Universal Network Error Correction MDS Codes

Xuan Guang[1] Fang-Wei Fu[1] Zhen Zhang[2]

[1] Chern Institute of Mathematics
Nankai University

[2] Department of Electrical Engineering
University of Southern California

The 2011 International Symposium on Network Coding

Beijing, China

July 25-27, 2011

Outline

1. Background and Motivation
2. Linear Network Error Correction Codes (LNEC codes)
3. Universal Network MDS Codes

Part I:

Background and Motivation

Background

- Network coding has been extensively studied under the assumption that the channels of networks are error-free.
- Unfortunately, all kinds of errors may occur in practical network communications:
  1. random errors;
  2. erasure errors (packet losses);
  3. error in header;
  4. malicious attack;
  5. ......

  In order to deal with such problems efficiently, network error correction coding (NEC) was proposed by Cai and Yeung in 2002.

Motivation

Problem

In network communication, the source often transmits the messages at several different information rates within a session. For the purposes of both information transmission and network error correction, it is expected that different linear network error correction MDS codes are applied for these information rates.

Motivation

Based on the existing results, the most efficient solution is...

Solution

Design a linear network error correction MDS code for each information rate, and use them for information transmission and network error correction.

Motivation

However...

Side-effects

- Each node has to store all local encoding kernels for these different network MDS codes. It takes a large amount of storage space for each node. This also increases the complexity of the system considerably.
- In transmission, the source node must tell each non-source node which information rate is used to transmit the messages.
- Then after reading the rate, each non-source node searches and uses the corresponding local encoding kernel for coding. Searching and changing the local encoding kernels at each non-source node consume resources and time in the network.

Motivation

Goal

In order to avoid these side-effects, we propose the concept of universal network MDS codes. That is, for these different information rates, construct different network MDS codes which have the same local encoding kernel at each non-source node. This can avoid all shortcomings as above.

Part II:

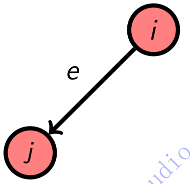
Linear Network Error Correction Codes

Basic Definitions and Notation

- Let $G = (V, E)$ be a single source multicast (one-to-many) network.
- A direct edge $e = (i, j) \in E$ represents a channel leading from node i to node j.
- Node i is called the tail of e and node j is called the head of e, respectively written as:

$$i = tail(e), \ j = head(e).$$

- Correspondingly, the channel e is called an outgoing channel of i and an incoming channel of j.



Basic Definitions and Notation

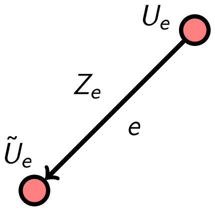
- For a node $i \in V$, define the following two sets:

$$Out(i) = \{e \in E : \ tail(e) = i\},$$
$$In(i) = \{e \in E : \ head(e) = i\}.$$

- The source node s has no incoming channels, each sink node has no outgoing channels. But we use the concept of imaginary incoming channels of the source node s and assume that these imaginary incoming channels provide the source messages to s.

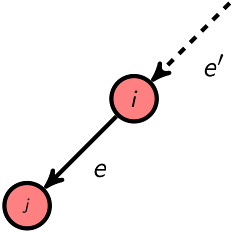
Linear Network Error Correction Codes

- If there is an error on channel e, the output of the channel is $\tilde{U}_e = U_e + Z_e$, where U_e is the message which should be transmitted over the channel e and Z_e is the error occurred on e.



Linear Network Error Correction Codes

- We treat Z_e as a message called error message. So for the channel e, introduce the imaginary channel e', and assume that Z_e is injected into the channel e by e'.



For each channel $e \in E$, an imaginary channel e' is introduced. The network with imaginary channels is called the **extended network** and denoted by $\tilde{G} = (\tilde{V}, \tilde{E})$.

Linear Network Error Correction Codes

For $\tilde{G}$, the global encoding kernel $\tilde{f}_e$ for each $e \in \tilde{E}$ is an $(\omega + |E|)$-dimensional column vector and the entries can be indexed by the channels in $In(s) \cup E$.

1. For **imaginary message channels** d_i' $(1 \leq i \leq \omega)$ and **imaginary error channels** $e' \in E'$, define

$$\tilde{f}_{d_i'} = 1_{d_i'} \text{ and } \tilde{f}_{e'} = 1_e,$$

   where 1_d is the indicator function of $d \in In(s) \cup E$.

2. For other global encoding kernels $\tilde{f}_e, e \in E$:

$$\tilde{f}_e = \sum_{d \in In(tail(e))} k_{d,e}\tilde{f}_d + 1_e.$$

Linear Network Error Correction Codes

The matrix $\tilde{F}_t = \left[\tilde{f}_e : \; e \in In(t)\right]$ is called the decoding matrix at sink node t, and use $\mathrm{row}_t(d)$ to denote the row vector of $\tilde{F}_t$ corresponding to the channel d, $d \in In(s) \cup E$.

Definition

Let ρ be an error pattern, define

$$\Delta(t,\rho) = \langle \{\mathrm{row}_t(d) : \; d \in \rho\} \rangle;$$

$$\Phi(t) = \langle \{\mathrm{row}_t(d) : \; d \in In(s)\} \rangle;$$

where we call $\Delta(t,\rho)$ the error space of error pattern ρ and $\Phi(t)$ the message space.

Linear Network Error Correction Codes

Definition

- A linear network error correction code is called a regular code if for any $t \in T$, $\dim(\Phi(t)) = \omega$.
- The minimum distance of a regular network error correction code at a sink node t is defined by

$$d_{\min}^{(t)} = \min\{|\rho| : \dim(\Delta(t, \rho) \cap \Phi(t)) > 0\}.$$

Part III:

Universal Network MDS Codes

Singleton Bound and Network MDS Codes

Theorem (The Refined Singleton Bound)

Let $d_{\min}^{(t)}$ be the minimum distance of a regular linear network error correction code at a sink node $t \in T$. Then

$$d_{\min}^{(t)} \leq \delta_t + 1,$$

where $\delta_t = C_t - \omega$ is the redundancy of the sink node t.

Singleton Bound and Network MDS Codes

Theorem (The Refined Singleton Bound)

Let $d_{\min}^{(t)}$ be the minimum distance of a regular linear network error correction code at a sink node $t \in T$. Then

$$d_{\min}^{(t)} \leq \delta_t + 1,$$

where $\delta_t = C_t - \omega$ is the redundancy of the sink node t.

Remark:

- This refined Singleton bound is achievable.
- A linear network error correction code is called network error correction maximum distance separable (MDS) code, or network MDS code for short, if it satisfies this bound with equality.

Basic Assumptions

- In a communication network G, the source node transmits the messages at several distinct rates $\omega_1, \omega_2, \cdots, \omega_h$ within a session.
- Let $\omega = \max\{\omega_1, \omega_2, \cdots, \omega_h\}$ satisfying

$$\omega \le \min_{t \in T} C_t,$$

where C_t is the minimum cut capacity between the source node s and the sink node t.
- There exists an ω-dimensional $\mathcal{F}$-value linear network error correction MDS code $\mathbf{C}_\omega$.

Conclusion

- An $(\omega - 1)$-dimensional network MDS code $\mathbf{C}_{\omega-1}$ with the same local encoding kernels as that of $\mathbf{C}_{\omega}$ at all non-source nodes can be constructed.
- Using this method recursively, we can construct all ω_i-dimensional $(1 \leq i \leq h)$ network MDS codes with the same local encoding kernels at all non-source nodes.

Lemma 1

Definition

Use $\mathrm{row}_t(d)$ to denote the row vector of the decoding matrix $\tilde{F}_t = \left[\tilde{f}_e : e \in In(t)\right]$ indicated by the channel $d \in In(s) \cup E$. Then,

$$\tilde{F}_t = \begin{bmatrix} F_t \\ G_t \end{bmatrix}$$

where $F_t = \begin{bmatrix} \mathrm{row}_t(d_1) \\ \vdots \\ \mathrm{row}_t(d_\omega) \end{bmatrix}$ and $G_t = \begin{bmatrix} \mathrm{row}_t(e_1) \\ \vdots \\ \mathrm{row}_t(e_{\mathcal{E}}) \end{bmatrix}$.

Lemma 1

Lemma 1

Let $\mathbf{C}_\omega$ be an ω-dimensional regular linear network error correction code over an acyclic network G, and $\vec{k} = (k_1, k_2, \cdots, k_{\omega-1})^\top \in \mathcal{F}^{\omega-1}$ be an arbitrary $(\omega-1)$-dimensional column vector. Define the matrix

$$F_t^{(\omega-1)}(\vec{k}) = \begin{bmatrix} I_{\omega-1} & \vec{k} \end{bmatrix} \cdot F_t,$$

where $I_{\omega-1}$ is an $(\omega-1) \times (\omega-1)$ identity matrix. Then the row vectors of $F_t^{(\omega-1)}(\vec{k})$ are still linearly independent, i.e.,

$$\mathrm{Rank}(F_t^{(\omega-1)}(\vec{k})) = \omega - 1.$$

Lemma 2

Definition

- Let $\tilde{f}_e$ be the extended global encoding kernel of $\mathbf{C}_\omega$ for the channel $e \in E$.
- Let $\vec{k} = (k_1, \cdots, k_{\omega-1})^\top \in \mathcal{F}^{\omega-1}$ be an arbitrary $(\omega-1)$-dimensional column vector.

For each non-imaginary channel e, define

$$\tilde{f}_e^{(\omega-1)}(\vec{k}) = \begin{bmatrix} I_{\omega-1} & \vec{k} & \underline{0}_{(\omega-1)\times\mathcal{E}} \\ \underline{0}_{\mathcal{E}\times(\omega-1)} & \underline{0}_{\mathcal{E}\times 1} & I_{\mathcal{E}} \end{bmatrix} \cdot \tilde{f}_e,$$

where $I_{\omega-1}$ and $I_{\mathcal{E}}$ denote $(\omega-1)\times(\omega-1)$ and $\mathcal{E}\times\mathcal{E}$ identity matrices, respectively, and $\underline{0}_{a\times b}$ represents an $a \times b$ all-zero matrix.

Lemma 2

Lemma 2

If $\{\tilde{f}_e : e \in E\}$ constitutes a global description of an ω-dimensional $\mathcal{F}$-value regular linear network error correction code $\mathbf{C}_\omega$ over an acyclic network G, then $\{\tilde{f}_e^{(\omega-1)}(\vec{k}) : e \in E\}$ constitutes a global description of an $(\omega - 1)$-dimensional regular linear network error correction code for G. In particular, the local encoding kernels of this $(\omega - 1)$-dimensional code at each non-source node are the same as that of the original ω-dimensional code $\mathbf{C}_\omega$.

Proof of Lemma 2

Idea of Proof: Mainly prove...

- For each channel $e \in Out(s)$, the following formula holds:

$$\tilde{f}_e^{(\omega-1)}(\vec{k}) = \sum_{i=1}^{\omega-1} k_{d_i,e}^{(\omega-1)}(\vec{k}) \cdot \tilde{f}_{d_i}^{(\omega-1)} + 1_e^{(\omega-1)},$$

where $k_{d_i,e}^{(\omega-1)}(\vec{k}) = k_{d_i,e} + k_i k_{d_\omega,e}$, $i = 1, 2, \cdots, \omega - 1$, and $1_e^{(\omega-1)}$ is an $(\omega - 1 + \mathcal{E})$-dimensional column vector which is the indicator function of e.

Proof of Lemma 2

- For other non-imaginary channel $e \notin Out(s)$, the following formula holds:

$$\tilde{f}_e^{(\omega-1)}(\vec{k}) = \sum_{d \in In(tail(e))} k_{d,e} \tilde{f}_d^{(\omega-1)}(\vec{k}) + 1_e^{(\omega-1)}.$$

Proof of Lemma 2

- For other non-imaginary channel $e \notin Out(s)$, the following formula holds:

$$\tilde{f}_e^{(\omega-1)}(\vec{k}) = \sum_{d \in In(tail(e))} k_{d,e} \tilde{f}_d^{(\omega-1)}(\vec{k}) + 1_e^{(\omega-1)}.$$

Note that the local encoding coefficients remain unchanged.

Proof of Lemma 2

- For other non-imaginary channel $e \notin Out(s)$, the following formula holds:

$$\tilde{f}_e^{(\omega-1)}(\vec{k}) = \sum_{d \in In(tail(e))} k_{d,e} \tilde{f}_d^{(\omega-1)}(\vec{k}) + 1_e^{(\omega-1)}.$$

Note that the local encoding coefficients remain unchanged.

- The global description $\{\tilde{f}_e^{(\omega-1)}(\vec{k}) : e \in E\}$ of this $(\omega-1)$-dimensional linear network error correction code is regular (Lemma 1 is required).

□

Lemma 3

Lemma 3

For the minimum distance of a regular linear network error correction code at sink node t, there exist the following equalities:

$$\begin{aligned} d_{\min}^{(t)} &= \min\{rank_t(\rho) : \ \Delta(t,\rho) \cap \Phi(t) \neq \{\underline{0}\}\} \\ &= \min\{|\rho| : \ \Delta(t,\rho) \cap \Phi(t) \neq \{\underline{0}\}\} \\ &= \min\{\dim(\Delta(t,\rho)) : \ \Delta(t,\rho) \cap \Phi(t) \neq \{\underline{0}\}\}. \end{aligned}$$

Proof of Lemma 3

Idea of Proof: Define the set of error patterns:

$$\Pi = \{\rho : \Delta(t,\rho) \cap \Phi(t) \neq \{\underline{0}\}\}.$$

- Clearly,

$$\min_{\rho\in\Pi} \dim(\Delta(t,\rho)) \leq \min_{\rho\in\Pi} rank_t(\rho) \leq \min_{\rho\in\Pi} |\rho|.$$

- Need to prove:

$$\min_{\rho\in\Pi} |\rho| \leq \min_{\rho\in\Pi} \dim(\Delta(t,\rho)).$$

□

Lemma 4

Lemma 4

For the ω-dimensional network MDS code $\mathbf{C}_\omega$ on G, define

$$Q(t) = \left\{ \text{error pattern } \rho : \Delta(t,\rho) \cap \Phi(t) \neq \{\underline{0}\} \text{ and } |\rho| = d_{\min}^{(t)} \right\}.$$

Then for any $\rho \in Q(t)$,

$$\dim(\Delta(t,\rho) \cap \Phi(t)) = 1.$$

Lemma 5

Lemma 5

For an acyclic network G, an ω-dimensional $\mathcal{F}$-value linear network error correction MDS code is given and $|\mathcal{F}| > \sum_{t\in T} |Q(t)|$. Then there exists an $(\omega-1)$-dimensional column vector $\vec{k} = (k_1, k_2, \cdots, k_{\omega-1})^\top \in \mathcal{F}^{\omega-1}$ such that

$$\dim(\Delta(t,\rho) \cap \Phi^{(\omega-1)}(t,\vec{k})) = 0$$

for each sink node $t \in T$ and each error pattern $\rho \in Q(t)$, where

$$\Phi^{(\omega-1)}(t,\vec{k}) = \langle\{\mathrm{row}_t(d_i) + k_i \cdot \mathrm{row}_t(d_\omega) : 1 \le i \le \omega-1\}\rangle.$$

[1]

[1] The proofs of Lemmas 4 and 5 are complicated, please refer to the paper for technical details.

Theorem

Theorem

Let $\mathbf{C}_\omega$ be an ω-dimensional $\mathcal{F}$-value linear network error correction MDS code and $\mathcal{F}$ be the base field satisfying $|\mathcal{F}| > \sum_{t \in T} |Q(t)|$. Then there exists an $(\omega - 1)$-dimensional $\mathcal{F}$-value linear network error correction MDS code $\mathbf{C}_{\omega-1}$ for this network G with the same local encoding kernels at all non-source nodes as that of $\mathbf{C}_\omega$.

Proof of Theorem

Idea of Proof:

There exists an $(\omega - 1)$-dimensional column vector $\vec{k} \in \mathcal{F}^{\omega-1}$ such that...

- $\{\tilde{f}_e^{(\omega-1)}(\vec{k}) : \ e \in E\}$ constitutes the set of all extended global encoding kernels of an $(\omega - 1)$-dimensional regular linear network error correction code. (Applying Lemmas 1 and 2)

Proof of Theorem

- For any $t \in T$ and any error pattern ρ with $|\rho| \leq \delta_t + 1$,

$$\Delta(t, \rho) \cap \Phi^{(\omega-1)}(t, \vec{k}) = \{\underline{0}\}.$$

  This implies

$$d_{\min}^{(t,\omega-1)} = \min\{|\rho| : \Delta(t, \rho) \cap \Phi^{(\omega-1)}(t, \vec{k}) \neq \{\underline{0}\}\} \geq \delta_t + 2.$$

  (Applying Lemmas 3, 4, and 5)

- On the other hand, by the refined Singleton bound, we have

$$d_{\min}^{(t,\omega-1)} \leq C_t - (\omega - 1) + 1 = \delta_t + 2.$$

□

Constructive Algorithm

Step 1: Construct an ω-dimensional network MDS code $\mathbf{C}_\omega$ on G;

Step 2: choose an $(\omega-1)$-dimensional column vector

$$\vec{k} = (k_1, k_2, \cdots, k_{\omega-1})^\top \in \mathcal{F}^{\omega-1}$$

such that $\Phi^{(\omega-1)}(t,\vec{k}) \cap \Delta(t,\rho) = \{\underline{0}\}$ for each $t \in T$ and each $\rho \in Q(t)$;

Step 3: $\{\tilde{f}_e^{(\omega-1)}(\vec{k}) : e \in E\}$ constitutes an $(\omega-1)$-dimensional network MDS code $\mathbf{C}_{\omega-1}$ with the same local encoding kernels at all internal nodes as that of $\mathbf{C}_\omega$.

Using this algorithm recursively, we can construct a family of universal network MDS codes of dimensions $1, 2, \cdots, \omega$.

Example

Preparation:

- $\omega = 2,\ C_{t_1} = C_{t_2} = 3,\ \delta_{t_1} = \delta_{t_2} = 1.$
- Base field $\mathcal{F} = \mathbb{Z}_3$.

Step 1:

All local encoding coefficients are
$k_{d_1,e_3} = k_{d_2,e_2} = k_{d_2,e_5} = 0$ and
$k_{d_1,e_1} = k_{d_1,e_2} = k_{d_1,e_4} = k_{d_1,e_5} = k_{d_2,e_1} =$
$k_{d_2,e_3} = k_{d_2,e_4} = k_{e_3,e_6} = k_{e_3,e_7} = 1.$

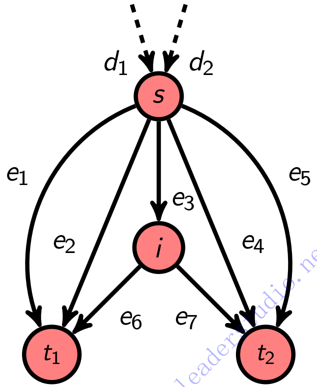


Figure: The network G.

Example

That is, all extended global kernels of this two-dimensional $\mathbb{Z}_3$-value network MDS code for all channels are

$$\tilde{f}_{e_1} = \begin{bmatrix} 1\\1\\1\\0\\0\\0\\0\\0\\0 \end{bmatrix} \quad \tilde{f}_{e_2} = \begin{bmatrix} 1\\0\\0\\1\\0\\0\\0\\0\\0 \end{bmatrix} \quad \tilde{f}_{e_3} = \begin{bmatrix} 0\\1\\0\\0\\1\\0\\0\\0\\0 \end{bmatrix} \quad \tilde{f}_{e_4} = \begin{bmatrix} 1\\1\\0\\0\\0\\1\\0\\0\\0 \end{bmatrix}$$

$$\tilde{f}_{e_5} = \begin{bmatrix} 1\\0\\0\\0\\0\\0\\1\\0\\0 \end{bmatrix} \quad \tilde{f}_{e_6} = \begin{bmatrix} 0\\1\\0\\0\\1\\0\\0\\1\\0 \end{bmatrix} \quad \tilde{f}_{e_7} = \begin{bmatrix} 0\\1\\0\\0\\1\\0\\0\\0\\1 \end{bmatrix}$$

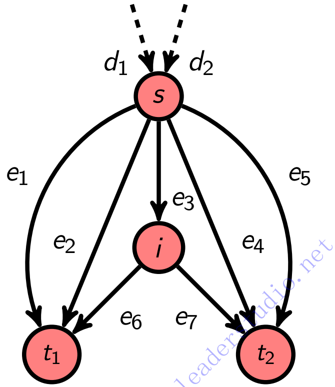


Figure: The network G.

Example

Step 2:

Let one-dimensional $\mathbb{Z}_3$-value column vector $\vec{k} = k = 1$. Then

$$k^{(\omega-1)}_{d_1,e_1}(\vec{k}) = k^{(\omega-1)}_{d_1,e_4}(\vec{k}) = 2,$$
$$k^{(\omega-1)}_{d_1,e_2}(\vec{k}) = k^{(\omega-1)}_{d_1,e_3}(\vec{k}) = k^{(\omega-1)}_{d_1,e_5}(\vec{k}) = 1,$$
$$k^{(\omega-1)}_{e_3,e_6}(\vec{k}) = k_{e_3,e_6} = 1,$$
$$k^{(\omega-1)}_{e_3,e_7}(\vec{k}) = k_{e_3,e_7} = 1.$$

Thus the $(\omega-1)$-dimensional decoding matrices are

$$\tilde{F}^{(\omega-1)}_{t_1}(\vec{k}) = \begin{bmatrix} 2&1&1\\ 1&0&0\\ 0&1&0\\ 0&0&1\\ 0&0&0\\ 0&0&0\\ 0&0&1\\ 0&0&0 \end{bmatrix}, \tilde{F}^{(\omega-1)}_{t_2}(\vec{k}) = \begin{bmatrix} 2&1&1\\ 0&0&0\\ 0&0&0\\ 0&0&1\\ 1&0&0\\ 0&1&0\\ 0&0&0\\ 0&0&1 \end{bmatrix}.$$

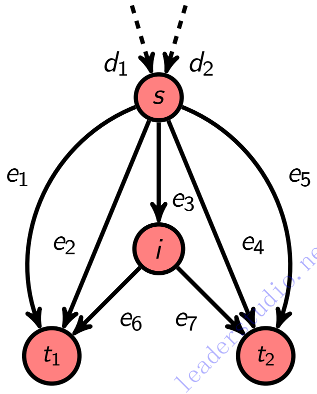


Figure: The network G.

Example

Step 3:

It is easy to check that the minimum distance of this code at t_1 (resp. t_2) is 3, i.e., an one-dimensional $\mathbb{Z}_3$-value network MDS code, and the local encoding kernels at all internal nodes are the same as that of the original two-dimensional $\mathbb{Z}_3$-value network MDS code.

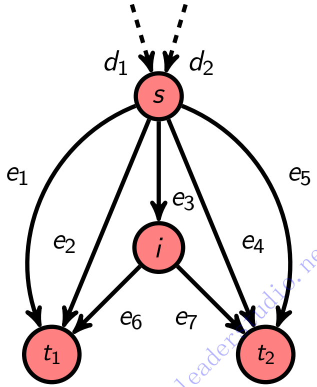


Figure: The network G.

Noncoherent Network Error Correction

If random network error correction coding is under consideration...

Theorem

Assume that random network coding is utilized in transmission on a single source multicast network G. Then universal network MDS codes can be constructed with high probability close to 1, if the size of the base field $\mathcal{F}$ is sufficiently large.

Reference

- R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204-1216, Jul. 2000.
- S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 371-381, Jul. 2003.
- R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. Netw.*, vol. 11, no. 5, pp. 782-795, Oct. 2003.
- R. W. Yeung and N. Cai, "Network error correction, part I: Basic concepts and upper bounds," *Communications in Infomation and Systems*, vol. 6, pp. 19-36, 2006.
- N. Cai and R. W. Yeung, "Network error correction, part II: Lower bounds," *Communications in Infomation and Systems*, vol. 6, pp. 37-54, 2006.
- Z. Zhang, "Linear network error correction codes in packet networks," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 209-218, Jan. 2008.

Reference

- X. Guang, F.-W. Fu, and Z. Zhang, "Construction of network error correction codes in packet networks," submitted to IEEE Trans. Inf. Theory. [Online]. Available: http://arxiv.org/abs/1011.1377.
- Z. Zhang, "Theory and Applications of Network Error Correction Coding," *Proceedings of the IEEE* , vol. 99, no. 3, pp. 406-420, Mar. 2011.
- S. Yang, R. W. Yeung, C. K. Ngai, "Refined coding bounds and code constructions for coherent network error correction," *IEEE Trans. Inf. Theory*, vol. 57, no. 3, pp. 1409-1424, Mar. 2011.
- S. L. Fong and R. W. Yeung, "Variable-rate linear network coding," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2618-2625, June 2010.
- T. Ho, R. Koetter, M. Médard, M. Effros, J. Shi, and D. Karger, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4413-4430, Oct. 2006.

Thanks for your attention!!!

Questions?