

# Vector Network Coding Gap Sizes for the Generalized Combination Network

Ha Nguyen

ha.nguyen@tum.de

September 5, 2019

- 1. Motivation
- 2. What is Network Coding?
- 3. Combinatorial Results
- 4. Computational Results
- 5. Conclusions



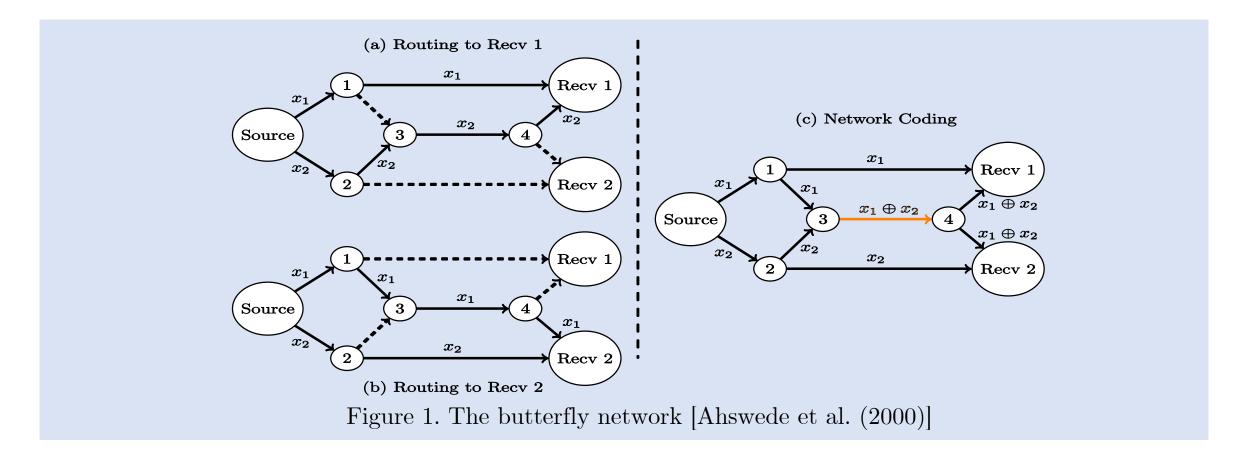
#### 1. Motivation

- 2. What is Network Coding?
- 3. Combinatorial Results
- 4. Computational Results
- 5. Conclusions



#### Motivation

Network coding gives a **potential gain in throughput** by communicating more information with fewer packet transmissions compared to the routing method.



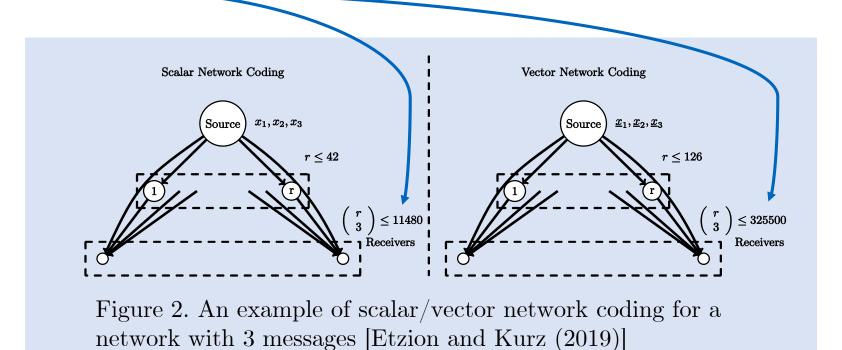


#### Motivation (cont.)

Vector network coding (VNC) → Field size reduction [Etzion and Wachter-Zeh (2018)].

E.g.  $\mathbb{F}_{2^8} \to \mathbb{F}_2^5$  (58472 middle-layer nodes)

Number of receivers is large.

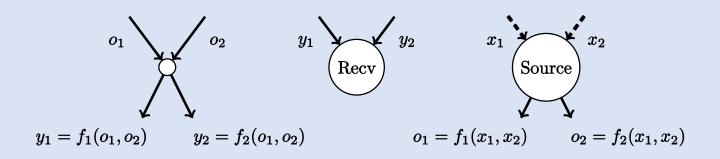




- 1. Motivation
- 2. What is Network Coding?
  - Coding at a Node
  - Our Choice of Network Model
  - Network as a Matrix Channel
  - Gap size between scalar and vector solutions
- 3. Combinatorial Results
- 4. Computational Results
- 5. Conclusions

## Coding at a node

Store-and-forward in simple routing |Yeung et al. (2006)|  $\rightarrow$  each node can transmit an arbitrary combination of its received packets in network coding [Ahswede et al. (2000)].



- a) Intermediate Node b) Destination Node
- c) Source Node

Figure 3. Incoming links and outgoing links of a node in network coding

- 1. Motivation
- 2. What is Network Coding?
  - Coding at a Node
  - Our Choice of Network Model
  - Network as a Matrix Channel
  - Gap size between scalar and vector solutions
- 3. Combinatorial Results
- 4. Computational Results
- 5. Conclusions

#### Our Choice of Network Model

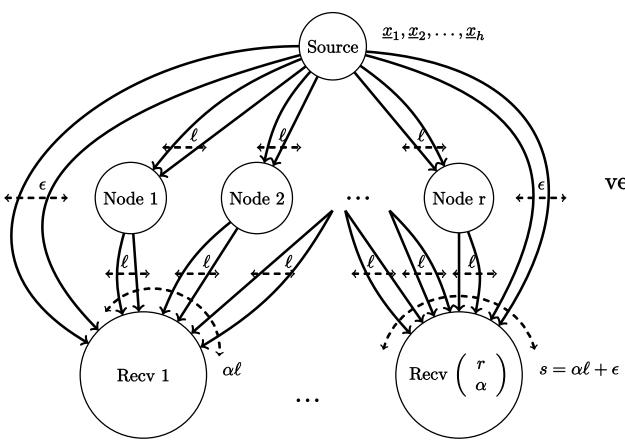


Figure 4. Generalized Combination Network (GCN)

Combination Network (CN) was introduced by Riis and Ahlswede in 2006.

A generalization of CN with  $\epsilon$  direct links and  $\ell$  multiple links was used to prove that vector network coding outperforms scalar network coding [Etzion and Wachter-Zeh 2018].

Able to demonstrate networks with large capacity.

## Our Choice of Network Model (cont.)

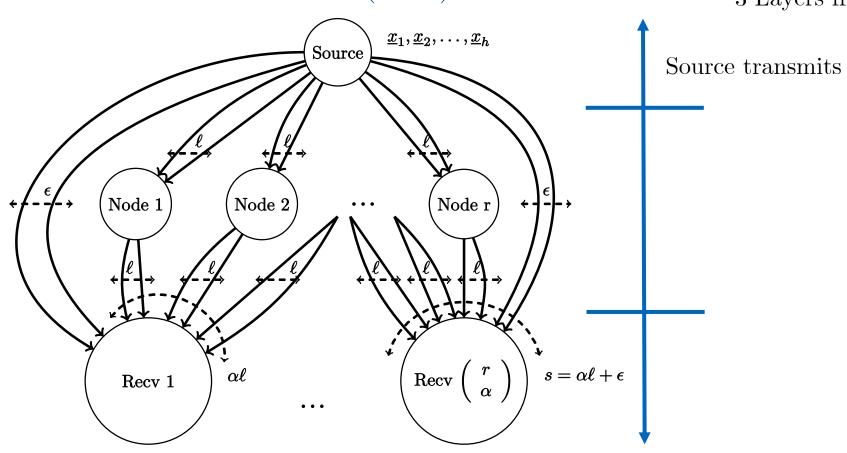


Figure 4. Generalized Combination Network (GCN)

#### 3 Layers from Top to Bottom

 $x_1, \dots, x_h \in \mathbb{F}_{q_s}$  (Scalar NC) or  $\underline{x}_1, \dots, \underline{x}_h \in \mathbb{F}_q^t$  (Vector NC)

# In

## Our Choice of Network Model (cont.)

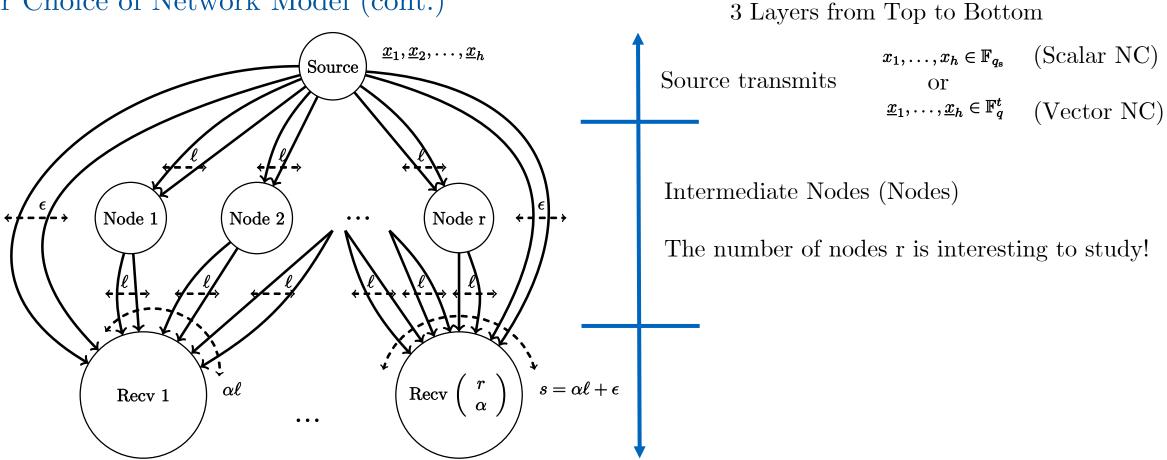


Figure 4. Generalized Combination Network (GCN)



## Our Choice of Network Model (cont.)

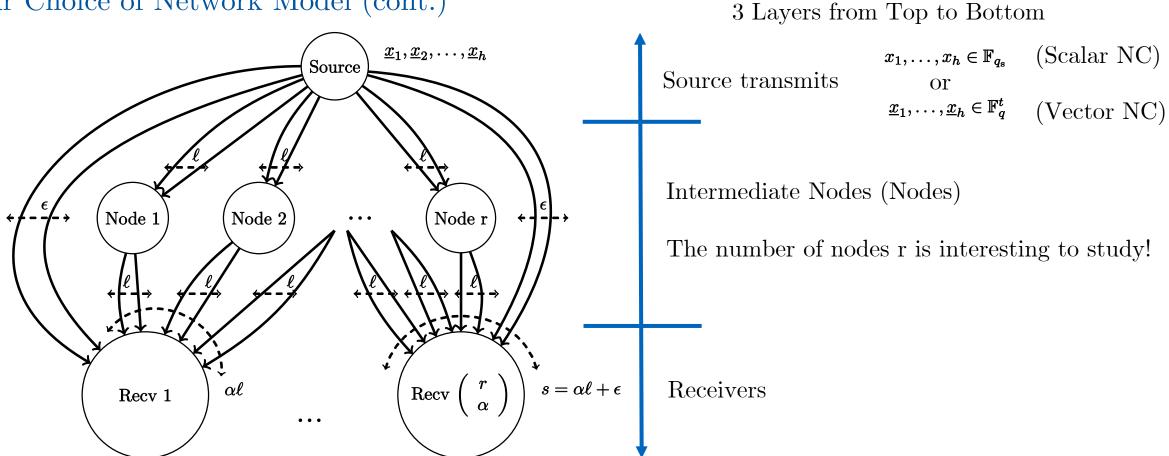


Figure 4. Generalized Combination Network (GCN)



## Our Choice of Network Model (cont.)

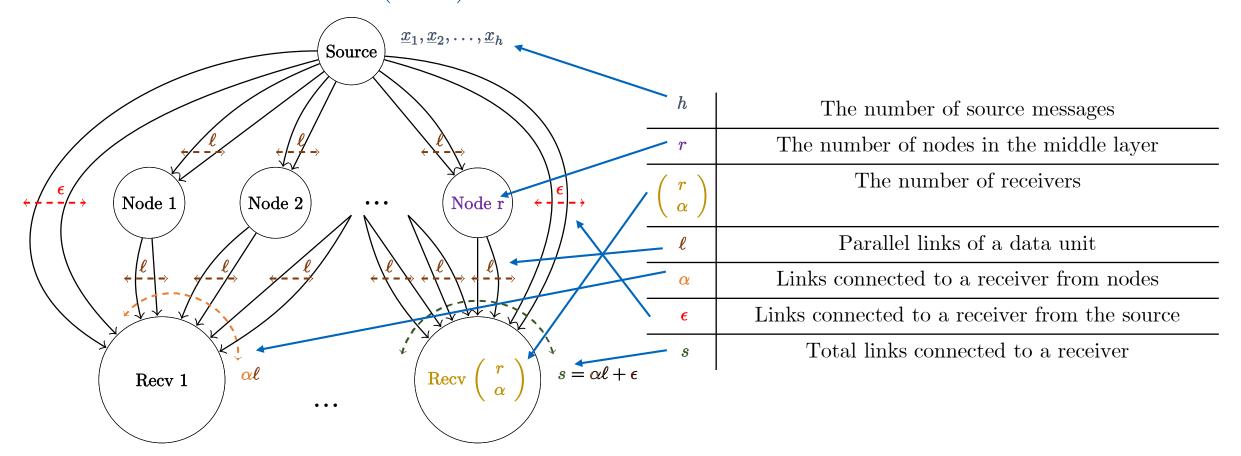


Figure 4. Generalized Combination Network (GCN)

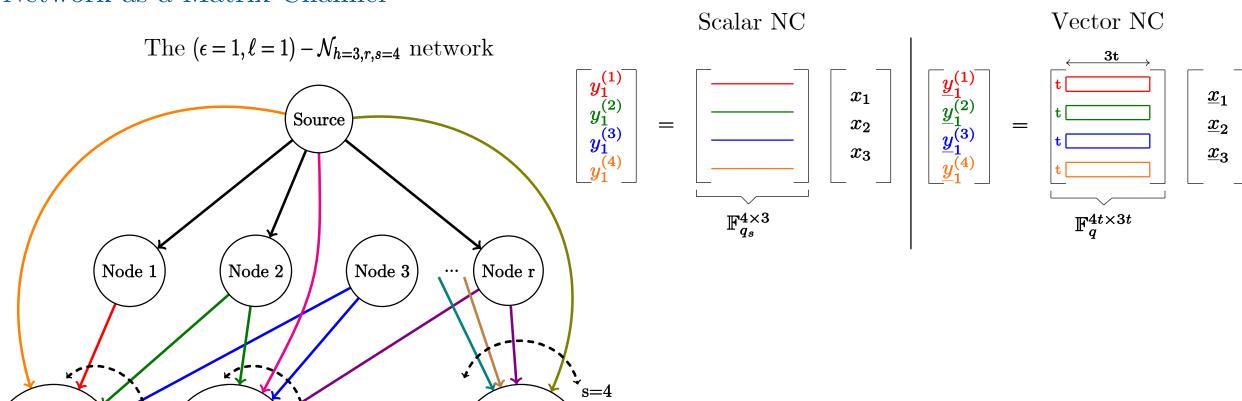


- 1. Motivation
- 2. What is Network Coding?
  - Coding at a Node
  - Our Choice of Network Model
  - Network as a Matrix Channel
  - Gap size between scalar and vector solutions
- 3. Combinatorial Results
- 4. Computational Results
- 5. Conclusions

Recv 1





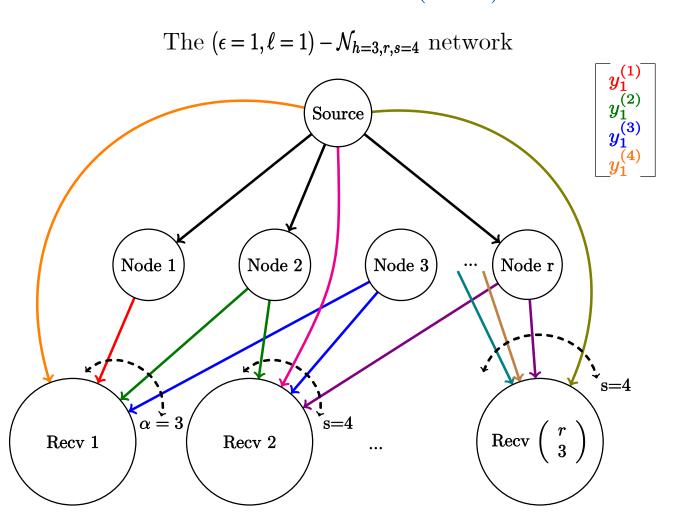


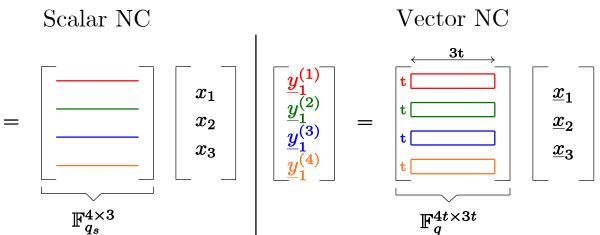
 $\operatorname{Recv}\left(egin{array}{c} r \ 3 \end{array}
ight)$ 

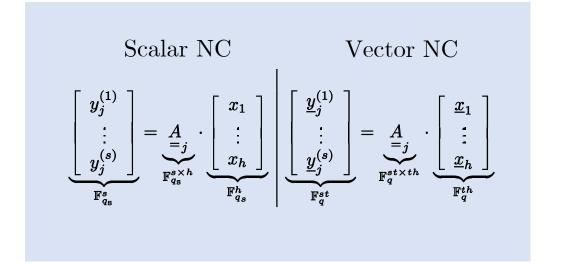
s=4

Recv 2



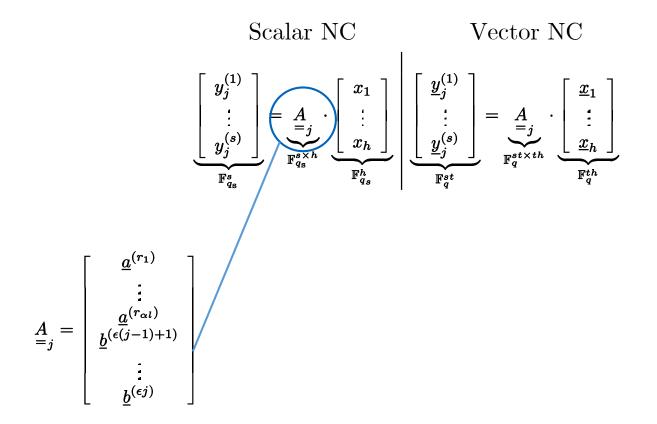






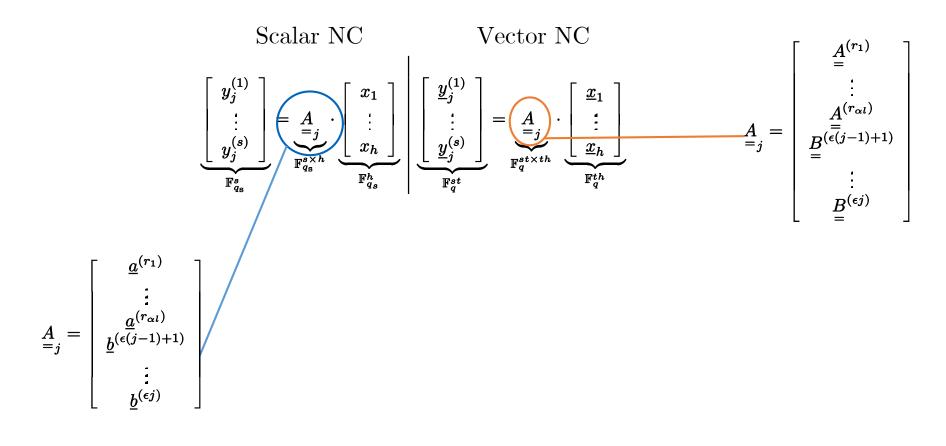




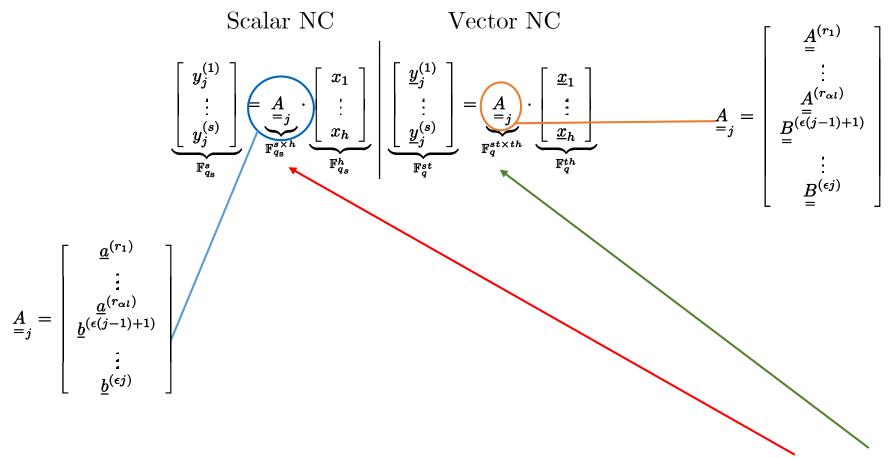












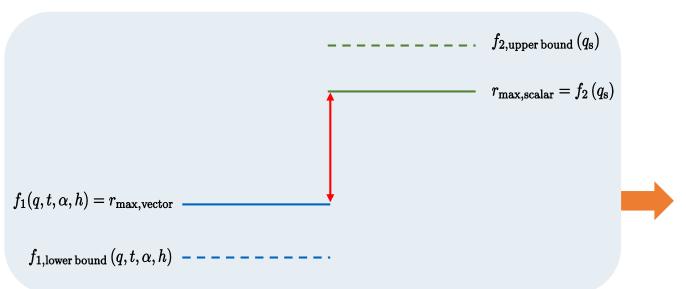
By using the vector coding, the upper bound number of solutions increases from  $q^{tsh}$  to  $q^{t^2sh}$ .

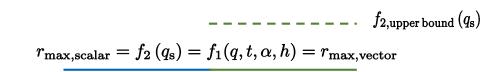


- 1. Motivation
- 2. What is Network Coding?
  - Coding at a Node
  - Our Choice of Network Model
  - Network as a Matrix Channel
  - Gap size between scalar and vector solutions
- 3. Combinatorial Results
- 4. Computational Results
- 5. Conclusions



## Gap size between scalar and vector solutions

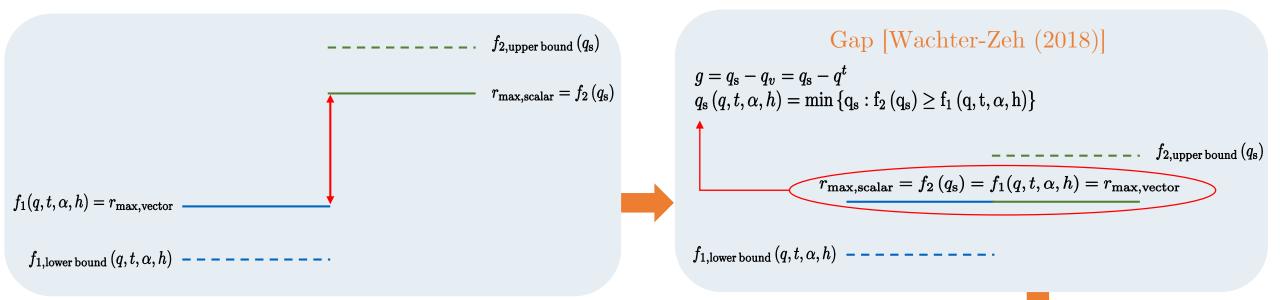


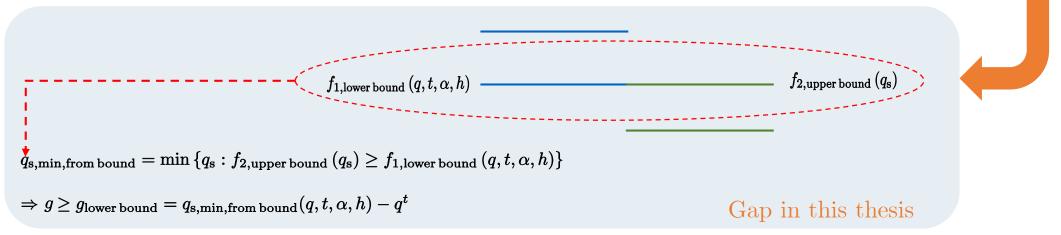


 $f_{1, ext{lower bound}}\left(q,t,lpha,h
ight) \ ------$ 



## Gap size between scalar and vector solutions (cont.)







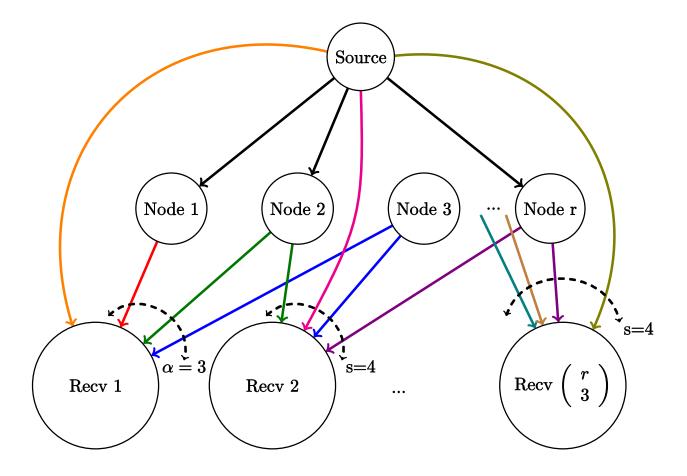
## Gap size between scalar and vector solutions (cont.)

Network	Gaps for a specific vector solution [Etzion and Wachter-Zeh (2018)]	Lower bounds on gaps for a general vector solution [Corollary 5.4 and Corollary 5.3]	
$(\epsilon=0,\ell=1)-\mathcal{N}_{h,r,s}$	N/A	$\mathrm{N/A}$	
$(\epsilon \geq 1, \ell = 1) - \mathcal{N}_{h,r,s}$	N/A	$q^{\frac{\epsilon(\alpha-h+\epsilon)}{(\alpha-1)(\alpha-h+\epsilon+1)(h-\epsilon-1)}t^2 + \mathcal{O}(t)}$	
$(\epsilon = 1, \ell > 1) - \mathcal{N}_{h=2\ell, r, s=2\ell+1}$	$q^{t^2/2+\mathcal{O}(t)}$	$q^{t^2/l+\mathcal{O}(t)}$	
$(\epsilon = \ell - 1, \ell) - \mathcal{N}_{h=2\ell, r, s=3\ell-1}$	$q^{t^2/2+\mathcal{O}(t)}$	$\mathrm{N/A}$	

Table 1. Lower bounds on gaps were found in this study.

- 1. Motivation
- 2. What is Network Coding?
- 3. Combinatorial Results
  - Proof of a gap for a network with 3 messages
- 4. Computational Results
- 5. Conclusions

We show the proof of the most simple case. Other cases considered in this study are similar to this proof.





Each receiver  $R_j$  has to solve a linear equation system of 3t variables with 4t equations to recover 3 source messages as below:

$$\begin{bmatrix} \underline{y}_{j}^{(1)} \\ \underline{y}_{j}^{(2)} \\ \underline{y}_{j}^{(3)} \\ \underline{y}_{j}^{(4)} \end{bmatrix} = \underbrace{A_{j}} \cdot \underline{x} = \begin{bmatrix} A^{(r_{1})} \\ A^{(r_{2})} \\ A^{(r_{3})} \\ A^{(r_{3})} \\ B^{(j)} \\ B \end{bmatrix} \cdot \begin{bmatrix} \underline{x}_{1} \\ \underline{x}_{2} \\ \underline{x}_{3} \end{bmatrix},$$

with 
$$\underline{x}_1, \dots, \underline{x}_3 \in \mathbb{F}_q^t$$

$$\underline{y}_j^{(1)}, \dots, \underline{y}_j^{(4)} \in \mathbb{F}_q^t$$

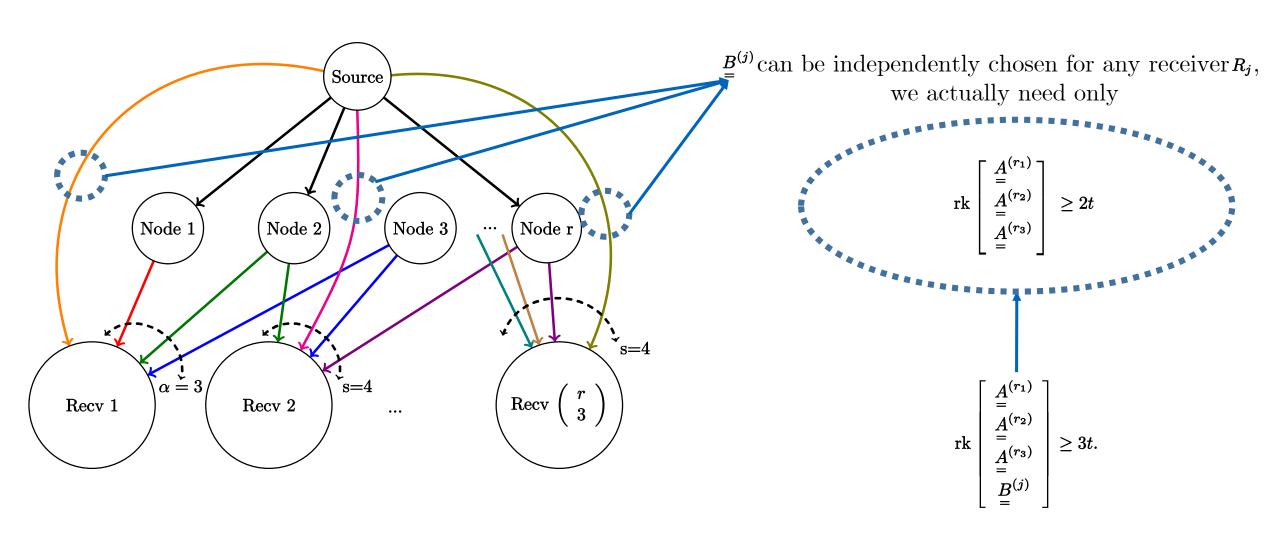
$$\underline{A}_j^{(r_1)}, \dots, \underline{A}_j^{(r_3)} \in \mathbb{F}_q^{t \times 3t} \text{ for } 1 \le r_1 < r_2 < r_3 \le r$$

$$\underline{B}_j^{(j)} \in \mathbb{F}_q^{t \times 3t} \text{ for } j \in \left\{1, \dots, \binom{r}{3}\right\}$$

The network is solvable if  $\underline{\underline{A}}_{j}$  has full rank,

$$\operatorname{rk} \left[ \begin{array}{c} A^{(r_1)} \\ = \\ A^{(r_2)} \\ = \\ A^{(r_3)} \\ = \\ B^{(j)} \\ = \end{array} \right] \geq 3t$$





We then apply the Lovász Local lemma to calculate a gap for the network [Proposed by Schwartz (2018)].

#### Lemma: Symmetric Lovász Local Lemma (LLL)

A set of events  $\mathcal{E}_i$ , such that each event occurs with probability at most p. If each event is independent of all others except for at most d of them and  $4pd \le 1$ , then:

$$\Pr\left[\bigcap_{i=1}^{n} \overline{\mathcal{E}}_{i}\right] > 0$$

We apply the LLL for the following events  $\mathcal{E}_{r_1,r_2,r_3}$ 

$$\mathcal{E}_{r_1,r_2,r_3} = \left\{ egin{array}{l} \operatorname{rk} \left[ egin{array}{l} A^{(r_1)} \ A^{(r_2)} \ A^{(r_3)} \ B \end{array} 
ight] < 2t 
ight\},$$

$$1 \le r_1 < r_2 < r_3 \le r$$

where

$$\underline{A}^{(r_1)}, \dots, \underline{A}^{(r_3)} \in \mathbb{F}_q^{t \times 3t}$$

 $\underline{A}^{(r_1)}, \dots, \underline{A}^{(r_3)} \in \mathbb{F}_q^{t \times 3t}$  are independently and uniformly random.



$$\Pr\left[\mathcal{E}_{r_{1},r_{2},r_{3}}\right] = \Pr\left[\operatorname{rk}\left[\begin{array}{c}A^{(r_{1})}\\ \equiv\\ A^{(r_{2})}\\ \equiv\\ A^{(r_{3})}\end{array}\right] < 2t\right] = \sum_{i=0}^{2t-1}\Pr\left[\operatorname{rk}\left[\begin{array}{c}A^{(r_{1})}\\ \equiv\\ A^{(r_{2})}\\ \equiv\\ A^{(r_{3})}\\ \equiv\\ \end{array}\right] = i\right]$$

$$= \sum_{i=0}^{2t-1}\frac{\operatorname{NM}_{i,3t,3t}}{q^{(3t)\cdot(3t)}}$$

$$= \sum_{i=0}^{2t-1}\frac{\prod_{j=0}^{i-1}\frac{\left(q^{3t}-q^{j}\right)^{2}}{q^{i}-q^{j}}}{q^{9t^{2}}}.$$

Number of  $[n \times m]$  matrices of rank *i* over  $\mathbb{F}_q$ |Overbeck (2007)|

$$NM_{i,n,m} = \prod_{j=0}^{i-1} \frac{(q^m - q^j) (q^n - q^j)}{q^i - q^j}.$$



$$\Pr\left[\mathcal{E}_{r_{1},r_{2},r_{3}}\right] = \Pr\left[\operatorname{rk}\begin{bmatrix} A^{(r_{1})} \\ A^{(r_{2})} \\ A^{(r_{3})} \\ A^{(r_{3})} \end{bmatrix} < 2t\right] = \sum_{i=0}^{2t-1} \Pr\left[\operatorname{rk}\begin{bmatrix} A^{(r_{1})} \\ A^{(r_{2})} \\ A^{(r_{3})} \\ A^{(r_{3})} \end{bmatrix} = i\right]$$

$$= \sum_{i=0}^{2t-1} \frac{\operatorname{NM}_{i,3t,3t}}{q^{(3t)\cdot(3t)}}$$

$$= \sum_{i=0}^{2t-1} \frac{\prod_{j=0}^{i-1} \frac{(q^{3t}-q^{j})^{2}}{q^{i}-q^{j}}}{q^{9t^{2}}}.$$

$$\operatorname{Lemma 5.2}$$

$$\Pr\left[\mathcal{E}_{r_{1},r_{2},r_{3}}\right] \leq p \in \Theta\left(q^{-t^{2}-2t-1}\right), \forall t \geq 2.$$

Number of  $[n \times m]$  matrices of rank *i* over  $\mathbb{F}_q$ |Overbeck (2007)|

$$NM_{i,n,m} = \prod_{j=0}^{i-1} \frac{(q^m - q^j)(q^n - q^j)}{q^i - q^j}.$$

Lemma 5.2

$$\Pr\left[\mathcal{E}_{r_1,r_2,r_3}\right] \le p \in \Theta\left(q^{-t^2-2t-1}\right), \forall t \ge 2.$$

We study the asymptotic behaviour of LLL parameters when  $q \to \infty$  by using the Bachmann-Landau notations.

 $\Theta(f(q,t))$  for a tight bound

 $\Omega(f(q,t))$  for a lower bound

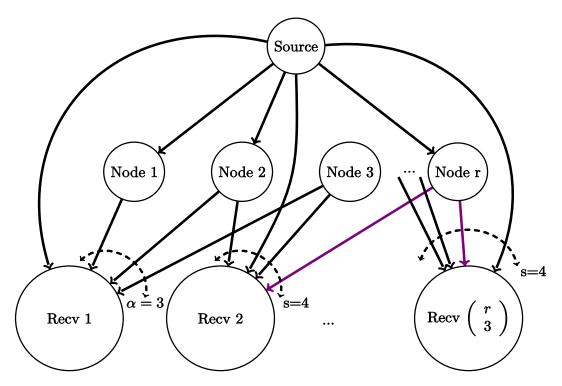
 $\mathcal{O}\left(f\left(q,t\right)\right)$  for an upper bound

#### Lemma 5.3

Each event is dependent at most  $d(r) \leq \frac{3}{2}r^2$  other events.

$$\mathcal{E}_{r_1,r_2,r_3}$$
 is dependent on  $\mathcal{E}_{r_1',r_2',r_3'}$  if and only if  $\{r_1,r_2,r_3\} \cap \left\{r_1',r_2',r_3'\right\} \neq \emptyset$ 

$$\Rightarrow d(r) \leq 3 \cdot \left(\begin{array}{c} r-1\\2 \end{array}\right)$$



Example that "Node r" is chosen for 2 receivers.



#### Lemma 5.3

Each event is dependent at most  $d(r) \leq \frac{3}{2}r^2$  other events.

#### Lemma 5.2

$$\Pr\left[\mathcal{E}_{r_1,r_2,r_3}\right] \le p \in \Theta\left(q^{-t^2-2t-1}\right), \forall t \ge 2.$$

#### Lemma: Symmetric Lovász Local Lemma (LLL)

A set of events  $\mathcal{E}_i$ , such that each event occurs with probability at most p. If each event is independent of all others except for at most d of them and  $4pd \leq 1$ , then:

$$\Pr\left[\bigcap_{i=1}^{n} \overline{\mathcal{E}}_{i}\right] > 0$$

#### Theorem 5.1

There is an  $r_{\text{max,vector}} \in \Omega\left(q^{t^2/2 + \mathcal{O}(t)}\right)$  such that for any  $r \leq r_{\text{max,vector}}$  there exists a vector solution for the  $(\epsilon = 1, l = 1) - \mathcal{N}_{h=3,r,s=4}$  network.



The optimal scalar solution exists for  $r_{\text{max,scalar}} \in \mathcal{O}(q_s^2)$  [Etzion and Wachter-Zeh (2018)].

Applying Theorem 5.1 on slide 32 and the formula of gap on slide 22, we have

$$r_{
m max,scalar} = r_{
m max,vector}$$
 $\Leftrightarrow q_{
m s,min,from\,bound}^2 = q^{t^2/2+\mathcal{O}(t)}$ 
 $\Leftrightarrow q_{
m s,min,from\,bound} = q^{t^2/4+\mathcal{O}(t)}$ 
 $\Rightarrow g_{
m lower\,bound} = q_{
m s,min,from\,bound} - q_v = q^{t^2/4+\mathcal{O}(t)}$ 

#### Corollary 5.1

The  $(\epsilon = 1, \ell = 1) - \mathcal{N}_{h=3,r,s=4}$  network has a vector solution with a gap  $q^{t^2/4+\mathcal{O}(t)}$ .

Similar to the  $(\epsilon = 1, \ell = 1) - \mathcal{N}_{h=3,r,s=4}$  network, we proved a gap for a more general network in Corollary 5.3.

#### Corollary 5.3

The  $(\epsilon = 1, \ell = 1) - N_{h,r,s}$  network has a vector solution with a gap  $q^{\frac{\alpha - h + 1}{(\alpha - 1)(\alpha - h + 2)(h - 2)}t^2} + \mathcal{O}(t)$ 



- 1. Motivation
- 2. What is Network Coding?
- 3. Combinatorial Results
- 4. Computational Results
- 5. Conclusions



## Computational Results

t	Scalar Solution	Vector Solution	$\begin{array}{c} {\rm Etzion~and~Kurz} \\ (2019) \end{array}$	Construction 1	Construction 2
2	$r_{\rm max,scalar} = 42$	$r_{ m max,vector} \geq 7$	$r_{\text{max,vector}} = 121$	$r_{\text{max,vector}} = 89$	N/A
3	$r_{\text{max,scalar}} = 146$	$r_{ m max,vector} \geq 62$	N/A	N/A	$\left(r_{ m max,vector} = 166\right)$
4	$r_{\rm max,scalar} = 546$	$r_{\rm max, vector} \ge 1317$	N/A	N/A	N/A
5	$r_{\text{max,scalar}} = 2114$	$r_{ m max,vector} \ge 58472$	N/A	N/A	N/A
6	$r_{\text{max,scalar}} = 8322$	$r_{\text{max,vector}} > 10^6$	N/A	N/A	N/A

For t = 2, Etzion and Kurz provide the best vector solution.

For t = 3, this study provides the only vector solution outperforming the optimal scalar solution.

For t = 4, 5, 6, the combinatorial results from this study already show large gaps.

## Computational Results (cont.)

Approaches that we tried in this study:

1. Random Increasing Method

✓

Start with a random pair [A, B], then randomly extend to [A, B, C].

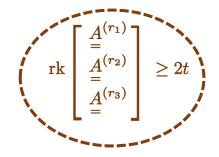
Similarly, we continue to extend until no more possibility.

## Computational Results (cont.)

Approaches that we tried in this study:

- 1. Random Increasing Method
- 2. Increasing Method (IM) with Extra Information

If we input a set of 4096 matrices, we know all subsets of 3 matrices satisfying the rank requirement. Then, we use this information to search for a vector solution.





## Computational Results (cont.)

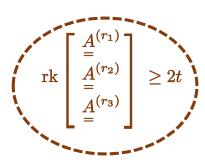
Approaches that we tried in this study:

- 1. Random Increasing Method
- 2. Increasing Method (IM) with Extra Information
- 3. Decreasing Method with Learning Bad Events over Each Step



Start with a set of all matrices

- → Check matrix with high frequency in events that the rank requirement is not satisfied.
- → Remove such a matrix
- → Keep doing until any 3 matrices left in the set meet the rank requirement.



- 1. Motivation
- 2. What is Network Coding?
- 3. Combinatorial Results
- 4. Computational Results
- 5. Conclusions



#### Conclusion

#### Summary:

- Tool to derive general vector solutions for instances of the generalized combination network based on the Lovász Local Lemma.
- By combinatorial results, vector solutions can be generally proved to outperform scalar solutions.

#### Further Results: (not in presentation)

• A new bound on a three-dimensional subspace code over  $\mathbb{F}_2^9$ .

#### Open:

- Code construction of the codebook found in the computational results.
- Apply the Lovász Local Lemma to all other instances of the generalized combination network.

## Conclusion (cont.)

#### Summary:

- Tool to derive general vector solutions for instances of the generalized combination network based on the Lovász Local Lemma.
- By combinatorial results, vector solutions can be generally proved to outperform scalar solutions.

#### Further Results: (not in presentation)

• A new bound on a three-dimensional subspace code over  $\mathbb{F}_2^9$ .

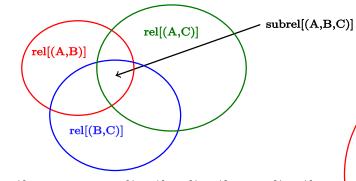
#### Open:

- Code construction of the codebook found in the computational results.
- Apply the Lovász Local Lemma to all other instances of the generalized combination network.

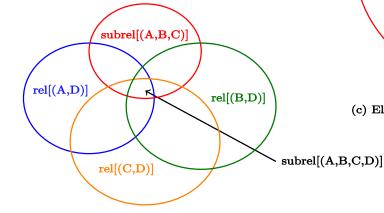
## Thank you for your attention!

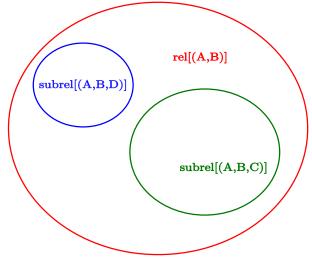
## Computational Results

We analyze the IM for case t = 3 of the  $(\epsilon = 1, \ell = 1) - \mathcal{N}_{h=3,r,s=4}$  network.



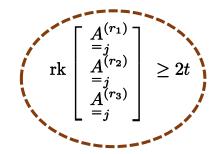
(a) subrel[(A,B,C)] is a subset of  $\operatorname{rel}[(A,B)]$ ,  $\operatorname{rel}[(B,C)]$  and  $\operatorname{rel}[(A,C)]$ 





(c) Elements of subrel[.] are always contained in rel[.]

(b)  $\mathrm{subrel}[(A,B,C,D)] \ \mathrm{is} \ \mathrm{a} \ \mathrm{subset} \ \mathrm{of} \ \mathrm{subrel}[(A,B,C)], \ \mathrm{rel}[(A,D], \ \mathrm{rel}[(B,D] \ \mathrm{and} \ \mathrm{rel}[(C,D] \ \mathrm{rel}(B,D)]$ 





#### Mapping

$$x_1,\dots,x_{h=3}\in\mathbb{F}_{2^2}$$
  $oldsymbol{x}_{ ext{scalar}}=(x_1,x_2,x_3)=(1,lpha,lpha+1).$   $oldsymbol{x}_1,\dots,oldsymbol{x}_{h=3}\in\mathbb{F}_2^2$   $oldsymbol{x}_{ ext{vector}}=(oldsymbol{x}_1,oldsymbol{x}_2,oldsymbol{x}_3).$ 

$$\left[ egin{array}{c} x_1=1 \ x_2=lpha \ x_3=lpha+1 \end{array} 
ight] 
ightarrow \left[ egin{array}{c} 1 \ 0 \ 0 \ 1 \ 1 \ 1 \end{array} 
ight],$$

$$a_0 \cdot \alpha^0 + a_1 \cdot \alpha^1 + \ldots + a_{t-1} \cdot \alpha^{t-1} \rightarrow \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix}.$$