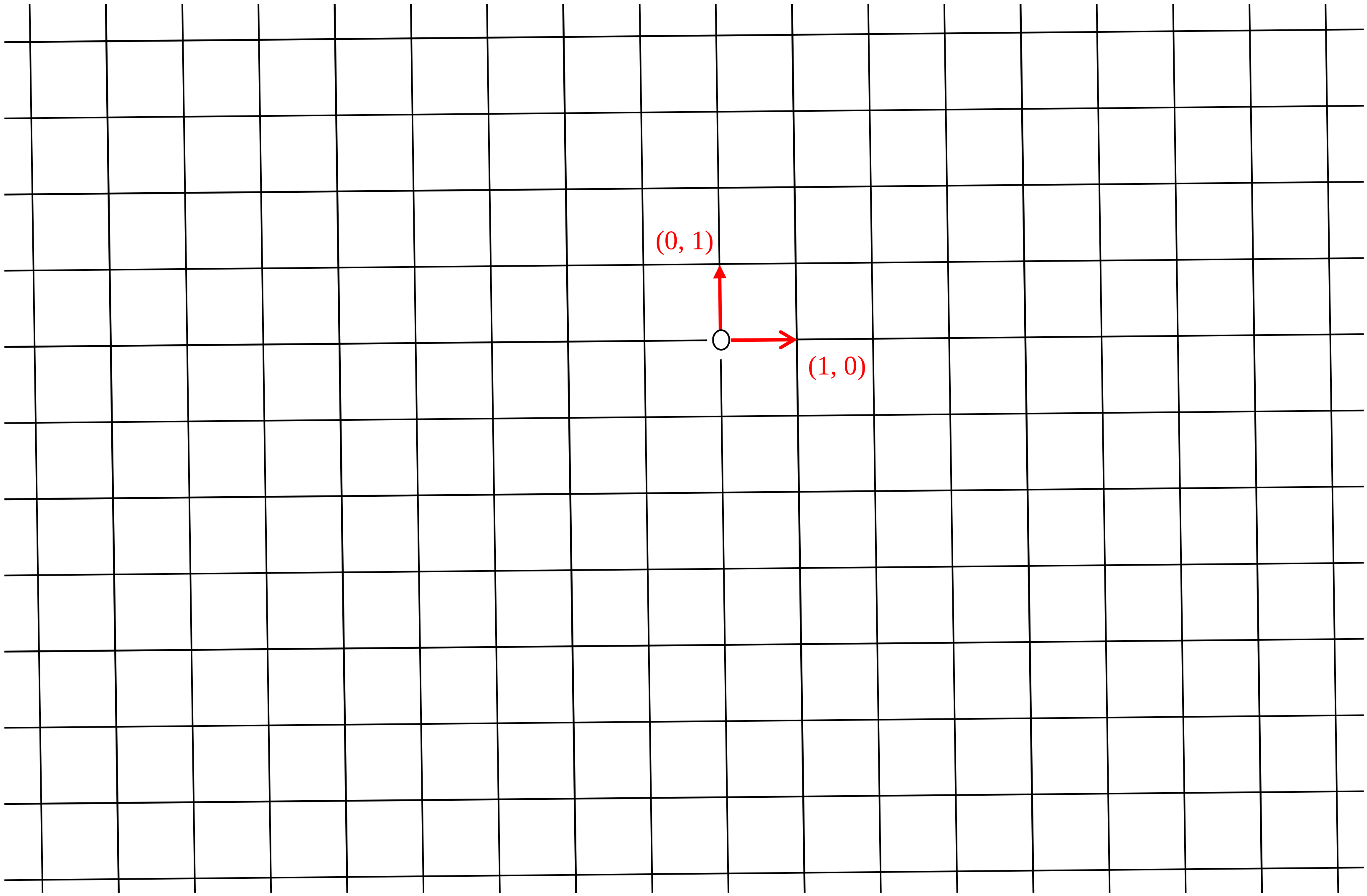
Inv. Factor Thm. of Free Submodule over a PID

By Invariant Factor Theorem of Free Submodule over a PID, every submodule of $\mathbb{P}^{\omega}$ is a free module over $\mathbb{P}$. // Free $\Rightarrow$ It has a rank $\leq \omega$.

We now illustrate this theorem with $\mathbb{P} = \mathbb{Z}$.

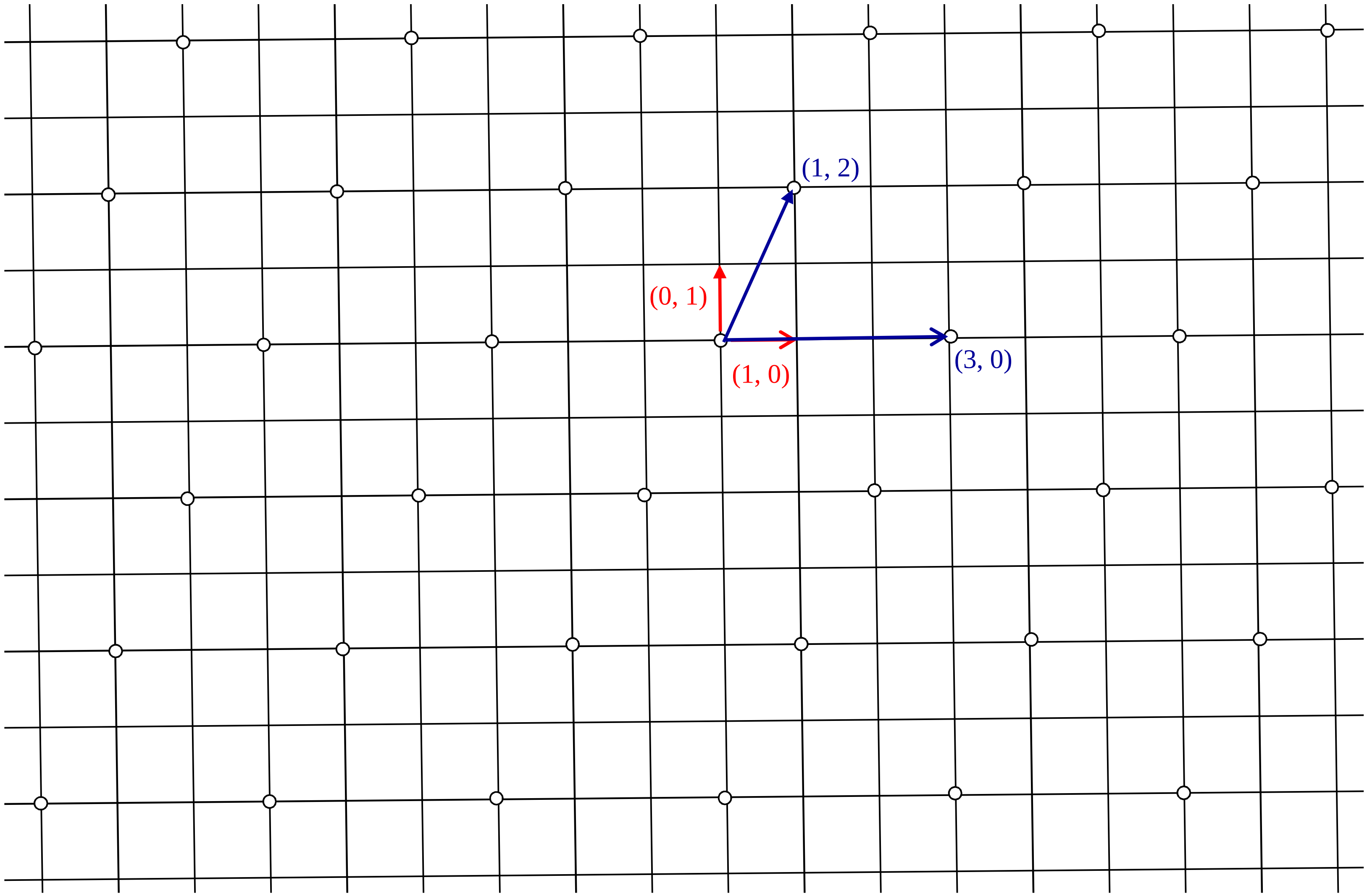
Inv. Factor Thm. of Free Submodule over a PID (= $\mathbb{Z}$)

Lattice points on the grid = $\mathbb{Z}^2$, a free $\mathbb{Z}$-module at the rank 2.



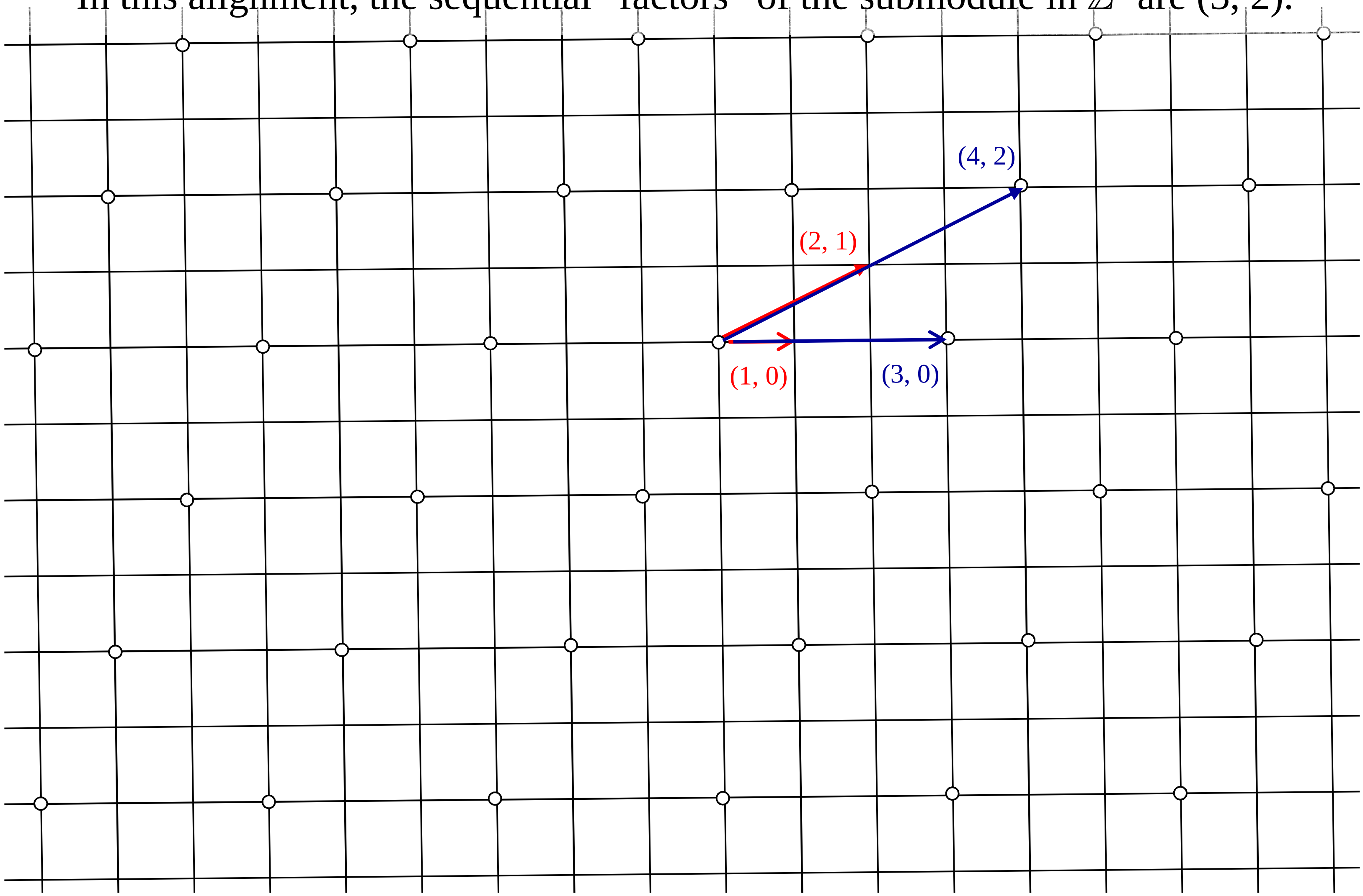
A submodule of a free $\mathbb{Z}$-module is automatically free.

The exemplifying submodule is at the rank 2 with a basis as shown.



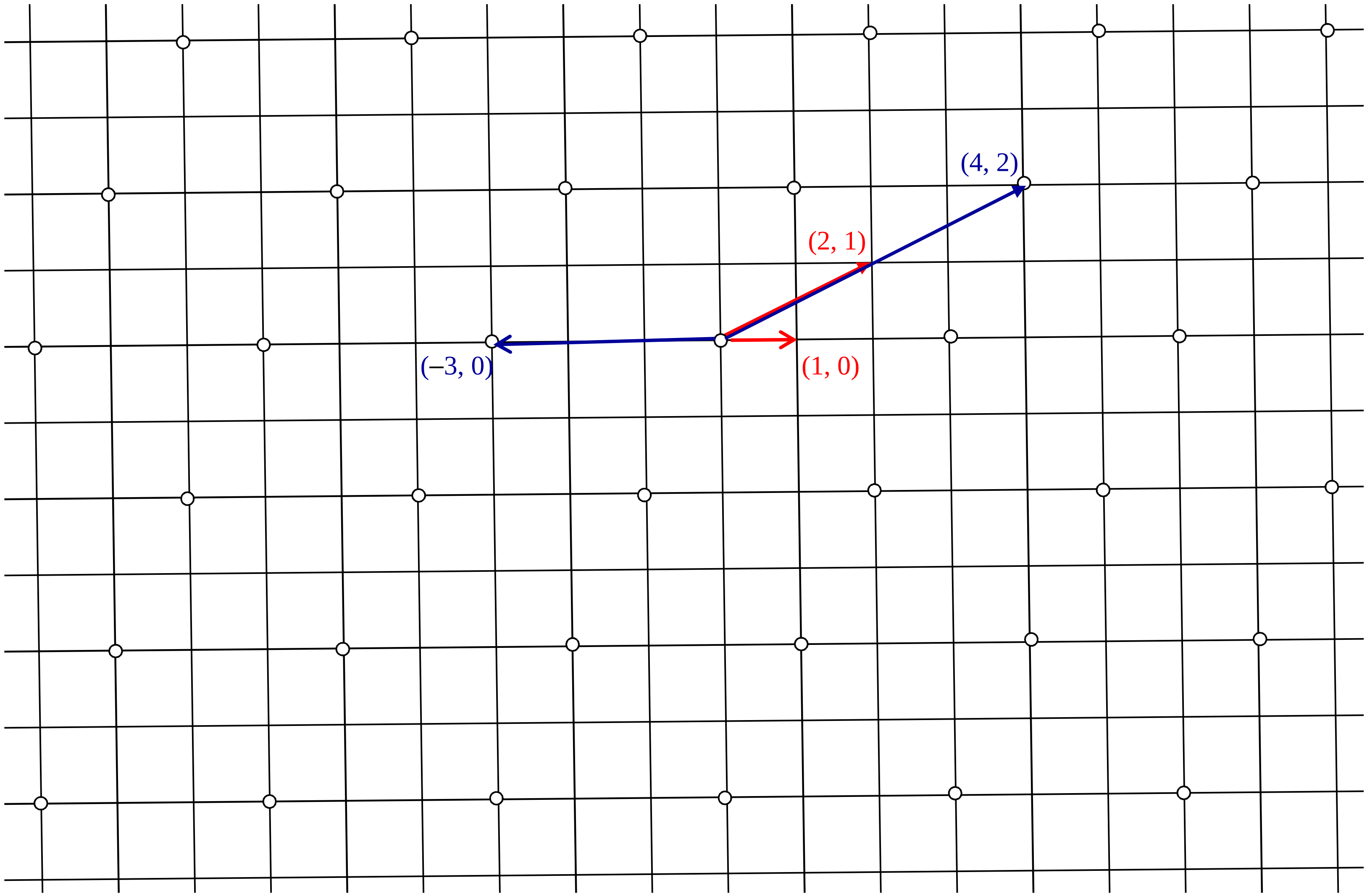
PID $\Rightarrow$ The submodule is also free, and the bases of can be aligned.

In this alignment, the sequential “factors” of the submodule in $\mathbb{Z}^2$ are (3, 2).



Another way to align the two bases

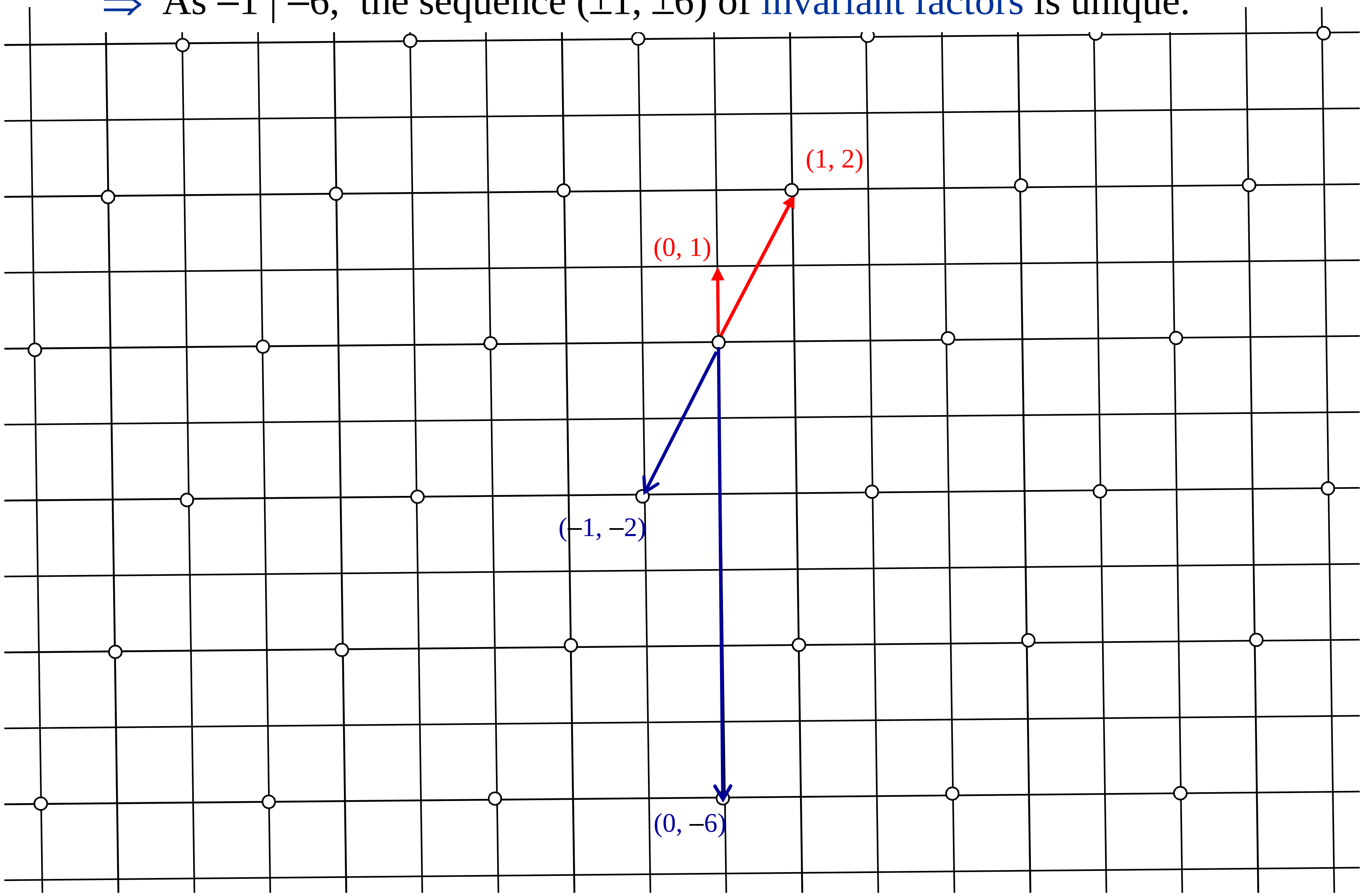
The sequential "factors" of the submodule in $\mathbb{Z}^2$ now become $(-3, 2)$.



PID ⇒ Can so align that “factors” divide one another

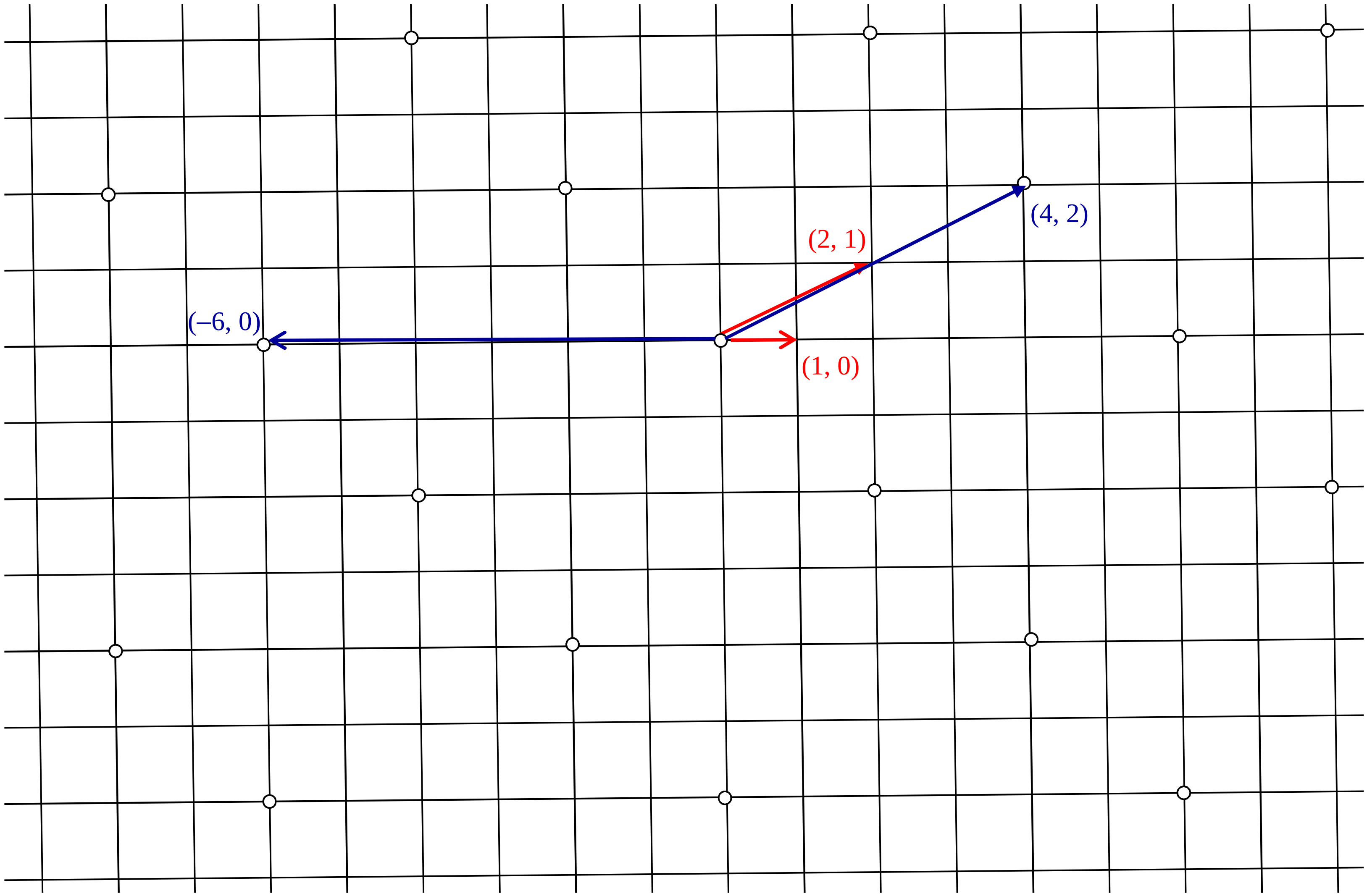
The sequential “factors” of the submodule in $\mathbb{Z}^2$ now become $(-1, -6)$.

⇒ As $-1 \mid -6$, the sequence $(\pm 1, \pm 6)$ of invariant factors is unique.



A smaller submodule at the rank 2

The invariant factors of this smaller submodule in $\mathbb{Z}^2$ are $(\pm 2, \pm 6)$.



$\mathbb{P}$-linear network code with optimal data reception

Let f_e be coding vectors of a normal $\mathbb{P}$-linear network code.

By Invariant Factor Theorem of Free Submodule over a PID, incoming coding vectors to a node v generate a free submodule of $\mathbb{P}^\omega$. The rank of this submodule is the data reception rate of v.

Definition. A normal $\mathbb{P}$-linear network code is said to be optimal when

- The data reception rate of every node v = maxflow from s to v.

Existence of optimal $\mathbb{P}$-linear NC

Theorem 1. There exists an optimal $\mathbb{P}$-linear NC when $|\mathbb{P}|$ is sufficiently large.

Proof. The fundamental theorem of LNC asserts the existence of an optimal $\mathbb{F}$-linear NC with all coding coefficients in any sufficiently large subset of $\mathbb{F}$.

So we may assume that $\mathbb{P}$ is *not* a field and hence is an infinite PID.

Applying the Lemma 1 to $\mathbb{F}$ = quotient field of $\mathbb{P}$, there exists

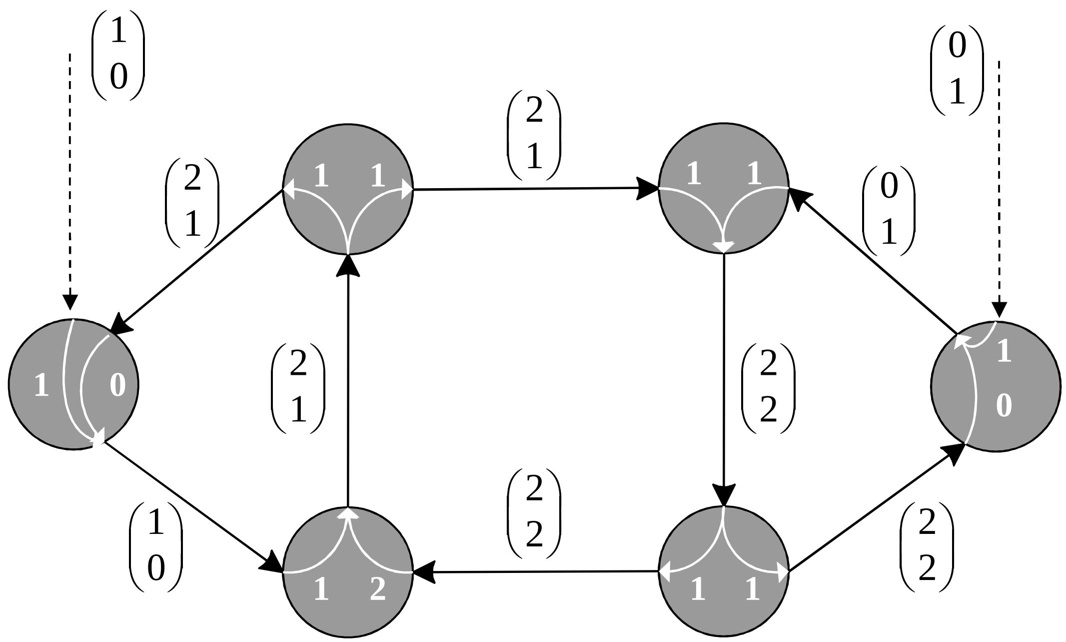
- an optimal $\mathbb{F}$-linear NC with coding coefficients in $\mathbb{P}$.

This NC qualifies as

- a nonsingular $\mathbb{P}$-linear network code.

Normalize the code into an optimal $\mathbb{P}$-linear NC.

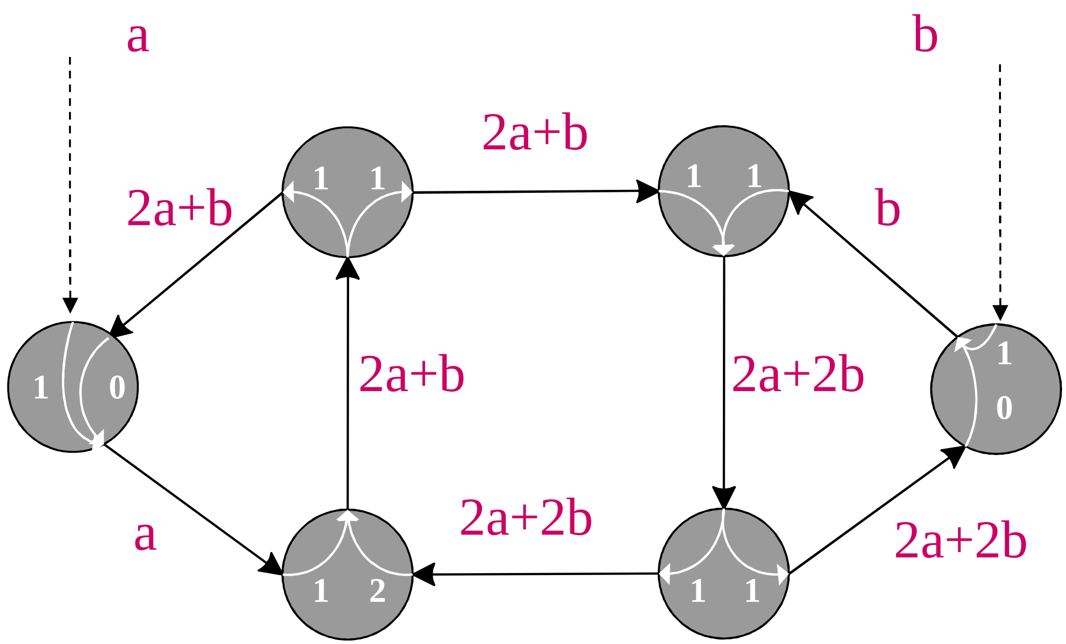
An optimal normal NC over $\mathbb{P}$ = GF(3)



A normal GF(3)-linear code on the *Shuttle Network*

An optimal normal NC over $\mathbb{P}$ = GF(3)

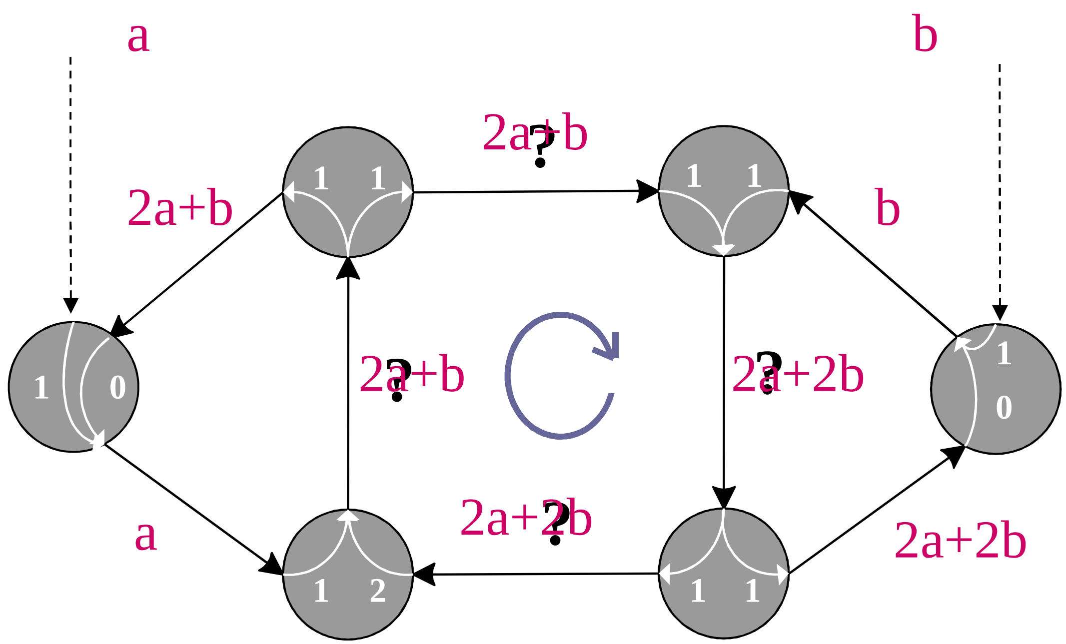
Message = (a b)



A normal GF(3)-linear code on the *Shuttle Network*

Deadlock in cyclic data propagation

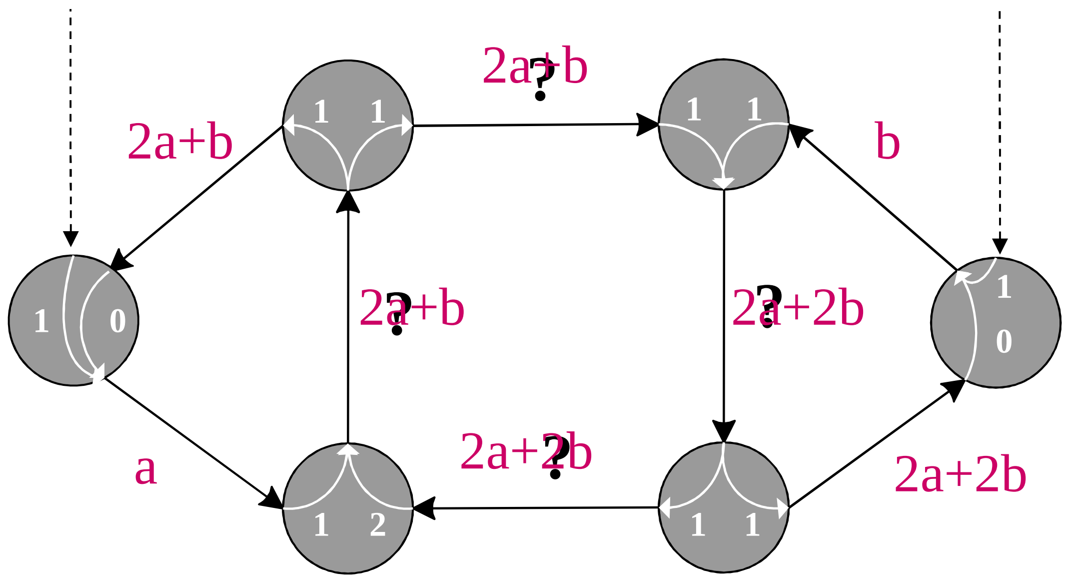
Message = (a b)



A normal GF(3)-linear code on the *Shuttle Network*

Deadlock in cyclic data propagation

To break deadlock in data propagation, we need some kind of acyclic attribute of either the network topology or the algebraic structure of data units.



In this case, the network contains cycles and the PID $\mathbb{P}$ = GF(3) does not provide the needed acyclic attribute either.

Contents

- PID-based network coding
  - Non-singular and normal network codes
  - Existence of optimal code

Open problem. Formulate something nice in between for an acyclic attribute.

- DVR-based causal network coding
  - Existence of optimal code
  - Decoding

$\mathbb{D}$-linear NC and causality

Definition. A $\mathbb{D}$-linear network code is said to be causal if:

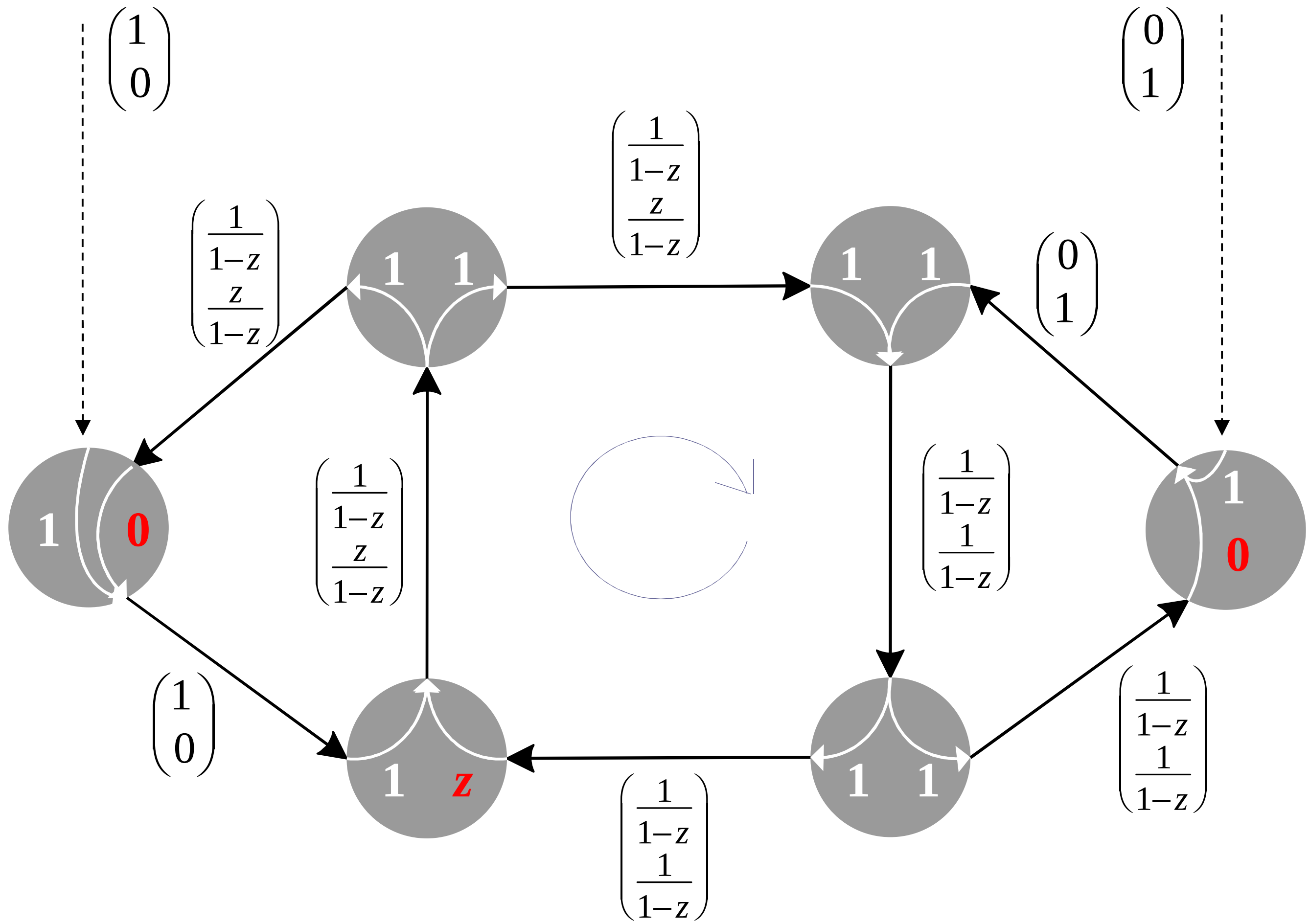
- On every cycle, at least one pair (d, e) is with $k_{d,e}$ divisible by z,

// z = uniformizer in $\mathbb{D}$

Theorem 2. Causality $\Rightarrow$ normality for a $\mathbb{D}$-linear network code.

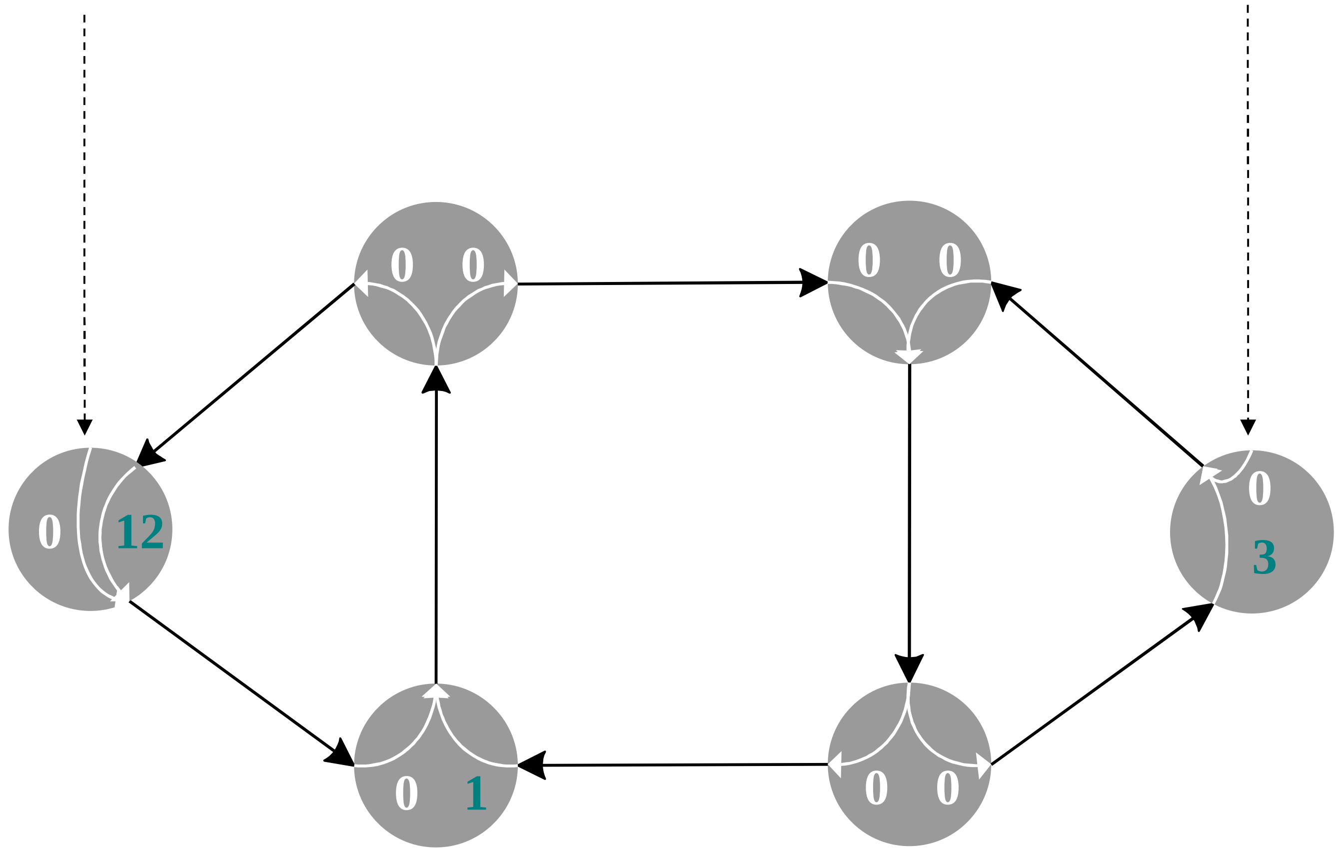
Proof. Skipped.

Example of a causal $\mathbb{F}[(D)]$-linear network code



Delay function on a network with cycles

Definitions. A delay function t maps adjacent pairs to integer ≥ 0 such that
• along every cycle, $t(d, e) > 0$ for at least one adjacent pair (d, e).



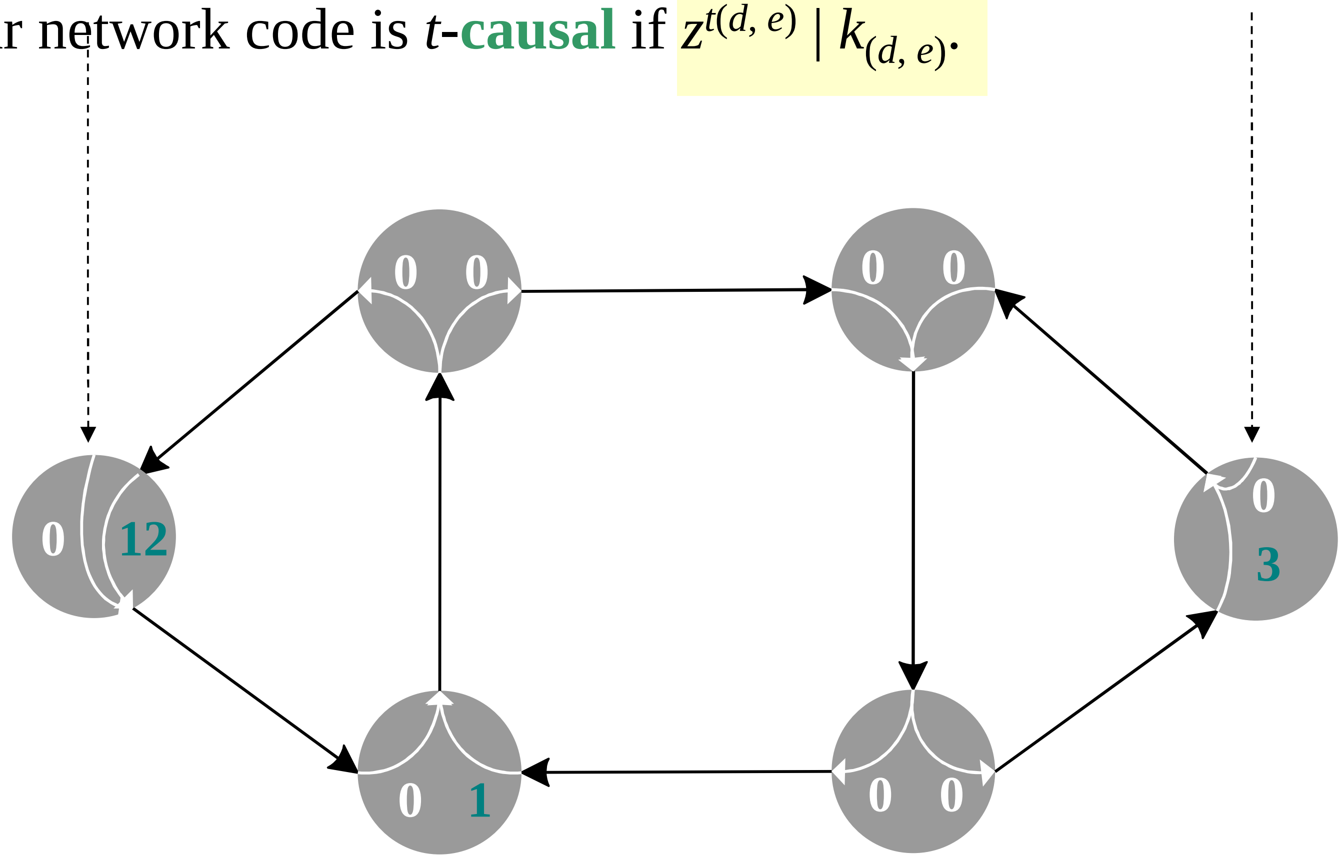
A delay function t.

Causal Data Propagation by DVR-based NC

Definitions. A delay function t maps adjacent pairs to integer ≥ 0 such that

- along every cycle, $t(d, e) > 0$ for at least one adjacent pair (d, e).

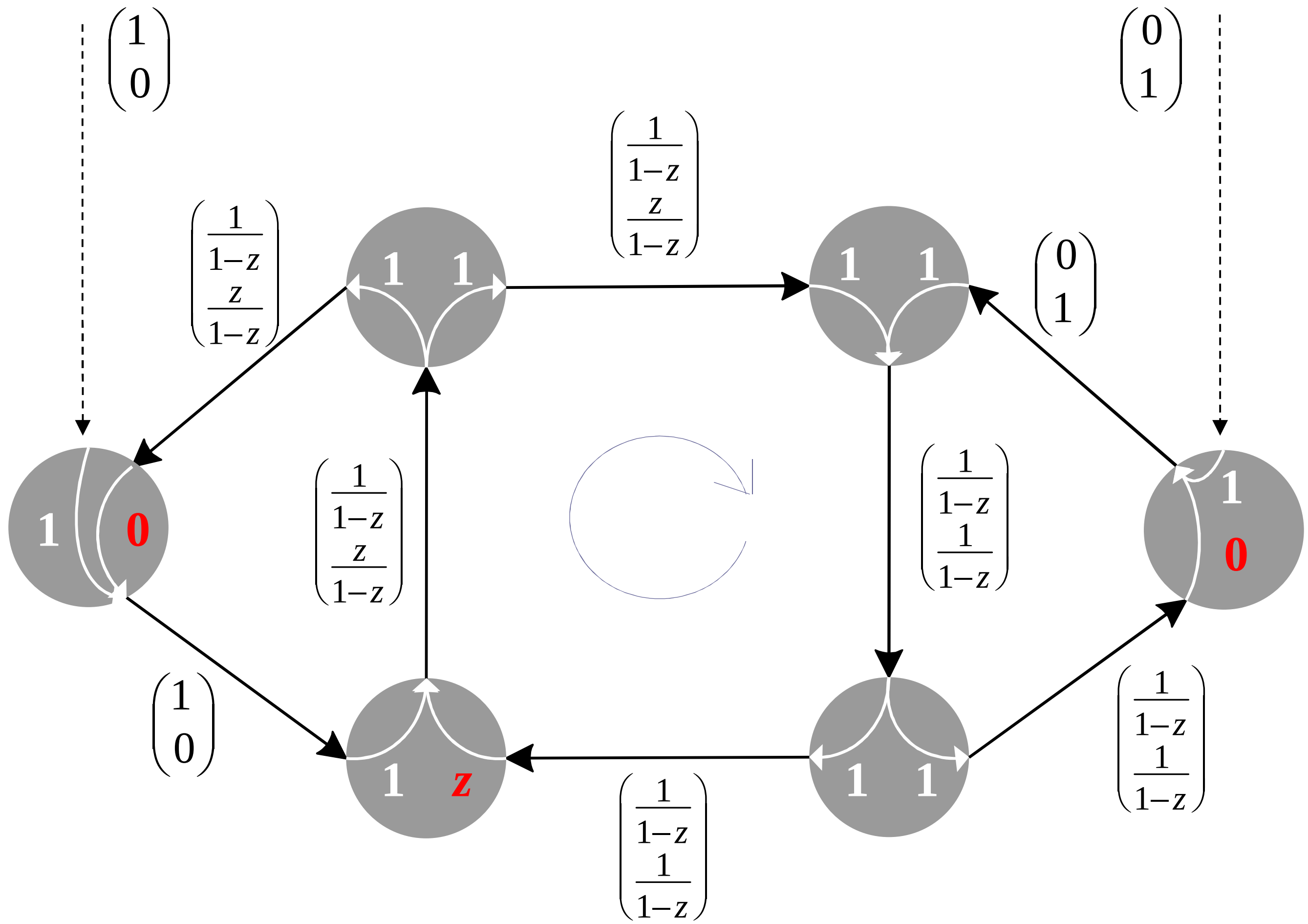
A $\mathbb{D}$-linear network code is t-**causal** if $z^{t(d, e)} \mid k_{(d, e)}$.



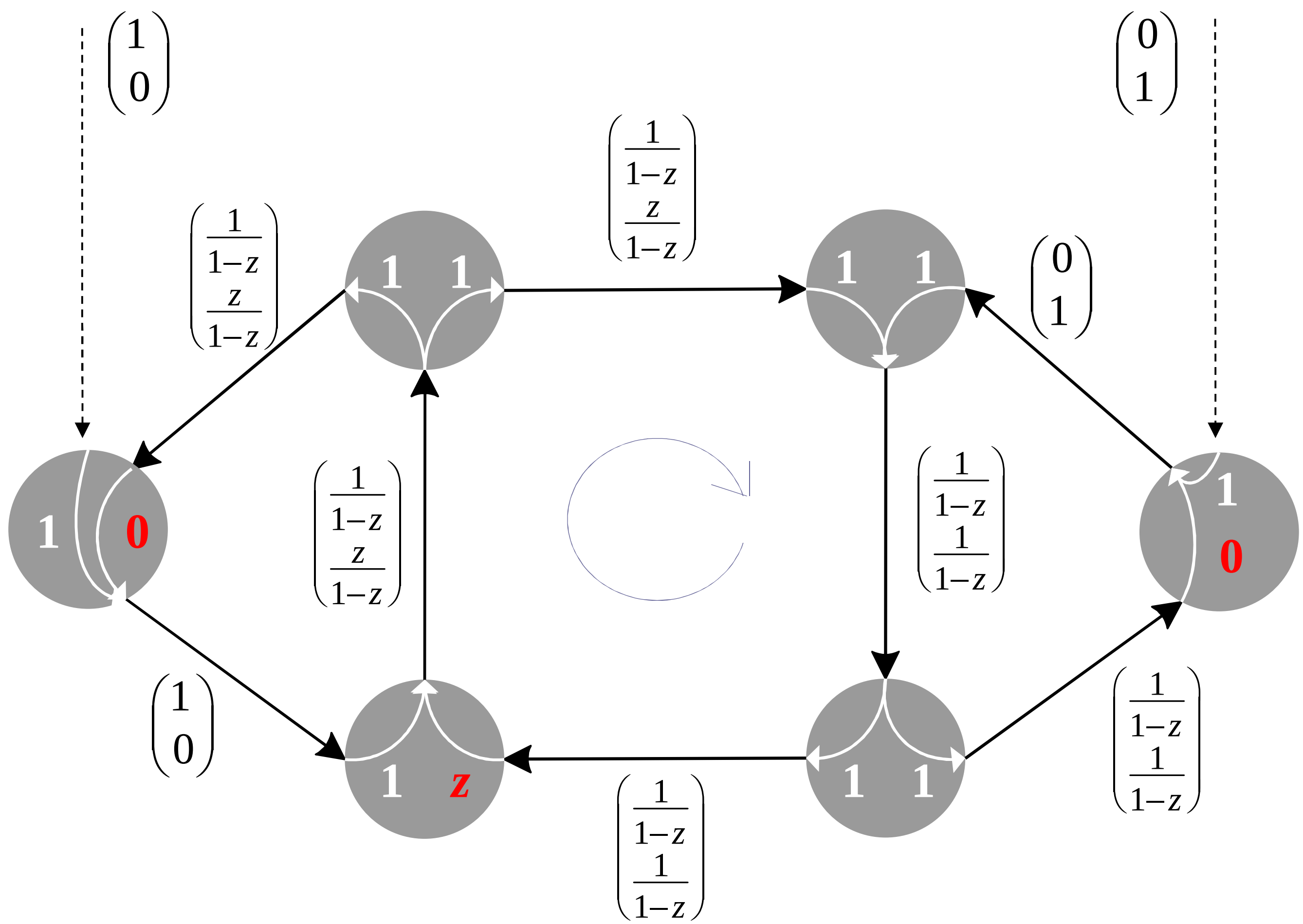
A delay function t.

A t-causal $\mathbb{D}$-linear network code

$z^{12} \mid 0; \quad z^{1} \mid z; \quad z^{3} \mid 0$



Example of a *t*-causal $\mathbb{F}[(D)]$-linear network code



Optimal DVR-based Network Codes

Theorem 3. Let $\mathbb{D}$ be a DVR. Given a delay function t, there exists an optimal t-causal $\mathbb{D}$-linear NC.

Proof. Let $\mathbb{Q}$ be the quotient field of $\mathbb{D}$, and m the largest $t(d, e)$ among all adjacent pairs (d, e).

The ideal $z^m \cdot \mathbb{D}$ shares the same cardinality with $\mathbb{D}$, which is infinite.

From the **Lemma 1**, there exists

- an optimal $\mathbb{Q}$-linear NC C with coding coefficients $k_{d,e} \in z^m \cdot \mathbb{D}$.

$\Rightarrow$ a t-causal $\mathbb{D}$-linear network code

$\Rightarrow$ a t-causal normal $\mathbb{D}$-linear network code

$\Rightarrow$ An optimal t-causal $\mathbb{D}$-linear NC as well

Optimal DVR-based Network Codes

Theorem 3. There exists an optimal t-causal $\mathbb{D}$-linear NC.

Proof. Skipped.

Optimal DVR-based Network Codes

Theorem 3. There exists an optimal causal $\mathbb{D}$-linear NC.

Proof. Skipped.

Contents

- PID-based network coding
  - Non-singular and normal network codes
  - Existence of optimal code
- **DVR-based causal network coding**
  - Existence of optimal code
  - **Decoding**

Inv. Factor Thm. of Free Submodule over a PID

Assume that v is eligible for receiving the message.

// maxflow from s to v is at least ω

By the Invariant Factor Theorem of Free Submodule over a PID :

1) The received submodule $\langle \boldsymbol{f}_e : e \in \mathrm{In}(v) \rangle$ of the source module $\mathbb{D}^\omega$ is also a free $\mathbb{D}$-module at the rank ω.
2) There is a basis $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\omega\}$ of the source module and a basis $\{d_1\boldsymbol{u}_1, \ldots, d_\omega\boldsymbol{u}_\omega\}$ of the received submodule, where $d_1, \ldots, d_\omega \in \mathbb{D}$.
3) The elements $d_1, \ldots, d_\omega$ can be so chosen that $d_1 \mid d_2 \mid \ldots \mid d_\omega$. Moreover, such a choice is unique up to unit factors. The unique d_1, $d_2, \ldots, d_\omega$ are called the invariant factors of the received submodule in the source module.

Inv. Factor Thm. of Free Submodule over a DVR

Assume that maxflow from s to v is at least ω.

// so that v is eligible for receiving the message

By the Invariant Factor Theorem of Free Submodule over a PID :

1) The received submodule $\langle \boldsymbol{f}_e : e \in \mathrm{In}(v) \rangle$ of the source module $\mathbb{D}^\omega$ is also a free $\mathbb{D}$-module at the rank ω.
2) There is a basis $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\omega\}$ of the source module and a basis $\{d_1\boldsymbol{u}_1, \ldots, d_\omega\boldsymbol{u}_\omega\}$ of the received submodule, where $d_1, \ldots, d_\omega \in \mathbb{D}$.

Since $\mathbb{D}$ is a DVR, we may write

- $d_1 = z^{i_1}, \ldots, d_\omega = z^{i_\omega}$ up to multiplication by units // $i_j \geq 0$

Then, reorder $d_1, \ldots, d_\omega$ so that $i_1 \leq \ldots \leq i_\omega$.

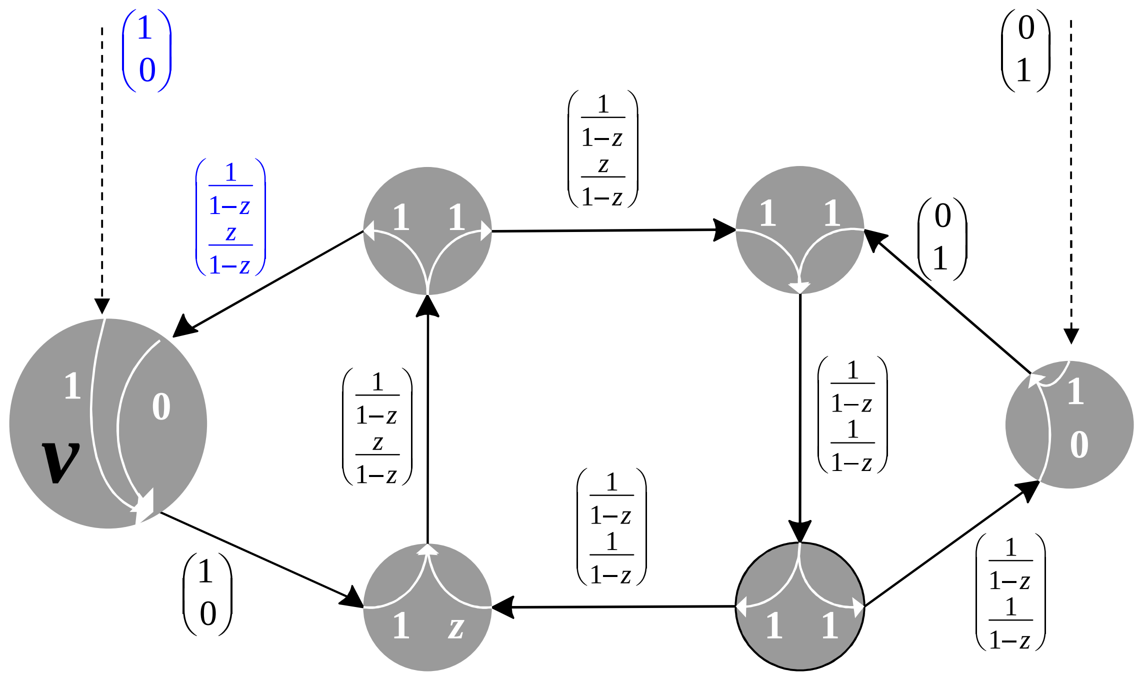
The sequence $(i_1, \ldots, i_\omega)$ is unique.

Example of decoding a $\mathbb{D}$-linear NC

Node $\boldsymbol{v}$ receives data units

$$(a \quad b)\cdot\begin{bmatrix}1 & \frac{1}{1-z}\\ 0 & \frac{z}{1-z}\end{bmatrix} = \left(a \quad \frac{a+bz}{1-z}\right)$$

Message = $(a \quad b) \in \mathbb{D}^2$



An optimal causal $\mathbb{D}$-linear NC on the *Shuttle Network*

Example of decoding a $\mathbb{D}$-linear NC

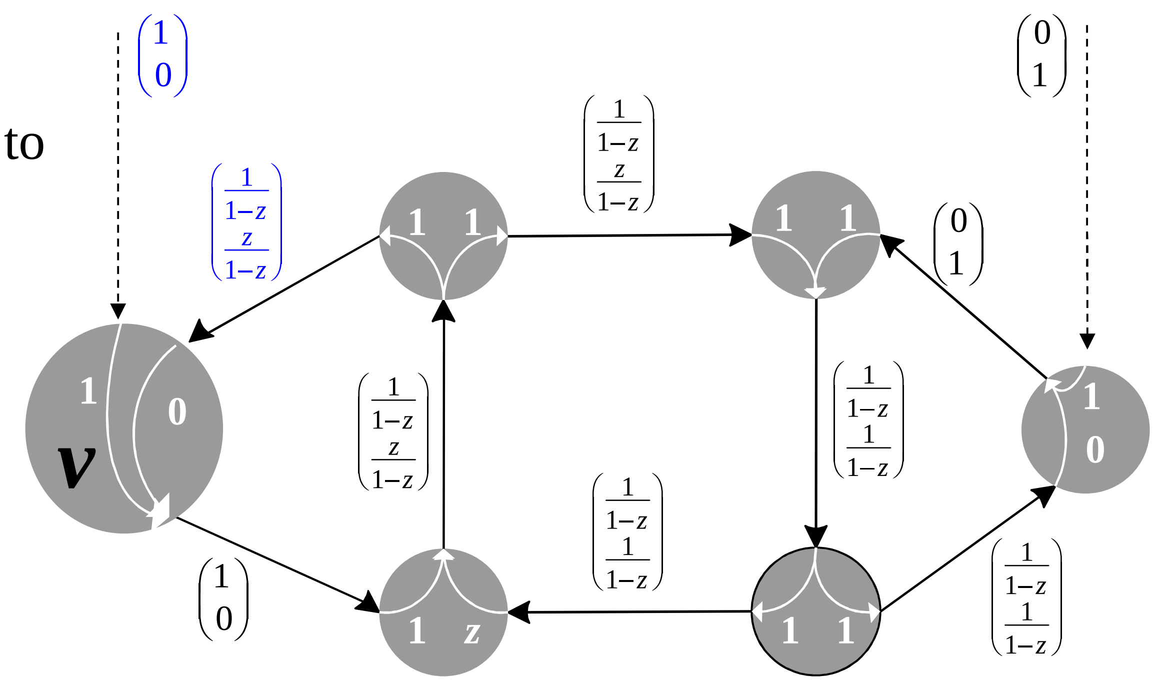
Node $\boldsymbol{v}$ receives data units

$$(a \quad b)\cdot\begin{bmatrix} 1 & \frac{1}{1-z} \\ 0 & \frac{z}{1-z} \end{bmatrix} = \begin{pmatrix} a & \frac{a+bz}{1-z} \end{pmatrix}$$

Apply Invariant Factor Theorem to $\langle \boldsymbol{f}_e : e \in \mathrm{In}(v) \rangle$. We find

$$i_1 = 0 \text{ and } i_2 = 1.$$

Message = $(a \quad b) \in \mathbb{D}^2$



An optimal causal $\mathbb{D}$-linear NC on the *Shuttle Network*

Decoding of an optimal causal $\mathbb{D}$-linear NC

v = an eligible receiver of the message. By the Invariant Factor Theorem of Free Submodule over a PID, the received submodule $\langle \boldsymbol{f}_e : e \in \mathrm{In}(v) \rangle$ of $\mathbb{D}^\omega$ is also a free $\mathbb{D}$-module of rank ω and there is a basis $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\omega\}$ of $\mathbb{D}^\omega$ so that $\{z^{i_1}\boldsymbol{u}_1, \ldots, z^{i_\omega}\boldsymbol{u}_\omega\}$ is a basis of $\langle \boldsymbol{f}_e : e \in \mathrm{In}(v) \rangle$, where $0 \le i_1 \le \ldots \le i_\omega = i$.

The goal is to establish:

$$[\boldsymbol{f}_e]_{e \in \mathrm{In}(v)} \cdot \text{[Some matrix]} = z^i I_\omega$$

Why? Let the message be the row vector $(a_1\ a_2 \ldots a_\omega)$. Then,

$$(a_1\ a_2 \ldots a_\omega) \cdot [\boldsymbol{f}_e]_{e \in \mathrm{In}(v)} \cdot \text{[Some matrix]} = z^i (a_1\ a_2 \ldots a_\omega)$$

Received data by the node v

A decoding matrix at the node v with the "decoding delay" z^i

$i = i_\omega$ is the highest valuation among invariant factors of the received submodule.

Example of decoding a $\mathbb{D}$-linear NC

Node $\boldsymbol{v}$ receives data units

$$\begin{pmatrix} a & b \end{pmatrix} \cdot \begin{bmatrix} 1 & \frac{1}{1-z} \\ 0 & \frac{z}{1-z} \end{bmatrix} = \begin{pmatrix} a & \frac{a+bz}{1-z} \end{pmatrix}$$

Apply Invariant Factor Theorem to $\langle f_e : e \in \mathrm{In}(v) \rangle$. We find

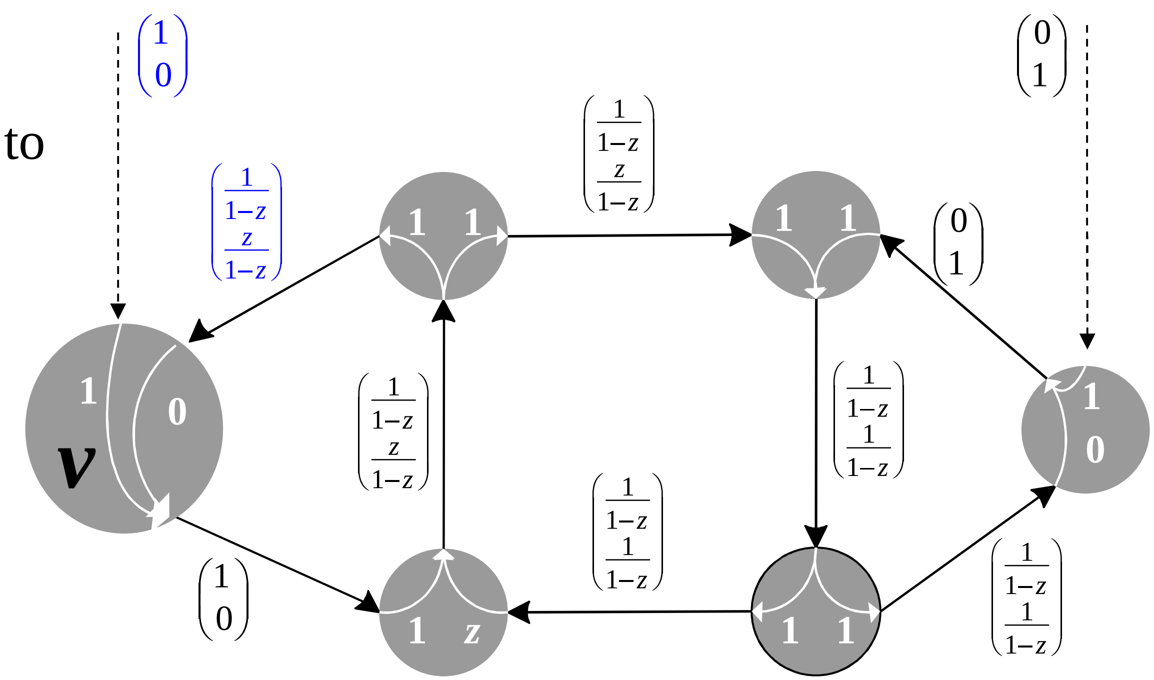
$$i_1 = 0 \text{ and } i_2 = 1$$

Decode the message (a b) with delay z^1 via

$$\begin{pmatrix} a & \frac{a+bz}{1-z} \end{pmatrix} \cdot \begin{bmatrix} z & -1 \\ 0 & 1-z \end{bmatrix} = z^1 \begin{pmatrix} a & b \end{pmatrix}$$

Decoding matrix

Message = $\begin{pmatrix} a & b \end{pmatrix} \in \mathbb{D}^2$



An optimal causal $\mathbb{D}$-linear NC on the *Shuttle Network*

Decoding of an optimal causal $\mathbb{D}$-linear NC

v = an eligible receiver of the message. By the Invariant Factor Theorem of Free Submodule over a PID, the received submodule $\langle \boldsymbol{f}_e : e \in \mathrm{In}(v) \rangle$ of $\mathbb{D}^\omega$ is also a free $\mathbb{D}$-module of rank ω and there is a basis $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\omega\}$ of $\mathbb{D}^\omega$ so that $\{z^{i_1}\boldsymbol{u}_1, \ldots, z^{i_\omega}\boldsymbol{u}_\omega\}$ is a basis of $\langle \boldsymbol{f}_e : e \in \mathrm{In}(v) \rangle$, where $0 \le i_1 \le \ldots \le i_\omega = i$.

Thus, there exists an $|\mathrm{In}(v)| \times \omega$ matrix $\boldsymbol{M}$ over $\mathbb{D}$ such that

$$[\boldsymbol{f}_e]_{e \in \mathrm{In}(v)} \cdot \boldsymbol{M} = [z^{i_j} \boldsymbol{u}_j]_{1 \le j \le \omega}$$

Decoding of an optimal causal $\mathbb{D}$-linear NC

v = an eligible receiver of the message. By the Invariant Factor Theorem of Free Submodule over a PID, the received submodule $\langle \boldsymbol{f}_e : e \in \mathrm{In}(v) \rangle$ of $\mathbb{D}^\omega$ is also a free $\mathbb{D}$-module of rank ω and there is a basis $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\omega\}$ of $\mathbb{D}^\omega$ so that $\{z^{i_1}\boldsymbol{u}_1, \ldots, z^{i_\omega}\boldsymbol{u}_\omega\}$ is a basis of $\langle \boldsymbol{f}_e : e \in \mathrm{In}(v) \rangle$, where $0 \le i_1 \le \ldots \le i_\omega = i$.

Thus, there exists an $|\mathrm{In}(v)| \times \omega$ matrix $\boldsymbol{M}$ over $\mathbb{D}$ such that

$$[\boldsymbol{f}_e]_{e \in \mathrm{In}(v)} \cdot \boldsymbol{M} = [z^{i_j}\boldsymbol{u}_j]_{1 \le j \le \omega}$$

Write $[z^{i_j}\boldsymbol{u}_j]_{1 \le j \le \omega} \cdot \boldsymbol{D} = [z^{i}\boldsymbol{u}_j]_{1 \le j \le \omega} = z^{i}[\boldsymbol{u}_j]_{1 \le j \le \omega}$, where $\boldsymbol{D}$ is the diagonal matrix with diagonal entries z^{i-i_j}.

Decoding of an optimal causal $\mathbb{D}$-linear NC

v = an eligible receiver of the message. By the Invariant Factor Theorem of Free Submodule over a PID, the received submodule $\langle \boldsymbol{f}_e : e \in \mathrm{In}(v) \rangle$ of $\mathbb{D}^\omega$ is also a free $\mathbb{D}$-module of rank ω and there is a basis $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\omega\}$ of $\mathbb{D}^\omega$ so that $\{z^{i_1}\boldsymbol{u}_1, \ldots, z^{i_\omega}\boldsymbol{u}_\omega\}$ is a basis of $\langle \boldsymbol{f}_e : e \in \mathrm{In}(v) \rangle$, where $0 \le i_1 \le \ldots \le i_\omega = i$.

Thus, there exists an $|\mathrm{In}(v)| \times \omega$ matrix $\boldsymbol{M}$ over $\mathbb{D}$ such that

$$[\boldsymbol{f}_e]_{e\in \mathrm{In}(v)} \cdot \boldsymbol{M} = [z^{i_j}\, \boldsymbol{u}_j]_{1\le j\le \omega}$$

Write $[z^{i_j}\, \boldsymbol{u}_j]_{1\le j\le \omega} \cdot \boldsymbol{D} = [z^{i}\, \boldsymbol{u}_j]_{1\le j\le \omega} = z^{i}\, [\boldsymbol{u}_j]_{1\le j\le \omega}$, where $\boldsymbol{D}$ is the diagonal matrix with diagonal entries z^{i-i_j}. Combining these two equalities,

$$[\boldsymbol{f}_e]_{e\in \mathrm{In}(v)} \cdot \boldsymbol{M} \cdot \boldsymbol{D} = z^{i}\, [\boldsymbol{u}_j]_{1\le j\le \omega}$$

Decoding of an optimal causal $\mathbb{D}$-linear NC

v = an eligible receiver of the message. By the Invariant Factor Theorem of Free Submodule over a PID, the received submodule $\langle \boldsymbol{f}_e : e \in \mathrm{In}(v) \rangle$ of $\mathbb{D}^\omega$ is also a free $\mathbb{D}$-module of rank ω and there is a basis $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\omega\}$ of $\mathbb{D}^\omega$ so that $\{z^{i_1}\boldsymbol{u}_1, \ldots, z^{i_\omega}\boldsymbol{u}_\omega\}$ is a basis of $\langle \boldsymbol{f}_e : e \in \mathrm{In}(v) \rangle$, where $0 \le i_1 \le \ldots \le i_\omega = i$.

Thus, there exists an $|\mathrm{In}(v)| \times \omega$ matrix $\boldsymbol{M}$ over $\mathbb{D}$ such that

$$[\boldsymbol{f}_e]_{e \in \mathrm{In}(v)} \cdot \boldsymbol{M} = [z^{i_j} \boldsymbol{u}_j]_{1 \le j \le \omega}$$

Write $[z^{i_j} \boldsymbol{u}_j]_{1 \le j \le \omega} \cdot \boldsymbol{D} = [z^i \boldsymbol{u}_j]_{1 \le j \le \omega} = z^i [\boldsymbol{u}_j]_{1 \le j \le \omega}$, where $\boldsymbol{D}$ is the diagonal matrix with z^{i-i_j} on the diagonal. Combining these two equalities,

$$[\boldsymbol{f}_e]_{e \in \mathrm{In}(v)} \cdot \boldsymbol{M} \cdot \boldsymbol{D} = z^i [\boldsymbol{u}_j]_{1 \le j \le \omega}$$

$$[\boldsymbol{f}_e]_{e \in \mathrm{In}(v)} \cdot \boldsymbol{M} \cdot \boldsymbol{D} \cdot ([\boldsymbol{u}_j]_{1 \le j \le \omega})^{-1} = z^i \boldsymbol{I}_\omega$$

Decoding of an optimal causal $\mathbb{D}$-linear NC

v = an eligible receiver of the message. By the Invariant Factor Theorem of Free Submodule over a PID, the received submodule $\langle \boldsymbol{f}_e : e \in \mathrm{In}(v) \rangle$ of $\mathbb{D}^{\omega}$ is also a free $\mathbb{D}$-module of rank ω and there is a basis $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\omega\}$ of $\mathbb{D}^{\omega}$ so that $\{z^{i_1}\boldsymbol{u}_1, \ldots, z^{i_\omega}\boldsymbol{u}_\omega\}$ is a basis of $\langle \boldsymbol{f}_e : e \in \mathrm{In}(v) \rangle$, where $0 \le i_1 \le \ldots \le i_\omega = i$.

$$[\boldsymbol{f}_e]_{e \in \mathrm{In}(v)} \cdot \boldsymbol{M} \cdot \boldsymbol{D} \cdot ([\boldsymbol{u}_j]_{1 \le j \le \omega})^{-1} = z^i \boldsymbol{I}_\omega$$

= [Some matrix]

for decoding

z^i = optimal decoding "delay"

v = an eligible receiver of the message. By the Invariant Factor Theorem of Free Submodule over a PID, the received submodule $\langle \boldsymbol{f}_e : e \in \mathrm{In}(v) \rangle$ of $\mathbb{D}^\omega$ is also a free $\mathbb{D}$-module of rank ω and there is a basis $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\omega\}$ of $\mathbb{D}^\omega$ so that $\{z^{i_1}\boldsymbol{u}_1, \ldots, z^{i_\omega}\boldsymbol{u}_\omega\}$ is a basis of $\langle \boldsymbol{f}_e : e \in \mathrm{In}(v) \rangle$, where $0 \le i_1 \le \ldots \le i_\omega = i$.

Task. Assuming the existence of a decoding matrix $\boldsymbol{A}$ at the "delay" z^k, we are to show that $k \ge i$.

z^i = optimal decoding "delay"

v = an eligible receiver of the message. By the Invariant Factor Theorem of Free Submodule over a PID, the received submodule $\langle \boldsymbol{f}_e : e \in \mathrm{In}(v) \rangle$ of $\mathbb{D}^\omega$ is also a free $\mathbb{D}$-module of rank ω and there is a basis $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\omega\}$ of $\mathbb{D}^\omega$ so that $\{z^{i_1}\boldsymbol{u}_1, \ldots, z^{i_\omega}\boldsymbol{u}_\omega\}$ is a basis of $\langle \boldsymbol{f}_e : e \in \mathrm{In}(v) \rangle$, where $0 \le i_1 \le \ldots \le i_\omega = i$.

Thus, there exists an $\omega \times |\mathrm{In}(v)|$ matrix $\boldsymbol{M'}$ over $\mathbb{D}$ such that

$[z^{i_j}\boldsymbol{u}_j]_{1\le j\le\omega} \cdot \boldsymbol{M'} = [\boldsymbol{f}_e]_{e\in \mathrm{In}(v)}$ // Symmetric to previous argument

Or equivalently,

$[\boldsymbol{u}_j]_{1\le j\le\omega} \cdot \boldsymbol{D'} \cdot \boldsymbol{M'} = [\boldsymbol{f}_e]_{e\in \mathrm{In}(v)}$, where $\boldsymbol{D'}$ is the diagonal matrix with diagonal entries z^{i_j}

z^i = optimal decoding "delay"

v = an eligible receiver of the message. By the Invariant Factor Theorem of Free Submodule over a PID, the received submodule $\langle \boldsymbol{f}_e: e \in \mathrm{In}(v) \rangle$ of $\mathbb{D}^\omega$ is also a free $\mathbb{D}$-module of rank ω and there is a basis $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\omega\}$ of $\mathbb{D}^\omega$ so that $\{z^{i_1}\boldsymbol{u}_1, \ldots, z^{i_\omega}\boldsymbol{u}_\omega\}$ is a basis of $\langle \boldsymbol{f}_e: e \in \mathrm{In}(v) \rangle$, where $0 \le i_1 \le \ldots \le i_\omega = i$.

Thus, there exists an $\omega \times |\mathrm{In}(v)|$ matrix $\boldsymbol{M'}$ over $\mathbb{D}$ such that

$$[\boldsymbol{u}_j]_{1 \le j \le \omega} \cdot \boldsymbol{D'} \cdot \boldsymbol{M'} = [\boldsymbol{f}_e]_{e \in \mathrm{In}(v)}$$

z^i = optimal decoding "delay"

v = an eligible receiver of the message. By the Invariant Factor Theorem of Free Submodule over a PID, the received submodule $\langle \boldsymbol{f}_e: e\in \mathrm{In}(v)\rangle$ of $\mathbb{D}^\omega$ is also a free $\mathbb{D}$-module of rank ω and there is a basis $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\omega\}$ of $\mathbb{D}^\omega$ so that $\{z^{i_1}\boldsymbol{u}_1, \ldots, z^{i_\omega}\boldsymbol{u}_\omega\}$ is a basis of $\langle \boldsymbol{f}_e: e\in \mathrm{In}(v)\rangle$, where $0 \le i_1 \le \ldots \le i_\omega = i$.

Thus, there exists an $\omega\times|\mathrm{In}(v)|$ matrix $\boldsymbol{M'}$ over $\mathbb{D}$ such that

$$[\boldsymbol{u}_j]_{1\le j\le\omega} \cdot \boldsymbol{D'} \cdot \boldsymbol{M'} = [\boldsymbol{f}_e]_{e\in \mathrm{In}(v)}$$

Task. Assuming $[\boldsymbol{f}_e]_{e\in \mathrm{In}(v)} \cdot \boldsymbol{A} = z^k\boldsymbol{I}_\omega$, we are to show that $k \ge i$.

$$[\boldsymbol{u}_j]_{1\le j\le\omega} \cdot \boldsymbol{D'} \cdot \boldsymbol{M'} \cdot \boldsymbol{A} = [\boldsymbol{f}_e]_{e\in \mathrm{In}(v)} \cdot \boldsymbol{A} = z^k\boldsymbol{I}_\omega$$

z^i = optimal decoding "delay"

v = an eligible receiver of the message. By the Invariant Factor Theorem of Free Submodule over a PID, the received submodule $\langle \boldsymbol{f}_e : e \in \mathrm{In}(v) \rangle$ of $\mathbb{D}^\omega$ is also a free $\mathbb{D}$-module of rank ω and there is a basis $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\omega\}$ of $\mathbb{D}^\omega$ so that $\{z^{i_1}\boldsymbol{u}_1, \ldots, z^{i_\omega}\boldsymbol{u}_\omega\}$ is a basis of $\langle \boldsymbol{f}_e : e \in \mathrm{In}(v) \rangle$, where $0 \le i_1 \le \ldots \le i_\omega = i$.

$$[\boldsymbol{u}_j]_{1 \le j \le \omega} \cdot \boldsymbol{D'} \cdot \boldsymbol{M'} \cdot \boldsymbol{A} = z^k \boldsymbol{I}_\omega$$

where $\boldsymbol{D'}$ is the diagonal matrix with diagonal entries z^{i_j}. Thus

$$\boldsymbol{D'} \cdot \boldsymbol{M'} \cdot \boldsymbol{A} \cdot [\boldsymbol{u}_j]_{1 \le j \le \omega} = z^k \boldsymbol{I}_\omega$$

Presence of z^i on the bottom row of the diagonal matrix $\boldsymbol{D'}$ $\Rightarrow$ $z^i \mid z^k$

Convolutional decoding with delay *i*

Abbreviate the matrix $[\boldsymbol{f}_e]_{e \in \mathrm{In}(v)}$ as $\boldsymbol{F}$.

Thus, there exists an $|\mathrm{In}(v)| \times \omega$ matrix $\boldsymbol{A}$ over $\mathbb{F}[(D)]$ such that

$$\boldsymbol{F} \cdot \boldsymbol{A} = D^i \boldsymbol{I}_\omega$$

Write $\boldsymbol{F} = \sum_{n=0}^{\infty} D^n \boldsymbol{F}_n$, where $\boldsymbol{F}_n$ is a matrix over $\mathbb{F}$,

$$\boldsymbol{A} = \sum_{n=0}^{\infty} D^n \boldsymbol{A}_n,$$ where $\boldsymbol{A}_n$ is a matrix over $\mathbb{F}$

Thus, $$\left(\sum_{n=0}^{\infty} D^n \boldsymbol{F}_n\right)\left(\sum_{n=0}^{\infty} D^n \boldsymbol{A}_n\right) = D^i \boldsymbol{I}_\omega$$

Equate coefficients of D^n on both sides by convolution among matrices.

- The coefficient of D^i is equal to $\boldsymbol{I}_\omega$.
- The coefficient of D^j is equal to the zero matrix for all $j \neq i$.

Decoding delay *i* of convolutional NC

The first i+1 equations of matrix convolution can be summarized as:

$$\begin{pmatrix} F_0 & F_1 & F_2 & \ldots & F_i \\ \mathrm{O} & F_0 & F_1 & \ldots & F_{i-1} \\ \mathrm{O} & \mathrm{O} & F_0 & \ldots & F_{i-2} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \mathrm{O} & \mathrm{O} & \mathrm{O} & \ldots & F_0 \end{pmatrix} \begin{pmatrix} A_0 & A_1 & A_2 & \ldots & A_i \\ \mathrm{O} & A_0 & A_1 & \ldots & A_{i-1} \\ \mathrm{O} & \mathrm{O} & A_0 & \ldots & A_{i-2} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \mathrm{O} & \mathrm{O} & \mathrm{O} & \ldots & A_0 \end{pmatrix} = \begin{pmatrix} \mathrm{O} & \mathrm{O} & \mathrm{O} & \ldots & I_\omega \\ \mathrm{O} & \mathrm{O} & \mathrm{O} & \ldots & \mathrm{O} \\ \mathrm{O} & \mathrm{O} & \mathrm{O} & \ldots & \mathrm{O} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \mathrm{O} & \mathrm{O} & \mathrm{O} & \ldots & \mathrm{O} \end{pmatrix}$$

for "time-variant decoding." Meanwhile,

$$\begin{pmatrix} \mathrm{O} & \mathrm{O} & \mathrm{O} & \ldots & \mathrm{O} \\ \mathrm{O} & F_0 & F_1 & \ldots & F_{i-1} \\ \mathrm{O} & \mathrm{O} & F_0 & \ldots & F_{i-2} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \mathrm{O} & \mathrm{O} & \mathrm{O} & \mathrm{O} & F_0 \end{pmatrix} \begin{pmatrix} A_0 & A_1 & A_2 & \ldots & A_i \\ \mathrm{O} & A_0 & A_1 & \ldots & A_{i-1} \\ \mathrm{O} & \mathrm{O} & A_0 & \ldots & A_{i-2} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \mathrm{O} & \mathrm{O} & \mathrm{O} & \ldots & A_0 \end{pmatrix} = \begin{pmatrix} \mathrm{O} & \mathrm{O} & \mathrm{O} & \ldots & \mathrm{O} \\ \mathrm{O} & \mathrm{O} & \mathrm{O} & \ldots & \mathrm{O} \\ \mathrm{O} & \mathrm{O} & \mathrm{O} & \ldots & \mathrm{O} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \mathrm{O} & \mathrm{O} & \mathrm{O} & \ldots & \mathrm{O} \end{pmatrix}$$

One way to calculate the decoding delay *i*

Thus the rank of the matrix $\begin{pmatrix} F_0 & F_1 & F_2 & \dots & F_i \\ O & F_0 & F_1 & \dots & F_{i-1} \\ O & O & F_0 & \dots & F_{i-2} \\ \dots & \dots & \dots & \dots & \dots \\ O & O & O & \dots & F_0 \end{pmatrix}$

is ω higher than that of $\begin{pmatrix} O & O & O & \dots & O \\ O & F_0 & F_1 & \dots & F_{i-1} \\ O & O & F_0 & \dots & F_{i-2} \\ \dots & \dots & \dots & \dots & \dots \\ O & O & O & O & F_0 \end{pmatrix}$.

This necessary condition for convolutional decoding at the delay *i* is also sufficient for "time-variant decoding" according to [Cai-Wang 2009], which is motivated by a result of [Massey-Sain 1968] on linear sequential circuit.

Summary of theory of linear NC

Acyclic LNC:

When the DVR *degenerates* into a field

A field $\mathbb{F}$ is a PID, but the unique maximal ideal is $\{0\}$. No uniformizer! It is the acyclic topology that endows LNC with normality & causality.

Convolutional NC:

When the DVR = $\mathbb{F}[(D)]$

DVR-based linear NC

The descending chain of ideals endows normality & causality.

Summary of theory of linear NC

Acyclic LNC:

when DVR degenerates into a field

Convolutional NC:

when DVR = $\mathbb{F}[(D)]$

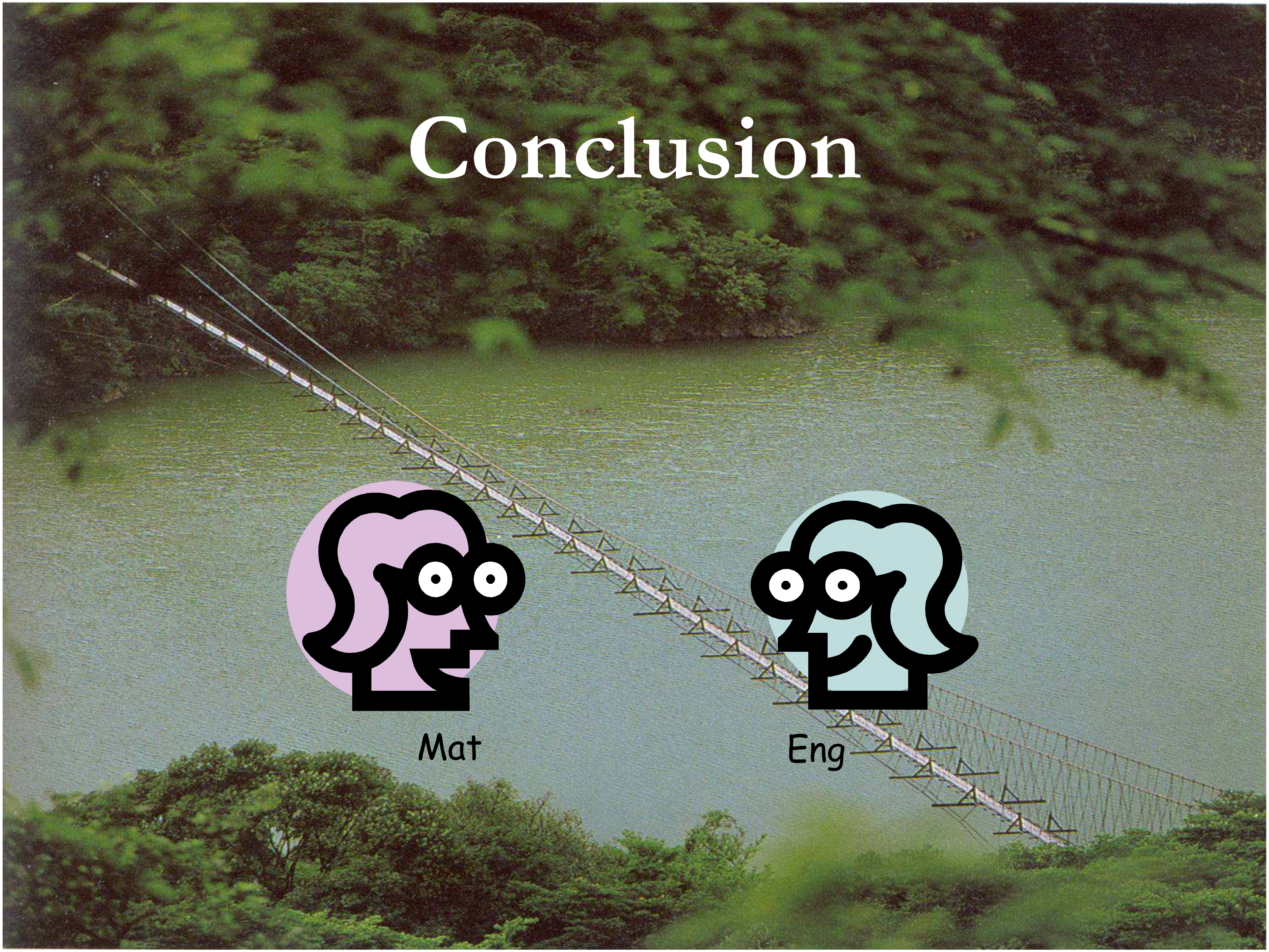
DVR-based linear NC

Ensure normality and causality.

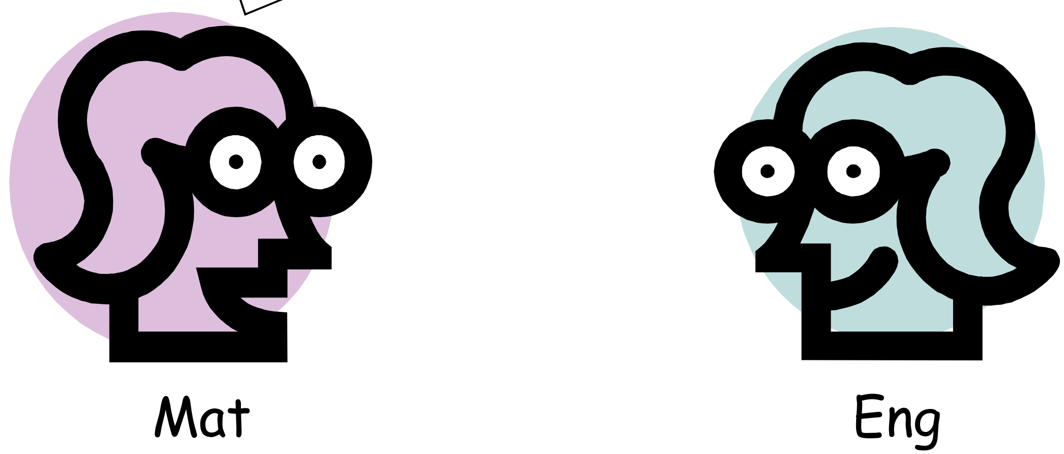
PID-based linear NC

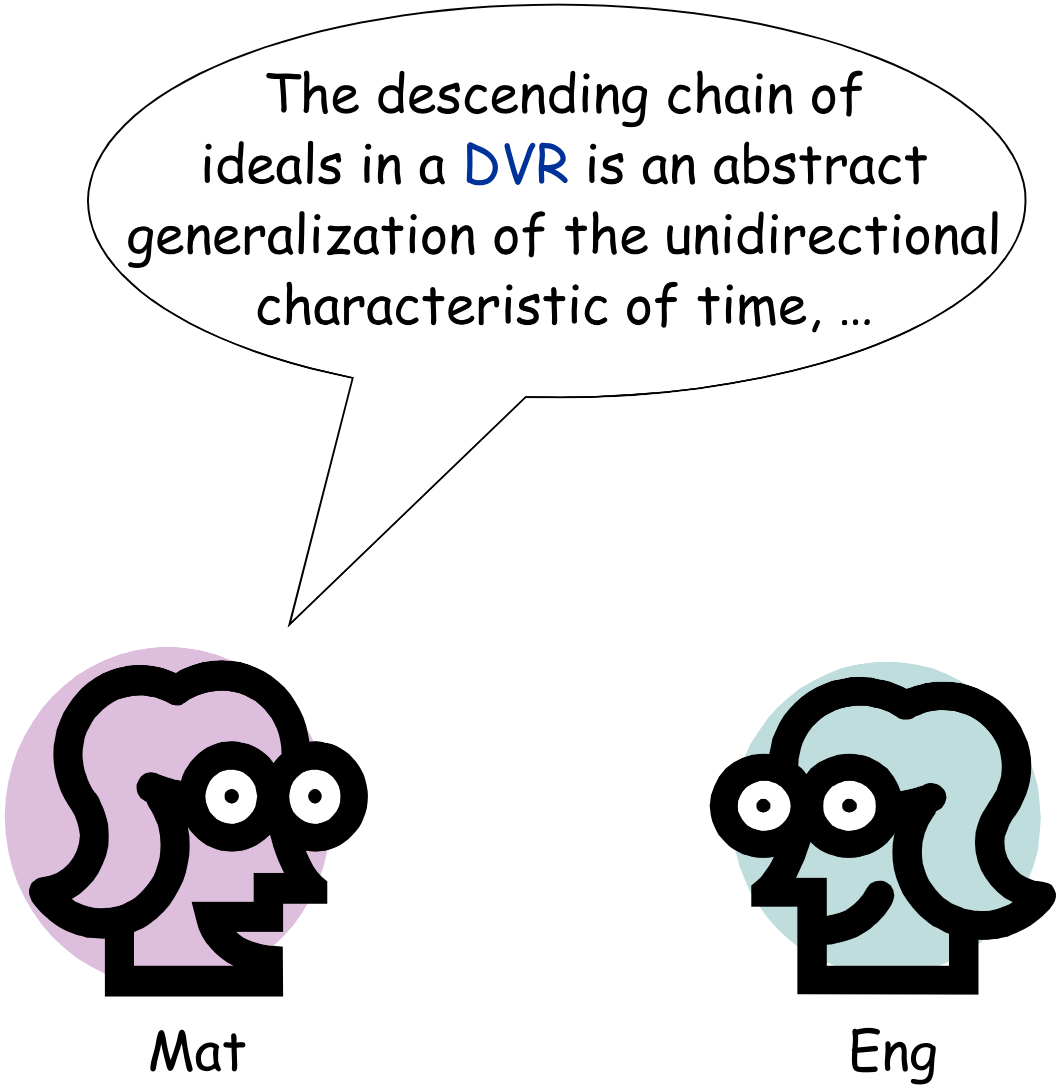
Formulate normality of a code.

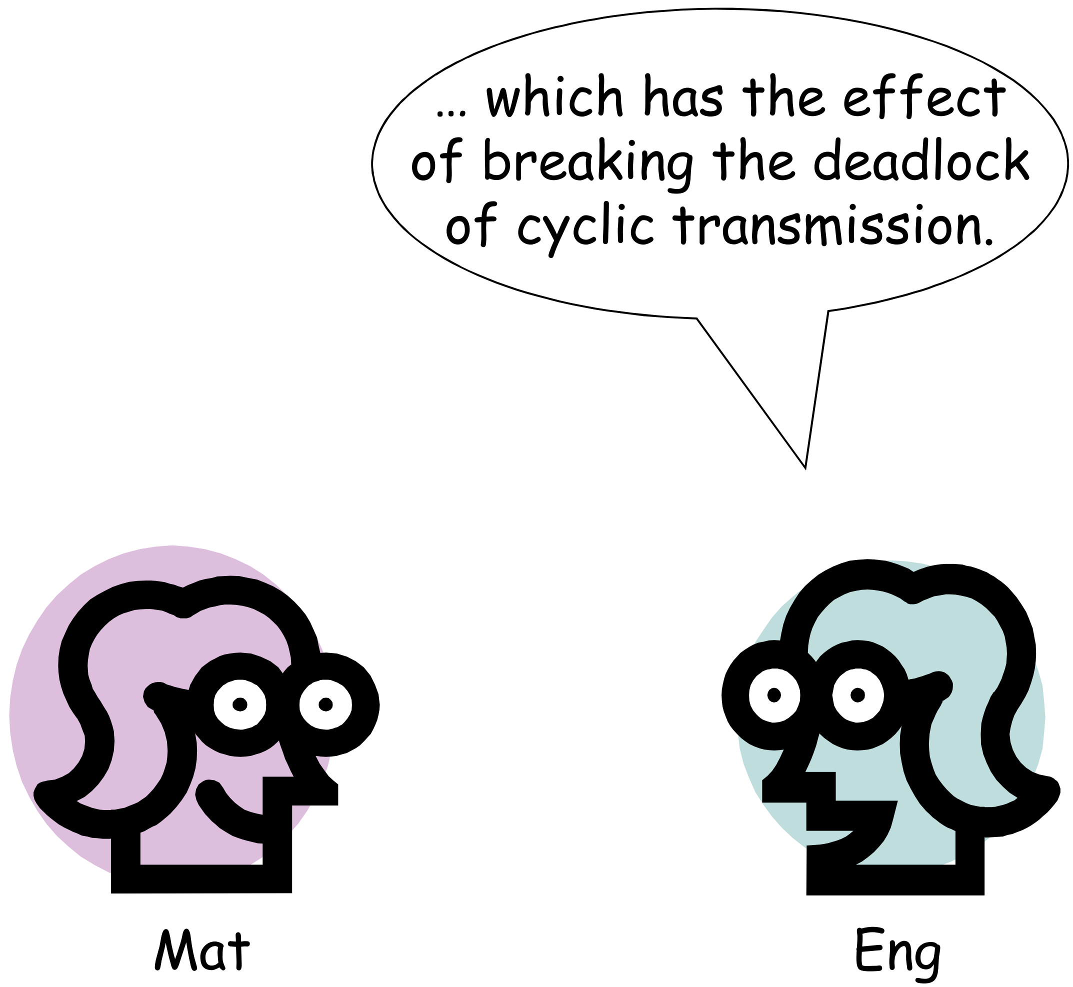
Conclusion

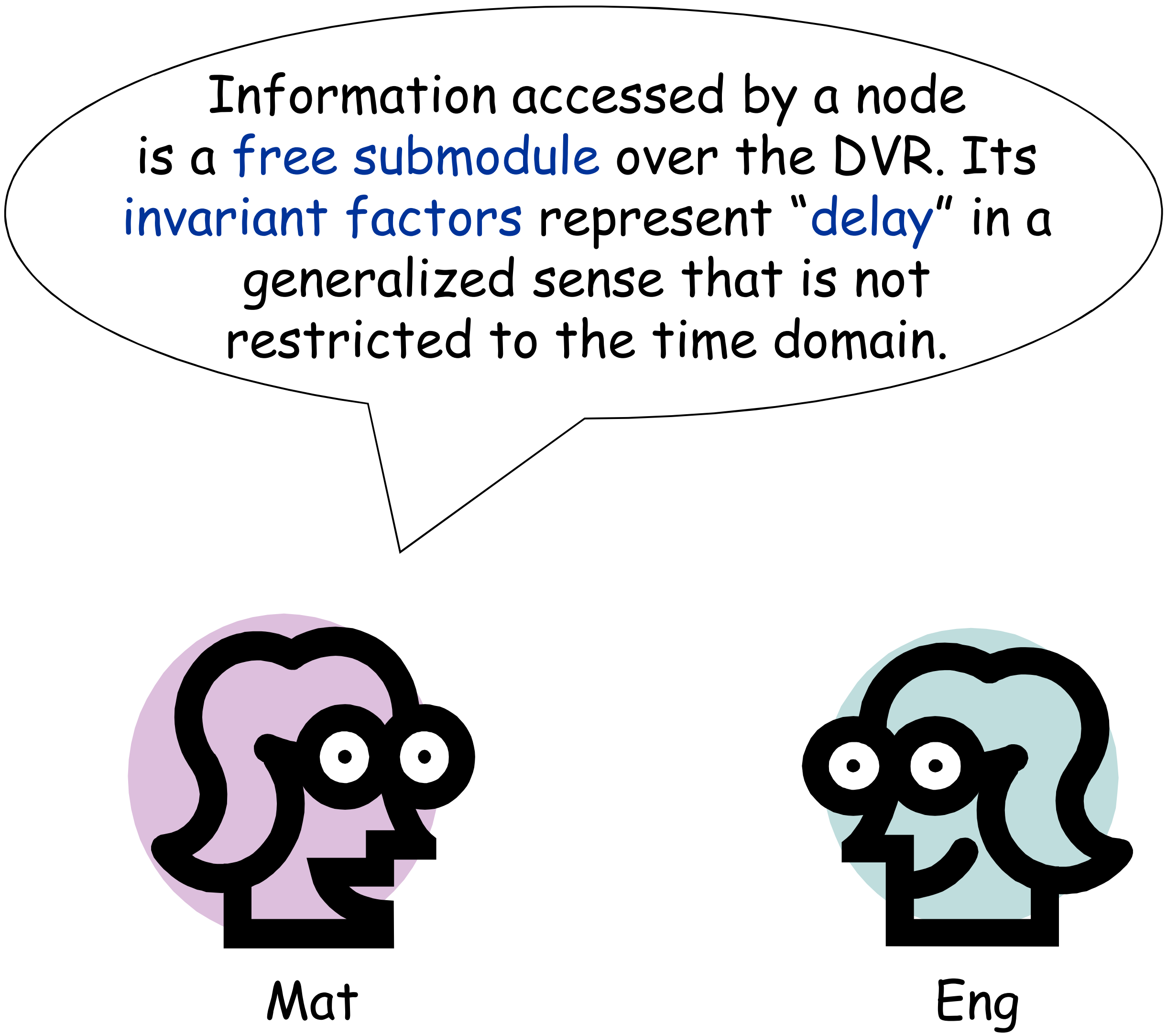


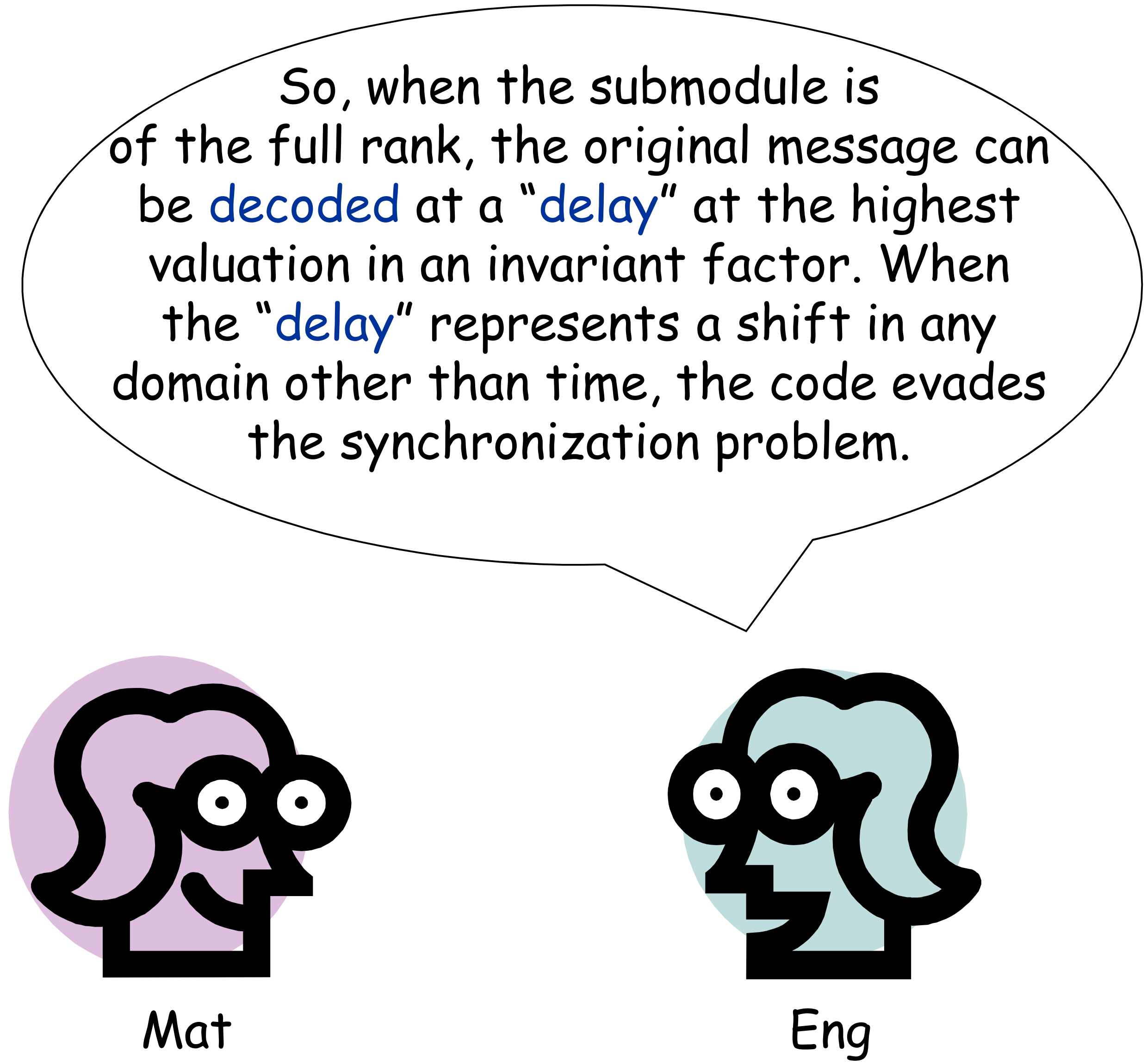
When the convolutional kernels belong to the polynomial ring $\mathbb{F}[D]$, there is no feedback, no loop and no inversion. Expansion of $\mathbb{F}[D]$ to $\mathbb{F}[(D)]$ enables the inversion of everything but time. This expansion means localization of $\mathbb{F}[D]$ at the prime ideal $\langle D \rangle$. The result $\mathbb{F}[(D)]$ is a local ring, in fact, a DVR.

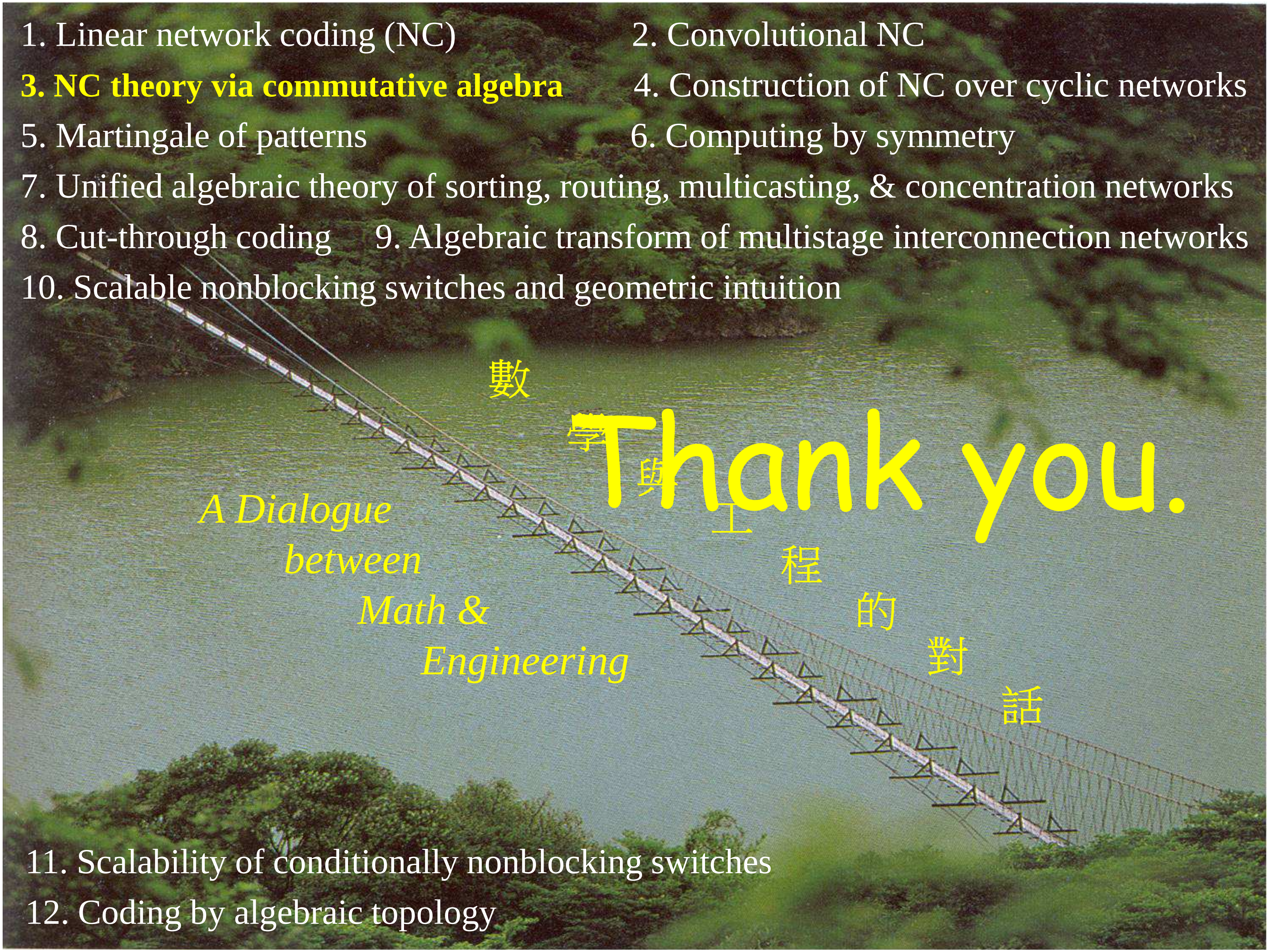



The descending chain of ideals in a DVR is an abstract generalization of the unidirectional characteristic of time, …
Mat
Eng


… which has the effect of breaking the deadlock of cyclic transmission.
Mat
Eng


Information accessed by a node is a free submodule over the DVR. Its invariant factors represent "delay" in a generalized sense that is not restricted to the time domain.
Mat
Eng


So, when the submodule is of the full rank, the original message can be decoded at a "delay" at the highest valuation in an invariant factor. When the "delay" represents a shift in any domain other than time, the code evades the synchronization problem.
Mat
Eng



1. Linear network coding (NC)
2. Convolutional NC
3. NC theory via commutative algebra
4. Construction of NC over cyclic networks
5. Martingale of patterns
6. Computing by symmetry
7. Unified algebraic theory of sorting, routing, multicasting, & concentration networks
8. Cut-through coding
9. Algebraic transform of multistage interconnection networks
10. Scalable nonblocking switches and geometric intuition

Thank you.

A Dialogue between Math & Engineering

數學與工程的對話

11. Scalability of conditionally nonblocking switches
12. Coding by algebraic topology

Some connections between Mathematics & Information Engineering