Vector Network Coding Based on Subspace Codes Outperforms Scalar Linear Network Coding

Tuvi Etzion & Antonia Wachter-Zeh

Computer Science Department
Technion—Israel Institute of Technology

May 1, 2016

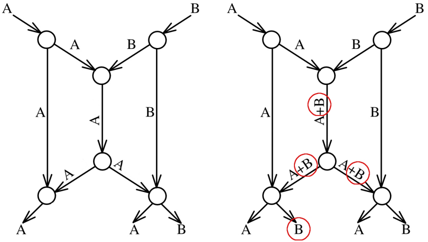
Technion CS Coding Seminar

Outline

Outline

Routing vs. Network Coding

Routing:
nodes simply
forward
packets

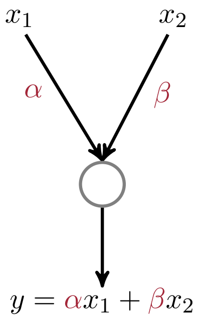


Network coding:
nodes perform
linear combinations

$\Longrightarrow$ Network coding achieves higher throughput than routing!

Task in network coding: determine coefficients of linear combinations such that all receivers obtain all packets.
(Here: **no** error-correction!)

Scalar and Vector Network Coding



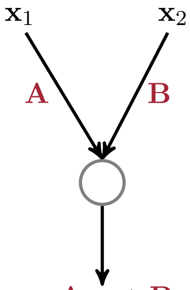
- scalar network coding:
  coefficients are scalars over field of size q_s
  $\rightsquigarrow$ for each coefficient: q_s possibilities

- vector network coding of dimension t:
  coefficients are $t \times t$ matrices over field of size q
  $\rightsquigarrow$ for each coefficient: q^{t^2} possibilities

For equivalent field sizes ($q_s = q^t$), vector network coding offers more freedom in choosing the coefficients!

- [Sun *et al.*, ISIT-2015]: There exist networks with a vector solution of dimension t over $\mathbb{F}_q$, but no scalar solution for $q_s \leq q^t$.
- Our contribution: gap of size $q^{t^2/2} - q^t$ (and more)

Scalar and Vector Network Coding



$\mathbf{y} = \mathbf{A}\mathbf{x}_1 + \mathbf{B}\mathbf{x}_2$

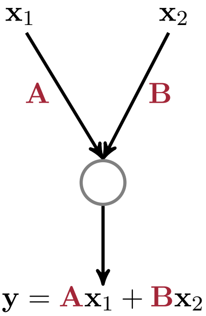
- scalar network coding:
  coefficients are scalars over field of size q_s
  $\rightsquigarrow$ for each coefficient: q_s possibilities

- vector network coding of dimension t:
  coefficients are $t \times t$ matrices over field of size q
  $\rightsquigarrow$ for each coefficient: q^{t^2} possibilities

For equivalent field sizes ($q_s = q^t$), vector network coding offers more freedom in choosing the coefficients!

- [Sun *et al.*, ISIT-2015]: There exist networks with a vector solution of dimension t over $\mathbb{F}_q$, but no scalar solution for $q_s \leq q^t$.
- Our contribution: gap of size $q^{t^2/2} - q^t$ (and more)

Scalar and Vector Network Coding



- scalar network coding:
  coefficients are scalars over field of size q_s
  $\rightsquigarrow$ for each coefficient: q_s possibilities
- vector network coding of dimension t:
  coefficients are $t \times t$ matrices over field of size q
  $\rightsquigarrow$ for each coefficient: q^{t^2} possibilities

For equivalent field sizes ($q_s = q^t$), vector network coding offers more freedom in choosing the coefficients!

- [Sun *et al.*, ISIT-2015]: There exist networks with a vector solution of dimension t over $\mathbb{F}_q$, but no scalar solution for $q_s \leq q^t$.
- Our contribution: gap of size $q^{t^2/2} - q^t$ (and more)

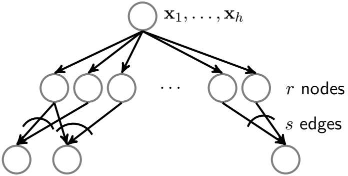
Previous Work on Vector Network Coding

[Médard–Effros–Karger–Ho, 2003]	example of a network which is *not* scalar solvable, but vector solvable
[Dougherty–Freiling–Zeger, 2005]	not every solvable network has a vector solution
[Jaggi–Cassuto–Effros, 2006]	low-complexity encoding schemes for vector network coding
[Cannons–Dougherty–Freiling–Zeger, 2006]	introduced fractional vector network coding
[Ebrahimi–Fragouli, 2011]	extended Kötter–Médard algebraic approach to *vector* network coding
[Dougherty–Freiling–Zeger, 2007]	vector codes outperform scalar linear codes in terms of achievable rate
[Langberg–Sprintson, 2008]	hardness of finding a general capacity-achieving vector solution
[Sun–Yang–Long–Li, 2015]	network with vector solution of field size q & dim. t, but no scalar solution of size q^t

Outline

The Combination Network

$\mathcal{N}_{h,r,s}$-combination network ($s \geq h$):



Three layers:

1. source with h messages
2. receive and forward linear combinations
3. $\binom{r}{s}$ receivers: connected to s middle nodes, request all h messages

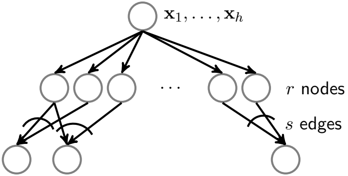
Theorem (Scalar Solution, e.g. [Riis & Ahlswede, 2006])

The $\mathcal{N}_{h,r,s}$-combination network has a scalar solution of field size q_s if and only if an $[r, h, d = r - s + 1]_{q_s}$ code exists.

$\implies$ if $h = s$: MDS code needed: $q_s \geq r - 1$
(if $k \in \{3, q - 1\}$ & q_s power of 2: $q_s \geq r - 2$)
$\implies$ decoding complexity: $\min\{\mathcal{O}(r \log^2 r), \mathcal{O}(h^{2.37})\}$ in $\mathbb{F}_{q_s}$

The Combination Network

$\mathcal{N}_{h,r,s}$-combination network ($s \geq h$):



Three layers:

1. source with h messages
2. receive and forward linear combinations
3. $\binom{r}{s}$ receivers: connected to s middle nodes, request all h messages

Theorem (Scalar Solution, e.g. [Riis & Ahlswede, 2006])

The $\mathcal{N}_{h,r,s}$-combination network has a scalar solution of field size q_s if and only if an $[r, h, d = r - s + 1]_{q_s}$ code exists.

$\Longrightarrow$ if $h = s$: MDS code needed: $q_s \geq r - 1$
(if $k \in \{3, q - 1\}$ & q_s power of 2: $q_s \geq r - 2$)
$\Longrightarrow$ decoding complexity: $\min\{\mathcal{O}(r \log^2 r), \mathcal{O}(h^{2.37})\}$ in $\mathbb{F}_{q_s}$

Vector Network Coding in the Combination Network

Construction

- $\mathcal{D}_t = \{\mathbf{C}_1, \mathbf{C}_2, \dots, \mathbf{C}_{q^t}\}$: *commutative* $\mathcal{MRD}[t \times t, t]_q$ *code defined by the powers of a companion matrix* $\mathbf{C}$
- *consider* $\mathcal{N}_{h,r,h}$*-combination network with* $r \leq q^t + 1$
- *messages* $\mathbf{x}_1, \dots, \mathbf{x}_h$

One node from the middle layer receives and transmits $\mathbf{y}_r = \mathbf{x}_h$ *and the other* $r-1$ *nodes of the middle layer receive and transmit* $\mathbf{y}_i = \begin{pmatrix} \mathbf{I}_t & \mathbf{C}_i & \mathbf{C}_i^2 & \dots & \mathbf{C}_i^{h-1} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{x}_1 & \mathbf{x}_2 & \dots & \mathbf{x}_h \end{pmatrix}^T \in \mathbb{F}_q^t$, $i = 1, \dots, r-1$.

Each receiver obtains

$$\begin{pmatrix} \mathbf{y}_{i_1} \\ \vdots \\ \mathbf{y}_{i_{k-1}} \\ \mathbf{y}_{i_k} \end{pmatrix} = \begin{pmatrix} \mathbf{I}_t & \mathbf{C}_{i_1} & \mathbf{C}_{i_1}^2 & \dots & \mathbf{C}_{i_1}^{k-1} \\ \mathbf{I}_t & \mathbf{C}_{i_2} & \mathbf{C}_{i_2}^2 & \dots & \mathbf{C}_{i_2}^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{I}_t & \mathbf{C}_{i_k} & \mathbf{C}_{i_k}^2 & \dots & \mathbf{C}_{i_k}^{k-1} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \vdots \\ \mathbf{x}_k \end{pmatrix}$$

Vector Network Coding in the Combination Network

Construction

- *$\mathcal{D}_t = \{\mathbf{C}_1, \mathbf{C}_2, \dots, \mathbf{C}_{q^t}\}$: commutative $\mathcal{MRD}[t \times t, t]_q$ code defined by the powers of a companion matrix $\mathbf{C}$*
- *consider $\mathcal{N}_{h,r,h}$-combination network with $r \leq q^t + 1$*
- *messages $\mathbf{x}_1, \dots, \mathbf{x}_h$*

One node from the middle layer receives and transmits $\mathbf{y}_r = \mathbf{x}_h$ and the other $r-1$ nodes of the middle layer receive and transmit $\mathbf{y}_i = \left(\mathbf{I}_t \ \mathbf{C}_i \ \mathbf{C}_i^2 \ \dots \ \mathbf{C}_i^{h-1}\right) \cdot \left(\mathbf{x}_1 \ \mathbf{x}_2 \ \dots \ \mathbf{x}_h\right)^T \in \mathbb{F}_q^t$, $i = 1, \dots, r-1$.

or

$$\begin{pmatrix} \mathbf{y}_{i_1} \\ \vdots \\ \mathbf{y}_{i_{k-1}} \\ \mathbf{y}_1 \end{pmatrix} = \begin{pmatrix} \mathbf{I}_t & \mathbf{C}_{i_1} & \mathbf{C}_{i_1}^2 & \dots & \mathbf{C}_{i_1}^{h-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{I}_t & \mathbf{C}_{i_{h-1}} & \mathbf{C}_{i_{h-1}}^2 & \dots & \mathbf{C}_{i_{h-1}}^{h-1} \\ \mathbf{0}_t & \mathbf{0}_t & \mathbf{0}_t & \dots & \mathbf{I}_t \end{pmatrix} \cdot \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \vdots \\ \mathbf{x}_k \end{pmatrix}$$

Vector Network Coding in the Combination Network

Construction

- $\mathcal{D}_t = \{\mathbf{C}_1, \mathbf{C}_2, \dots, \mathbf{C}_{q^t}\}$: *commutative* $\mathcal{MRD}[t \times t, t]_q$ *code defined by the powers of a companion matrix* $\mathbf{C}$
- *consider* $\mathcal{N}_{h,r,h}$*-combination network with* $r \leq q^t + 1$
- *messages* $\mathbf{x}_1, \dots, \mathbf{x}_h$

One node from the middle layer receives and transmits $\mathbf{y}_r = \mathbf{x}_h$ *and the other* $r-1$ *nodes of the middle layer receive and transmit* $\mathbf{y}_i = \left(\mathbf{I}_t \ \mathbf{C}_i \ \mathbf{C}_i^2 \ \dots \ \mathbf{C}_i^{h-1}\right) \cdot \left(\mathbf{x}_1 \ \mathbf{x}_2 \ \dots \ \mathbf{x}_h\right)^T \in \mathbb{F}_q^t$, $i = 1, \dots, r-1$.

or

$$\begin{pmatrix} \mathbf{y}_{i_1} \\ \vdots \\ \mathbf{y}_{i_{k-1}} \\ \mathbf{y}_1 \end{pmatrix} = \begin{pmatrix} \mathbf{I}_t & \mathbf{C}_{i_1} & \mathbf{C}_{i_1}^2 & \dots & \mathbf{C}_{i_1}^{h-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{I}_t & \mathbf{C}_{i_{h-1}} & \mathbf{C}_{i_{h-1}}^2 & \dots & \mathbf{C}_{i_{h-1}}^{h-1} \\ \mathbf{0}_t & \mathbf{0}_t & \mathbf{0}_t & \dots & \mathbf{I}_t \end{pmatrix} \cdot \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \vdots \\ \mathbf{x}_k \end{pmatrix}$$

$\Longrightarrow$ matrices have full rank (due to commutative MRD code)

$\Longrightarrow$ there is a unique solution for $(\mathbf{x}_1 \ \mathbf{x}_2 \ \dots \ \mathbf{x}_h)$

Vector Network Coding in the Combination Network

Theorem

For the $\mathcal{N}_{h,q^t+1,h}$-combination network, a vector linear solution of field size q and dimension t exists.
The decoding complexity is in $\mathcal{O}(t^2 h \log^2 h)$ over $\mathbb{F}_q$ for each receiver.

Comparison to scalar solution:

- equivalent field sizes (q^t)
- reduction of decoding complexity:
  for small h improvement from $h^{2.34}$ to quasi-linear in h

Remark: $k = 2$ was solved in [Sun *et al.*, ISIT-2015].

Vector Network Coding in the Combination Network

Theorem

For the $\mathcal{N}_{h,q^t+1,h}$-combination network, a vector linear solution of field size q and dimension t exists.
The decoding complexity is in $\mathcal{O}(t^2 h \log^2 h)$ over $\mathbb{F}_q$ for each receiver.

Comparison to scalar solution:

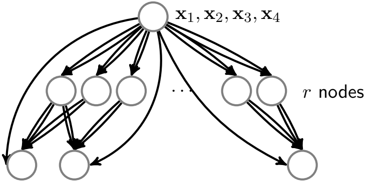
- equivalent field sizes (q^t)
- reduction of decoding complexity:
  for small h improvement from $h^{2.34}$ to quasi-linear in h

Remark: $k = 2$ was solved in [Sun *et al.*, ISIT-2015].

Outline

A Modified Combination Network

$\mathcal{N}^*_{4,r,4}$ network:



Three layers:

1. source with $h = 4$ messages
2. receive and forward linear combinations
3. $\binom{r}{2}$ receivers: connected to 2 middle nodes, request all 4 messages, extra link from source

Theorem (Scalar Solution)

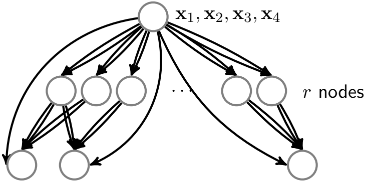
There is a scalar linear solution of field size q_s for the $\mathcal{N}^*_{4,r,4}$-network if and only if $(q_s^2+1)(q_s^2+q_s+1) \geq r$.

Proof: next slide.

$\implies q_s \in \mathcal{O}(r^{1/4})$

A Modified Combination Network

$\mathcal{N}^*_{4,r,4}$ network:



Three layers:

1. source with $h = 4$ messages
2. receive and forward linear combinations
3. $\binom{r}{2}$ receivers: connected to 2 middle nodes, request all 4 messages, extra link from source

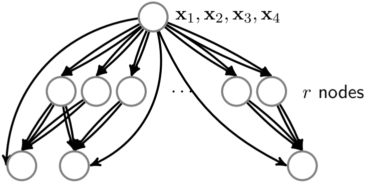
Theorem (Scalar Solution)

There is a scalar linear solution of field size q_s for the $\mathcal{N}^*_{4,r,4}$-network if and only if $(q_s^2 + 1)(q_s^2 + q_s + 1) \geq r$.

Proof: next slide.

$\implies q_s \in \mathcal{O}(r^{1/4})$

A Modified Combination Network—Scalar Solution



Theorem (Scalar Solution)

There is a scalar linear solution of field size q_s for the $\mathcal{N}^*_{4,r,4}$-network if and only if $(q_s^2+1)(q_s^2+q_s+1) \geq r$.

Proof idea:

- $\mathbf{B}$ is $4 \times 2r$-matrix divided into r blocks of two columns s.t. any two blocks together have rank at least three
- transmit symbols of one block of $(x_1, x_2, x_3, x_4) \cdot \mathbf{B}$ at each middle node
- extra links: transmit symbol p_i s.t. full rank at receiver
- blocks: 4×2-matrix representations of all 2-dimensional subspaces of $\mathbb{F}_{q_s}^4$
  $\Longrightarrow r \leq \begin{bmatrix}4\\2\end{bmatrix}_{q_s} = (q_s^2+1)(q_s^2+q_s+1) \in \mathcal{O}(q_s^4)$
- “only if” can be shown since there is no scheme that provides more blocks $\square$

$\Longrightarrow q_s \in \mathcal{O}(r^{1/4})$

Vector Network Coding

Construction

Let $\mathcal{C} = \{\mathbf{C}_1, \mathbf{C}_2, \dots, \mathbf{C}_{q^{2t^2+2t}}\}$ *be an* $\mathcal{MRD}[2t \times 2t, t]_q$ *code and let* $r \leq q^{2t^2+2t}$*. Consider the* $\mathcal{N}^*_{4,r,4}$*-network with message vectors* $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4 \in \mathbb{F}_q^t$*. The* i*-th middle node receives and transmits:*

$$\begin{pmatrix} \mathbf{y}_{i_1} \\ \mathbf{y}_{i_2} \end{pmatrix} = \begin{pmatrix} \mathbf{I}_{2t} & \mathbf{C}_i \end{pmatrix} \cdot \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \mathbf{x}_3 \\ \mathbf{x}_4 \end{pmatrix} \in \mathbb{F}_q^{2t}, \quad i = 1, \dots, r.$$

The extra link from the source which ends in the same receiver as the links from two distinct nodes $i, j \in \{1, 2, \dots, r\}$ *of the middle layer transmits the vector* $\mathbf{z}_{ij} = \mathbf{P}_{ij} \cdot \left(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4\right)^T \in \mathbb{F}_q^t$*, where the* $t \times 4t$ *matrix* $\mathbf{P}_{ij}$ *is chosen such that*

$$\mathrm{rk} \begin{pmatrix} \mathbf{I}_{2t} & \mathbf{C}_i \\ \mathbf{I}_{2t} & \mathbf{C}_j \\ \multicolumn{2}{c}{\mathbf{P}_{ij}} \end{pmatrix} = 4t.$$

Vector Network Coding

Theorem

Our construction provides a vector solution of field size q and dimension t to the $\mathcal{N}^*_{4,r,4}$-network for $r \leq q^{2t(t+1)}$.

Proof: On each receiver, we obtain

$$\begin{pmatrix} \mathbf{y}_{i_1} \\ \mathbf{y}_{i_2} \\ \mathbf{y}_{j_1} \\ \mathbf{y}_{j_2} \\ \mathbf{z}_{ij} \end{pmatrix} = \begin{pmatrix} \mathbf{I}_{2t} & \mathbf{C}_i \\ \mathbf{I}_{2t} & \mathbf{C}_j \\ \multicolumn{2}{c}{\mathbf{P}_{ij}} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \mathbf{x}_3 \\ \mathbf{x}_4 \end{pmatrix}.$$

Since $\operatorname{rk}\begin{pmatrix} \mathbf{I}_{2t} & \mathbf{C}_i \\ \mathbf{I}_{2t} & \mathbf{C}_j \end{pmatrix} \geq 3t$, $\mathbf{P}_{ij}$ can be chosen such that overall rank is $4t$.

$\implies$ unique solution for $(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4)$ □

Comparison to scalar solution: $q_s \in \mathcal{O}(q^{t^2/2})$ vs. q^t

$\implies$ significant reduction of field size!

Vector Network Coding

Theorem

Our construction provides a vector solution of field size q and dimension t to the $\mathcal{N}^*_{4,r,4}$-network for $r \leq q^{2t(t+1)}$.

Proof: On each receiver, we obtain

$$\begin{pmatrix} \mathbf{y}_{i_1} \\ \mathbf{y}_{i_2} \\ \mathbf{y}_{j_1} \\ \mathbf{y}_{j_2} \\ \mathbf{z}_{ij} \end{pmatrix} = \begin{pmatrix} \mathbf{I}_{2t} & \mathbf{C}_i \\ \mathbf{I}_{2t} & \mathbf{C}_j \\ \multicolumn{2}{c}{\mathbf{P}_{ij}} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \mathbf{x}_3 \\ \mathbf{x}_4 \end{pmatrix}.$$

Since $\mathrm{rk} \begin{pmatrix} \mathbf{I}_{2t} & \mathbf{C}_i \\ \mathbf{I}_{2t} & \mathbf{C}_j \end{pmatrix} \geq 3t$, $\mathbf{P}_{ij}$ can be chosen such that overall rank is $4t$.

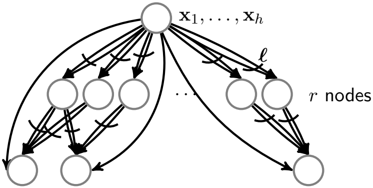
$\Longrightarrow$ unique solution for $(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4)$ $\square$

Comparison to scalar solution: $q_s \in \mathcal{O}(q^{t^2/2})$ vs. q^t

$\Longrightarrow$ significant reduction of field size!

Generalization

$\mathcal{N}^*_{h,r,h}$-combination network
with ℓ parallel edges ($h = 2\ell$)



Three layers:

1. source with $h = 2\ell$ ($\ell \geq 2$) messages
2. receive and forward linear combinations, ℓ parallel edges
3. $\binom{r}{2}$ receivers: connected to ℓ middle nodes, request all h messages, gets $2\ell + 1$ links

Solutions

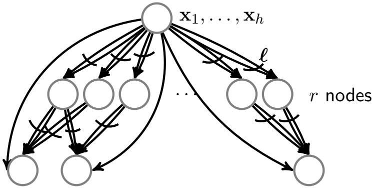
- scalar solution exists if and only if $r \leq \mathcal{O}(q_s^{2\ell})$
- vector solution: use $\mathcal{MRD}[\ell t \times \ell t, (\ell - 1)t]_q$ of size $q^{\ell t^2 + \ell t}$

Comparison: $q_s \in \mathcal{O}(q^{t^2/2})$ vs. q^t (for any $k = 2\ell$, $\ell \geq 2$)

$\Longrightarrow$ significant reduction of field size!

Generalization

$\mathcal{N}^*_{h,r,h}$-combination network
with ℓ parallel edges ($h = 2\ell$)



Three layers:

1. source with $h = 2\ell$ ($\ell \geq 2$) messages
2. receive and forward linear combinations, ℓ parallel edges
3. $\binom{r}{2}$ receivers: connected to ℓ middle nodes, request all h messages, gets $2\ell + 1$ links

Solutions

- scalar solution exists if and only if $r \leq \mathcal{O}(q_s^{2\ell})$
- vector solution: use $\mathcal{MRD}[\ell t \times \ell t, (\ell - 1)t]_q$ of size $q^{\ell t^2 + \ell t}$

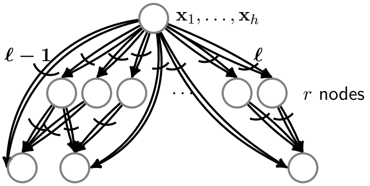
Comparison: $q_s \in \mathcal{O}(q^{t^2/2})$ vs. q^t (for any $k = 2\ell$, $\ell \geq 2$)

$\Longrightarrow$ significant reduction of field size!

Outline

Another Modified Combination Network

$\mathcal{N}^+_{h,r,h}$-combination network with ℓ parallel edges ($h = 2\ell$) and $\ell - 1$ direct links



Three layers:

1. source with $h = 2\ell$ ($\ell \geq 2$) messages
2. receive and forward linear combinations, ℓ parallel edges
3. $\binom{r}{2}$ receivers: connected to ℓ middle nodes, request all h messages, gets $3\ell - 1$ links

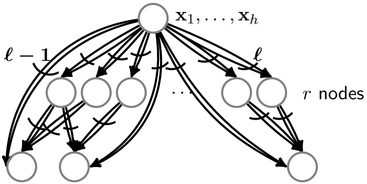
Lemma (Scalar Solution)

There is a scalar solution of field size q_s for the $\mathcal{N}^+_{h,r,h}$-network with $h = 2\ell$ messages, where $\ell \geq 2$, if and only if $q_s^{\ell^2} \geq r$.

$\implies q_s \in \mathcal{O}(r^{1/\ell^2})$

Another Modified Combination Network

$\mathcal{N}^{+}_{h,r,h}$-combination network with ℓ parallel edges ($h = 2\ell$) and $\ell - 1$ direct links



Three layers:

1. source with $h = 2\ell$ ($\ell \geq 2$) messages
2. receive and forward linear combinations, ℓ parallel edges
3. $\binom{r}{2}$ receivers: connected to ℓ middle nodes, request all h messages, gets $3\ell - 1$ links

Lemma (Scalar Solution)

There is a scalar solution of field size q_s for the $\mathcal{N}^{+}_{h,r,h}$-network with $h = 2\ell$ messages, where $\ell \geq 2$, if and only if $q_s^{\ell^2} \geq r$.

$\implies q_s \in \mathcal{O}(r^{1/\ell^2})$

Vector Network Coding

Construction

$\{\mathbf{C}_1, \dots, \mathbf{C}_{q^{\ell(\ell-1)t^2+\ell t}}\}$ is $\mathcal{MRD}[\ell t \times \ell t, t]_q$ code and $r \leq q^{\ell(\ell-1)t^2+\ell t}$. Consider the $\mathcal{N}^+_{h,r,h}$-network with messages $\mathbf{x}_1, \dots, \mathbf{x}_h \in \mathbb{F}_q^t$, where $h = 2\ell$, $\ell \geq 2$. The i-th middle node receives and transmits:

$$\begin{pmatrix} \mathbf{y}_{i_1} \\ \mathbf{y}_{i_2} \end{pmatrix} = \begin{pmatrix} \mathbf{I}_{\ell t} & \mathbf{C}_i \end{pmatrix} \cdot \begin{pmatrix} \mathbf{x}_1 \\ \vdots \\ \mathbf{x}_{2\ell} \end{pmatrix} \in \mathbb{F}_q^{\ell t}, \quad i = 1, \dots, r.$$

The $\ell - 1$ direct links from the source transmit the vectors $\mathbf{z}_{ijs} = \mathbf{P}_{ijs} \cdot \left(\mathbf{x}_1, \dots, \mathbf{x}_{2\ell}\right)^T \in \mathbb{F}_q^t$, for $s = 1, \dots, \ell - 1$, where the $t \times 2\ell t$ matrices $\mathbf{P}_{ijs}$ are chosen s.t.

$$\mathrm{rk} \begin{pmatrix} \mathbf{I}_{\ell t} & \mathbf{C}_i \\ \mathbf{I}_{\ell t} & \mathbf{C}_j \\ \multicolumn{2}{c}{\mathbf{P}_{ij1}} \\ \multicolumn{2}{c}{\vdots} \\ \multicolumn{2}{c}{\mathbf{P}_{ij(\ell-1)}} \end{pmatrix} = 2\ell t.$$

Vector Network Coding

Theorem

Our construction provides a vector solution of field size q and dimension t to the $\mathcal{N}^{+}_{h,r,h}$-network for $r \leq q^{\ell(\ell-1)t^2+\ell t}$, where $h = 2\ell$ and $\ell \geq 2$.

Proof:

Since $\operatorname{rk}\begin{pmatrix} \mathbf{I}_{\ell t} & \mathbf{C}_i \\ \mathbf{I}_{\ell t} & \mathbf{C}_j \end{pmatrix} \geq \ell t + t = (\ell+1)t$, the $(\ell-1)t$ rows of the matrices $\mathbf{P}_{ijs}$ can be chosen such that the overall rank $2\ell t$.

$\Longrightarrow$ unique solution for $(\mathbf{x}_1, \ldots, \mathbf{x}_{2\ell})$ $\square$

Comparison to scalar solution:

$q_s \in \mathcal{O}(r^{1/\ell^2}) = \mathcal{O}(q^{\left(1-\frac{1}{\ell}\right)t^2})$ vs. q^t

$\Longrightarrow$ significant reduction of field size!

Vector Network Coding

Theorem

Our construction provides a vector solution of field size q and dimension t to the $\mathcal{N}^{+}_{h,r,h}$-network for $r \leq q^{\ell(\ell-1)t^2+\ell t}$, where $h = 2\ell$ and $\ell \geq 2$.

Proof:
Since $\operatorname{rk}\begin{pmatrix} \mathbf{I}_{\ell t} & \mathbf{C}_i \\ \mathbf{I}_{\ell t} & \mathbf{C}_j \end{pmatrix} \geq \ell t + t = (\ell+1)t$, the $(\ell-1)t$ rows of the matrices $\mathbf{P}_{ijs}$ can be chosen such that the overall rank $2\ell t$.
$\Longrightarrow$ unique solution for $(\mathbf{x}_1, \ldots, \mathbf{x}_{2\ell})$ $\square$

Comparison to scalar solution:
$q_s \in \mathcal{O}(r^{1/\ell^2}) = \mathcal{O}(q^{\left(1-\frac{1}{\ell}\right)t^2})$ vs. q^t

$\Longrightarrow$ significant reduction of field size!

Outline

Vector Network Coding

Contributions:

- Use MRD matrices as vector network coding coefficients
  $\Longrightarrow$ reduce decoding complexity
  $\Longrightarrow$ large gap in field size of scalar & vector coding:
  $$q^{\left(1-\frac{1}{\ell}\right)t^2} - q^t \text{ for any } \ell \geq 2$$
- Slight improvement by using other subspace codes
- For $h = 3$: gap of smaller size for some parameters

Open Questions:

- Networks with $h = 2, 3$ and large gap?
- Largest possible gap?
- Network with h edge disjoint paths and large gap?
- Gap between non-linear and linear network coding?

Vector Network Coding

Contributions:

- Use MRD matrices as vector network coding coefficients
  $\Longrightarrow$ reduce decoding complexity
  $\Longrightarrow$ large gap in field size of scalar & vector coding:
  $$q^{\left(1-\frac{1}{\ell}\right)t^2} - q^t \text{ for any } \ell \geq 2$$
- Slight improvement by using other subspace codes
- For $h = 3$: gap of smaller size for some parameters

Open Questions:

- Networks with $h = 2, 3$ and large gap?
- Largest possible gap?
- Network with h edge disjoint paths and large gap?
- Gap between non-linear and linear network coding?

...for your attention!

Questions?