Vector versus Scalar Linear Codes for Multicast Network Coding

Qifu (Tyler) Sun

(Joint work with Xiaolong Yang, Keping Long and Zongpeng Li)

Feb, 2015 @ INC, CUHK

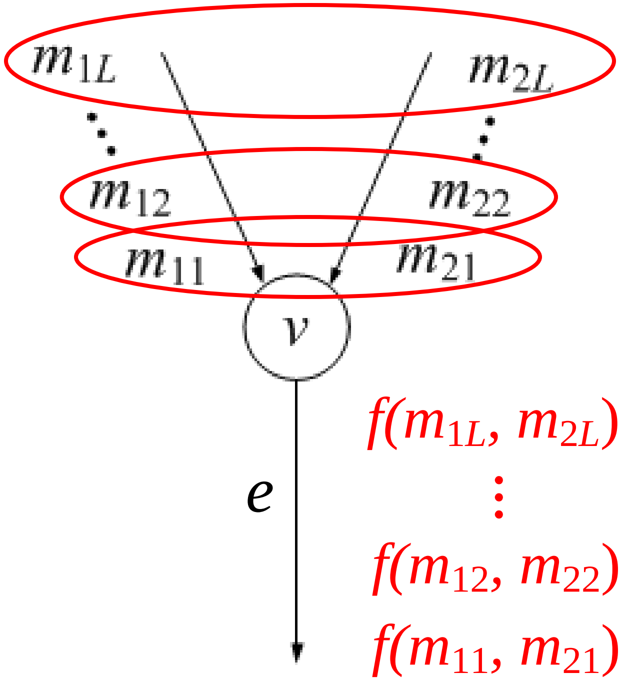
北京科技大学 University of Science and Technology Beijing

INC

UNIVERSITY OF CALGARY

Scalar versus Vector Linear NC (LNC): a Recap

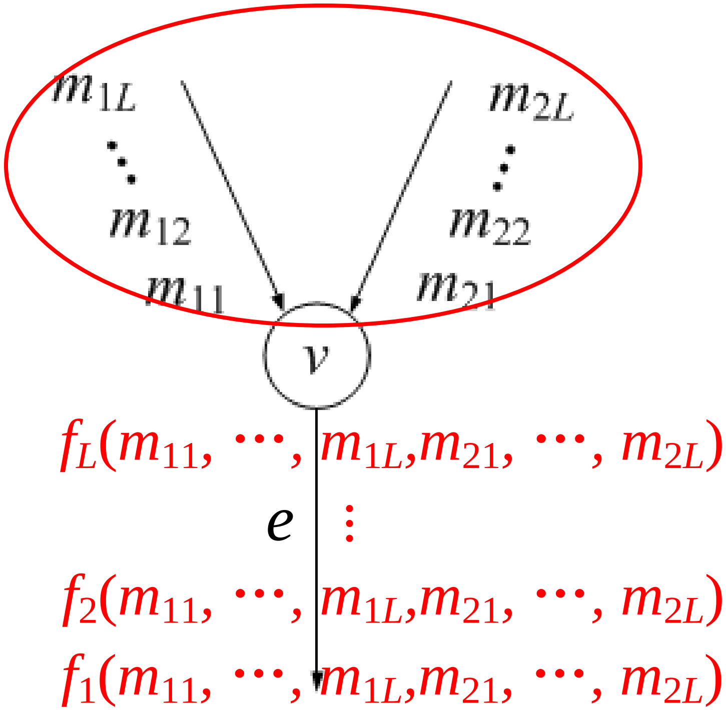
- Every edge transmits a sequence of L data symbols over GF(q).



- For **scalar** coding: the L data symbols transmitted on $e \in \text{Out}(v)$ are sequentially determined by a *single* linear function f over GF(q).

Scalar versus Vector LNC: a Recap

- Every edge transmits a sequence of L data symbols over GF(q).



- For **scalar** coding: the L data symbols transmitted on $e \in \text{Out}(v)$ are sequentially determined by a *single* linear function f over GF(q).

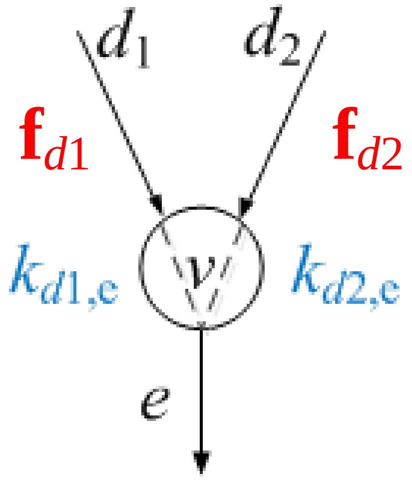
- For **vector (block)** coding: the L data symbols transmitted on $e \in \text{Out}(v)$ are determined by L *different* linear functions f_l over GF(q).

Scalar versus Vector LNC: a Recap

- Scalar coding:
  - Local encoding kernel: $k_{d,e} \in \mathrm{GF}(q)$
  - Global encoding kernel: $\mathbf{f}_e \in \mathrm{GF}(q)^{\omega}$

$$\mathbf{f}_e = \sum_{d \in In(v)} k_{d,e} \mathbf{f}_d$$

$$m_e = \mathbf{m}_S \mathbf{f}_e \in \mathrm{GF}(q)$$



$$\mathbf{f}_e = k_{d1,\mathrm{e}} \mathbf{f}_{d1} + k_{d2,\mathrm{e}} \mathbf{f}_{d2}$$

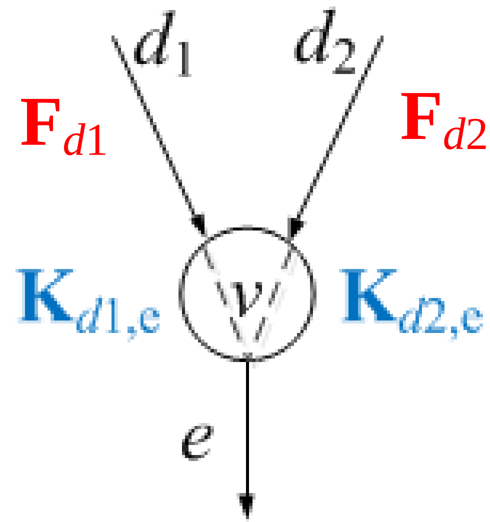
Scalar versus Vector LNC: a Recap

- Scalar coding:
  - Local encoding kernel: $k_{d,e} \in \mathrm{GF}(q)$
  - Global encoding kernel: $\mathbf{f}_e \in \mathrm{GF}(q)^{\omega}$

$$\mathbf{f}_e = \sum_{d \in In(v)} k_{d,e} \mathbf{f}_d$$

$$m_e = \mathbf{m}_S \mathbf{f}_e \in \mathrm{GF}(q)$$

- Vector coding:
  - Local encoding kernel: $\mathbf{K}_{d,e} \in \mathrm{GF}(q)^{L \times L}$
  - Global encoding kernel: $\mathbf{F}_e \in \mathrm{GF}(q)^{\omega L \times L}$



$$\mathbf{F}_e = \mathbf{F}_{d1}\mathbf{K}_{d1,e} + \mathbf{F}_{d2}\mathbf{K}_{d2,e}$$

$$\mathbf{F}_e = \sum_{d \in In(v)} \mathbf{F}_d \mathbf{K}_{d,e}$$

$\mathbf{m}_e = \mathbf{m}_S \mathbf{F}_e$ // L-dim row vector over $\mathrm{GF}(q)$

Scalar versus Vector LNC: a Recap

- Assume the alphabet size of data units = q^L:

	Scalar LNC	Vector LNC
Data unit alphabet	Base field GF(q^L)	Vector space GF(q)^L
Local encoding kernel	Element in GF(q^L)	$L \times L$ matrix over GF(q)
# of candidates for local encoding kernels	q^L	q^{L^2}

Vector LNC *exponentially* enriches the choices of coding operations at intermediate nodes!

Scalar versus Vector LNC: a Recap

- Scalar LNC can be regarded as a special case of vector LNC from two facets:
  - Straightforwardly,
    a scalar linear code over GF(q^L)
    → a vector linear code of dimension 1 over GF(q^L)
  - In a stronger sense,
    a scalar linear code over GF(q^L)
    → a vector linear code of dimension L over GF(q)
    (a vector linear code over GF(q)^L for short)

// By the standard matrix representation of finite field GF(q^L)

Matrix Representation of GF(q^L)

- Let **C** be the $L \times L$ *companion matrix* of a primitive polynomial $p(x)$ of degree L over GF(q).

e.g. $p(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$ $\qquad$ $\mathbf{C} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$

The *characteristic polynomial* of **C**

$$\det(\mathbf{I}x - \mathbf{C}) = p(x).$$

Thus, according to the Caylay-Hamilton theorem,

$$p(\mathbf{C}) = \mathbf{0}.$$

GF(q^L) can be represented by $\{\mathbf{0}, \mathbf{C}, \mathbf{C}^2, \ldots, \mathbf{C}^{q^L-1} (= \mathbf{I})\}$ with the arithmetic among matrices.

Every scalar code over GF(q^L) can be transformed into a vector code over GF(q)^L

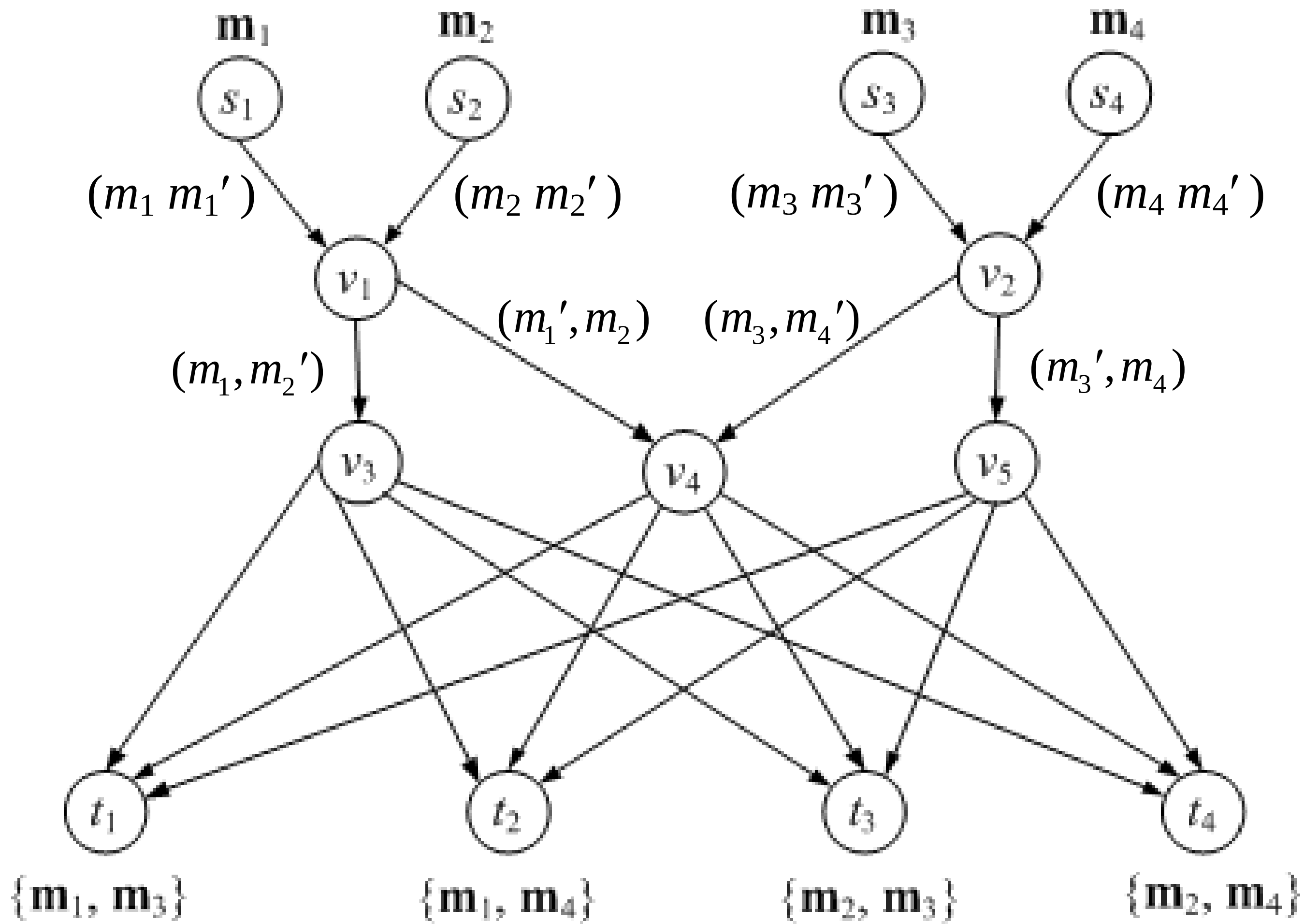
- Let **C** be the $L \times L$ *companion matrix* of a primitive polynomial $p(x)$ of degree L over GF(q).

  GF(q^L) can be represented by $\{\mathbf{0}, \mathbf{C}, \mathbf{C}^2, \ldots, \mathbf{C}^{q^L-1} (= \mathbf{I})\}$ with the arithmetic among matrices.

- Given a (not necessarily multicast) network, a scalar linear code ($k_{d,e}$) over GF(q^L) is a solution *iff* the corresponding vector linear code ($\Phi(k_{d,e})$) over GF(q)^L is a solution.

Benefits of vector LNC

A classical example without a scalar linear solution over any GF(q) has a simple vector linear solution over GF$(2)^2$ [Médard et.al. 2003].



Benefits of vector LNC on multicast networks

On a (single-source) multicast network, scalar LNC is sufficient to yield a solution when GF(q) is large enough.

Vector LNC still has the following benefits:

- Vector LNC can set base field = GF(2) in advance, and then merely increase L to yield a solution.
- Low-complexity vector LNC schemes only involving permutation and addition are proposed [JaggiCassutoEffros'06].
- Under the same alphabet size, random vector LNC potentially has better performance in terms of higher probability to yield a solution [Ho et.al'06].

Benefits of vector LNC on multicast networks

More benefits of vector LNC [EbrahimiFragouli'11],

- Vector LNC is more flexible to update upon network variations

  $GF(q)^L \rightarrow GF(q)^{L+1}$ is easy, $GF(q^L) \rightarrow GF(q^{L+1})$ not.

- Vector linear solutions over $GF(q)^{L_1}$ and over $GF(q)^{L_2}$ can naturally induce a vector linear solution over $GF(q)^{L_1+L_2}$.

  (Conjecture) Scalar linear solvability over both $GF(q^{L_1})$ and $GF(q^{L_2})$ does *not* necessarily imply scalar linear solvability over $GF(q^{L_1+L_2})$.

- **(Conjecture)** There is a multicast network that has a vector linear solution over $GF(q)^L$ but no scalar linear solution over $GF(q')$ for any $q' \leq q^L$.

Benefits of vector LNC on multicast networks

Since vector coding *exponentially* enriches the choices of NC operations, it would be a folklore for these two conjectured benefits to be correct.

- Vector linear solutions over $\mathrm{GF}(q)^{L_1}$ and over $\mathrm{GF}(q)^{L_2}$ can naturally induce a vector linear solution over $\mathrm{GF}(q)^{L_1+L_2}$.

  (Conjecture) Scalar linear solvability over both $\mathrm{GF}(q^{L_1})$ and $\mathrm{GF}(q^{L_2})$ does *not* necessarily imply scalar linear solvability over $\mathrm{GF}(q^{L_1+L_2})$.

- **(Conjecture)** There is a multicast network that has a vector linear solution over $\mathrm{GF}(q)^L$ but no scalar linear solution over $\mathrm{GF}(q')$ for any $q' \leq q^L$.

Benefits of vector LNC on multicast networks

- [EbrahimiFragouli'11] partially proved them under their algebraic framework in terms of multivariate determinant polynomials of transfer functions.
- No multicast network has ever been found yet!

- Vector linear solutions over $\mathrm{GF}(q)^{L_1}$ and over $\mathrm{GF}(q)^{L_2}$ can naturally induce a vector linear solution over $\mathrm{GF}(q)^{L_1+L_2}$.

(Conjecture) Scalar linear solvability over both $\mathrm{GF}(q^{L_1})$ and $\mathrm{GF}(q^{L_2})$ does *not* necessarily imply scalar linear solvability over $\mathrm{GF}(q^{L_1+L_2})$.

- **(Conjecture)** There is a multicast network that has a vector linear solution over $\mathrm{GF}(q)^L$ but no scalar linear solution over $\mathrm{GF}(q')$ for any $q' \leq q^L$.

Highlight of the remaining talk

- We demonstrate explicit networks to verify Conjecture 1.
- Propose a general method to construct multicast networks that verify Conjecture 2.
- We also show examples where scalar code outperforms vector one in terms of alphabet size to yield a solution.

- Vector linear solutions over $GF(q)^{L_1}$ and over $GF(q)^{L_2}$ can naturally induce a vector linear solution over $GF(q)^{L_1+L_2}$.

(Conjecture 1) Scalar linear solvability over both $GF(q^{L_1})$ and $GF(q^{L_2})$ does *not* necessarily imply scalar linear solvability over $GF(q^{L_1+L_2})$.

- **(Conjecture 2)** There is a multicast network that has a vector linear solution over $GF(q)^L$ but no scalar linear solution over $GF(q')$ for any $q' \leq q^L$.

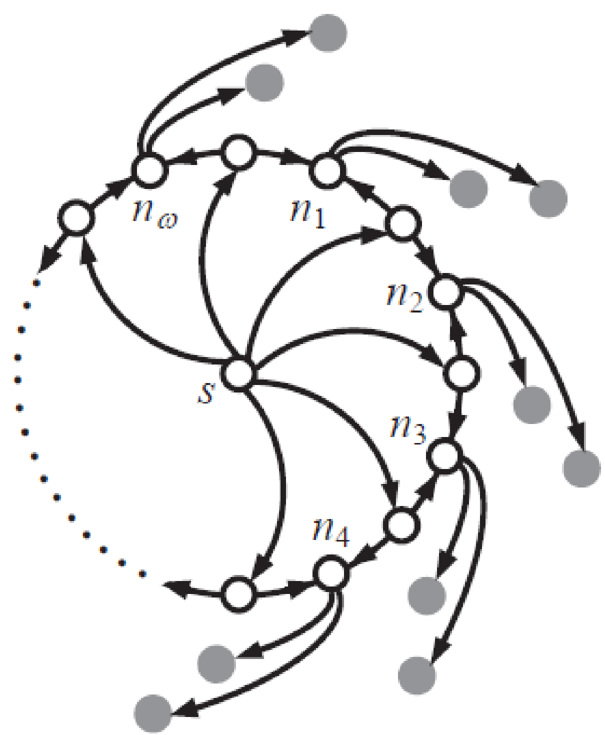
Verification of Conjecture 1

Theorem. There exists a multicast network scalar linearly solvable over GF(q^{L_1}), GF(q^{L_2}), …, GF(q^{L_m}) but *not* over GF($q^{L_1+L_2+\ldots+L_m}$).

Motivation. The first few multicast networks scalar linearly solvable over GF(q) but not over GF(q') with some $q' > q$.

The Swirl network with $\omega \geq 3$ [Sun et.al'2014]

- It can have an arbitrary source dimension $\omega \geq 3$.
- For every ω grey nodes with full maxflow ω from s, there is a receiver connected from them.



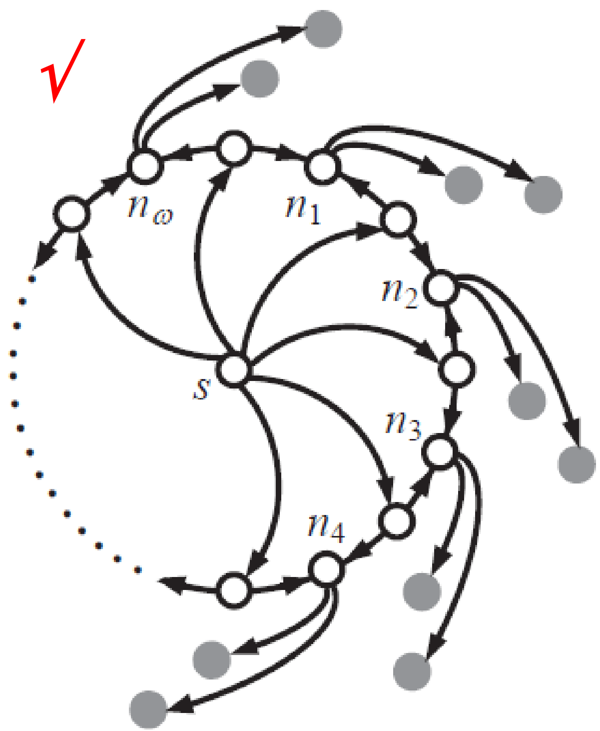
The Swirl network with (large enough) ω

Proposition. $q_{min} = 5$. The Swirl network is scalar linearly solvable over all GF(2^p) except for the case that $2^p - 1$ is prime.

Key reason: It is linearly solvable over GF(q) iff

$\exists$ a proper subgroup $G \subset GF(q)^\times$ s.t. $|G| \geq 2$.

$G = \{1, 4\} \subset GF(5)^\times$ √



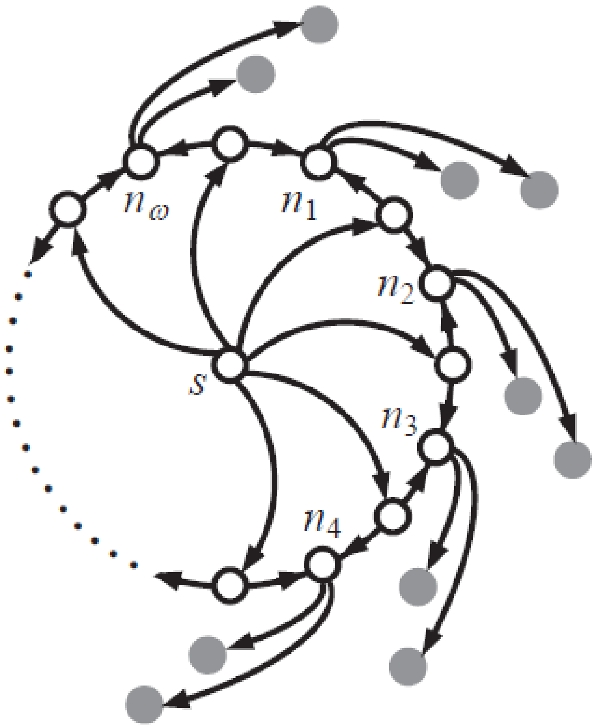
When $2^p - 1$ is prime

$\{1\} = GF(2^p)^\times$ ✗

Verification of Conjecture 1

Proposition. q_{min} = 5. The Swirl network is scalar linearly solvable over all GF(2^p) except for the case that $2^p - 1$ is prime.

Idea: To test whether there exist L_1, L_2 such that $2^{L_1} - 1$ and $2^{L_2} - 1$ are ***composite*** while $2^{L_1+L_2} - 1$ is ***prime***.



Mersenne numbers

- Mersenne numbers: $2^n - 1$
- Mersenne primes: $2^p - 1$

#	*p*	$2^p - 1$
1	2	3
2	3	7
3	5	31
4	7	127
5	13	8191
6	17	131071

Done!

$= (2^4 \cdot 2^9 - 1)$

Goal: find p s.t. $p = m + n$, $2^m - 1$ and $2^n - 1$ are composite numbers.

Mersenne numbers

- Mersenne numbers: $2^n - 1$
- Mersenne primes: $2^p - 1$

#	*p*	$2^p - 1$
1	2	3
2	3	7
3	5	31
4	7	127
5	13	8191
6	17	131071

Done!

$= (2^4 \cdot 2^9 - 1)$

- The Swirl network (with ω large enough) is scalar linearly solvable over $GF(2^4)$ and $GF(2^9)$ but not over $GF(2^{13})$.

Mersenne numbers

- Mersenne numbers: $2^n - 1$
- Mersenne primes: $2^p - 1$

#	*p*	$2^p - 1$
1	2	3
2	3	7
3	5	31
4	7	127
5	13	8191
6	17	131071

Done!

$= (2^4 \cdot 2^9 - 1)$

$= (2^4 \cdot 2^4 \cdot 2^9 - 1)$

$= (2^8 \cdot 2^9 - 1)$

For the n^{th} (≥ 5) Mersenne prime $2^p - 1$, we can write $p = L_1 + \ldots + L_m$ ($2 \leq m \leq n-3$) s.t. $2^{L_j} - 1$ is a composite.

Verification of Conjecture 1

- **Proposition**. The Swirl network (with ω large enough) is scalar linearly solvable over $GF(2^{L_1})$, $GF(2^{L_2})$, …, $GF(2^{L_m})$ for some $L_1, \ldots, L_m$, but *not* over $GF(2^{L_1+L_2+\ldots+L_m})$.

- **Corollary**. There exists a multicast network scalar linearly solvable over $GF(q^{L_1})$, $GF(q^{L_2})$, …, $GF(q^{L_m})$ but *not* over $GF(q^{L_1+L_2+\ldots+L_m})$. When there are infinitely many Mersenne primes, m can tend to infinity.

- **Remark**. Our approach only verifies the Conjecture for the *even* characteristic case. The case that q is odd is still open.

Vector linear solvability of Swirl network

- **Proposition**. The Swirl network (with ω large enough) is scalar linearly solvable over GF(2^{L_1}), GF(2^{L_2}), …, GF(2^{L_m}) for some L_1, …, L_m, but *not* over GF($2^{L_1+L_2+\ldots+L_m}$).

A scalar linear solution ($k_{d,e,j}$) over GF(2^{L_j})

$$\Downarrow \quad \mathbf{K}_{d,e,j} = \Phi(k_{d,e,j})$$

A vector linear solution ($\mathbf{K}_{d,e,j}$) over GF$(2)^{L_j}$

$$\Downarrow \quad \mathbf{K}_{d,e} = \begin{bmatrix} \Phi(k_{d,e,1}) & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \Phi(k_{d,e,2}) & \cdots & \cdots \\ \cdots & \cdots & \ddots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \Phi(k_{d,e,m}) \end{bmatrix}$$

A vector linear solution ($\mathbf{K}_{d,e,j}$) over GF$(2)^{L_1+L_2+\ldots+L_m}$

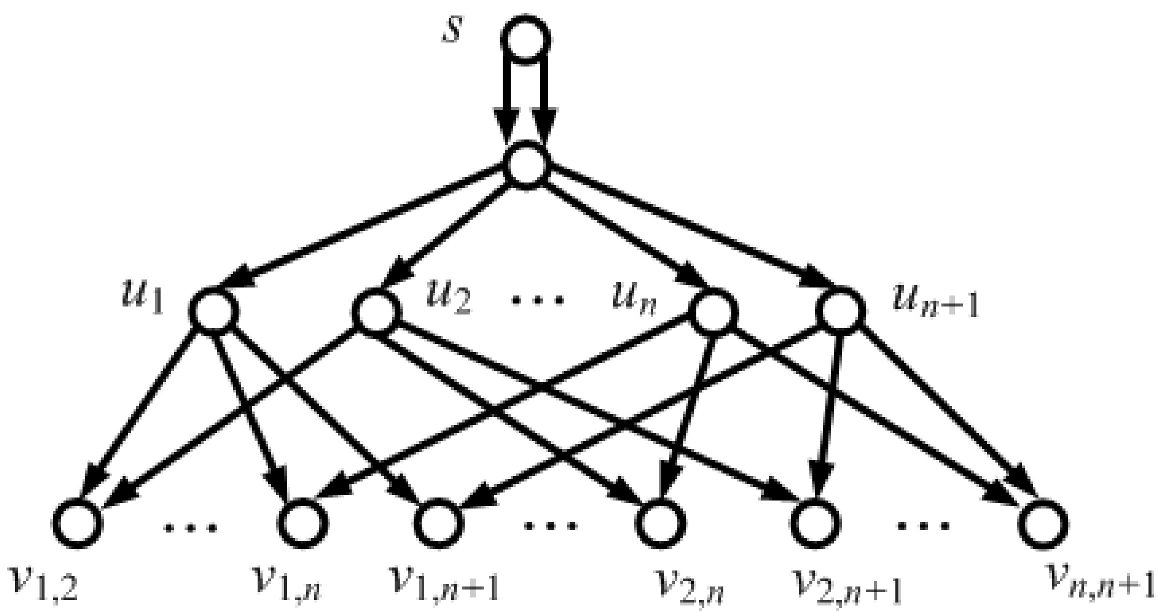
Vector linear solvability of Swirl network

- **Proposition**. When $L \geq 5$ and $2^L - 1$ is a prime, the Swirl network (with ω large enough) is vector linearly solvable over $GF(2)^L$, but not scalar linearly solvable over $GF(2^L)$.

- However, the Swirl network is scalar linearly solvable over GF(5). Still one step away to verify Conjecture 2.

- Provide a general method to construct a multicast network with a vector linear solution over $GF(q)^L$ but without a scalar linear solution over any $GF(q')$ with $q' \leq q^L$.

(n+1, 2)-Combination Network

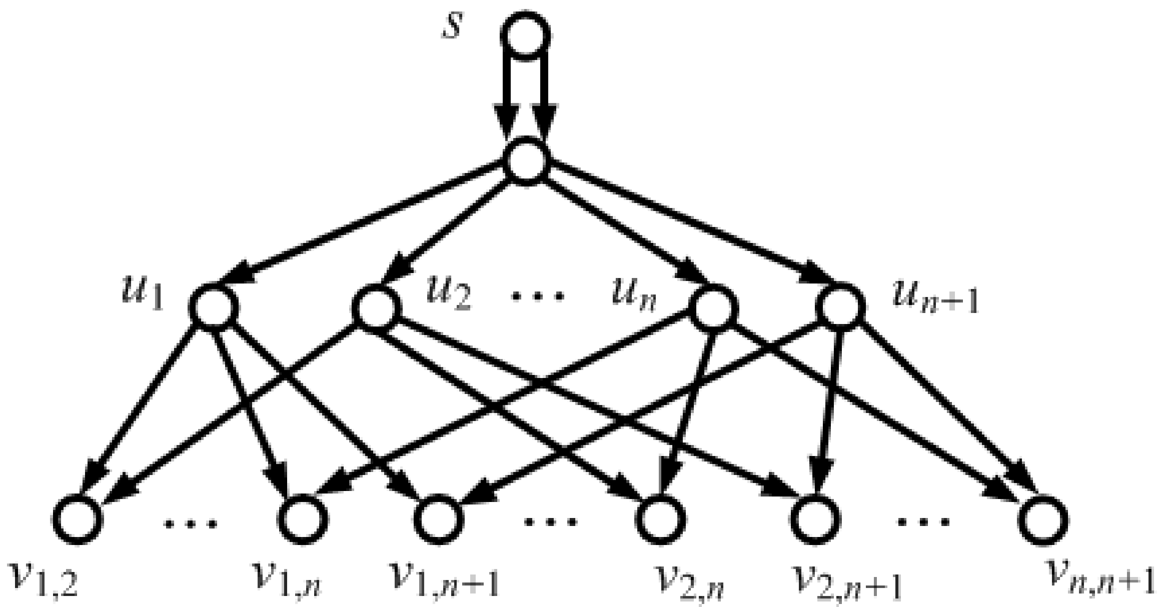


- ∃ a *scalar* linear solution over GF(q^L)

$$iff \begin{bmatrix} 1 & 0 & 1 & \dots & 1 \\ 0 & 1 & a_1 & \dots & a_{n-1} \end{bmatrix} \quad \begin{matrix} a_i \in \mathrm{GF}(q^L)\backslash\{0\} \\ a_i \neq a_j \end{matrix}$$

iff $q^L \geq n$.

(n+1, 2)-Combination Network



- ∃ a *vector* linear solution over $GF(q)^L$

iff $\begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{I} & \ldots & \mathbf{I} \\ \mathbf{0} & \mathbf{I} & \mathbf{A}_1 & \ldots & \mathbf{A}_{n-1} \end{bmatrix}$

$\mathbf{A}_i$: $L \times L$ invertible matrix over GF(q)

$rank(\mathbf{A}_i - \mathbf{A}_j) = L$

Rank-metric codes

- $\{\mathbf{0}, \mathbf{A}_1, \ldots, \mathbf{A}_{n-1}\}$ forms an $L \times L$ *rank-metric code* of distance L over GF(q). // $d(\mathbf{A}_i, \mathbf{A}_j) = rank(\mathbf{A}_i - \mathbf{A}_j)$

- Singleton-bound for an $L \times L$ rank-metric code $\mathcal{C}$ over GF(q) with minimum distance d:

$$|\, \mathcal{C} \,| \leq q^{L(L-d+1)}$$

- $|\{\mathbf{0}, \mathbf{A}_1, \ldots, \mathbf{A}_{n-1}\}| \leq q^L$ // Maximum Rank Distance code

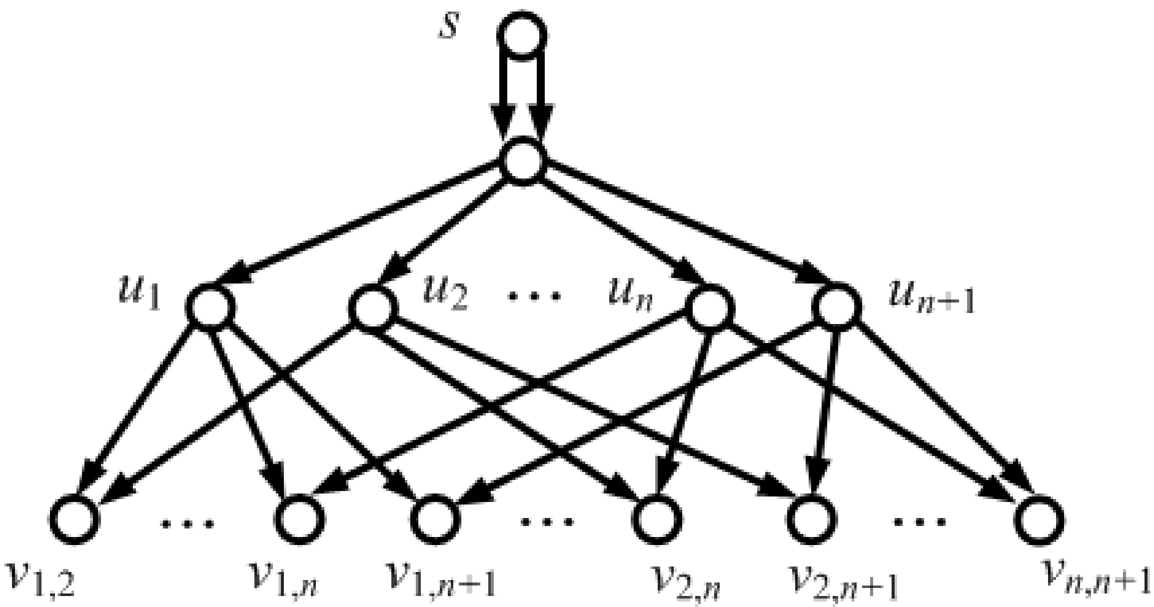
- $\exists$ a *vector* linear solution over GF(q)^L

$$iff \begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{I} & \ldots & \mathbf{I} \\ \mathbf{0} & \mathbf{I} & \mathbf{A}_1 & \ldots & \mathbf{A}_{n-1} \end{bmatrix}$$

$\mathbf{A}_i$: $L \times L$ invertible matrix over GF(q)

$rank(\mathbf{A}_i - \mathbf{A}_j) = L$

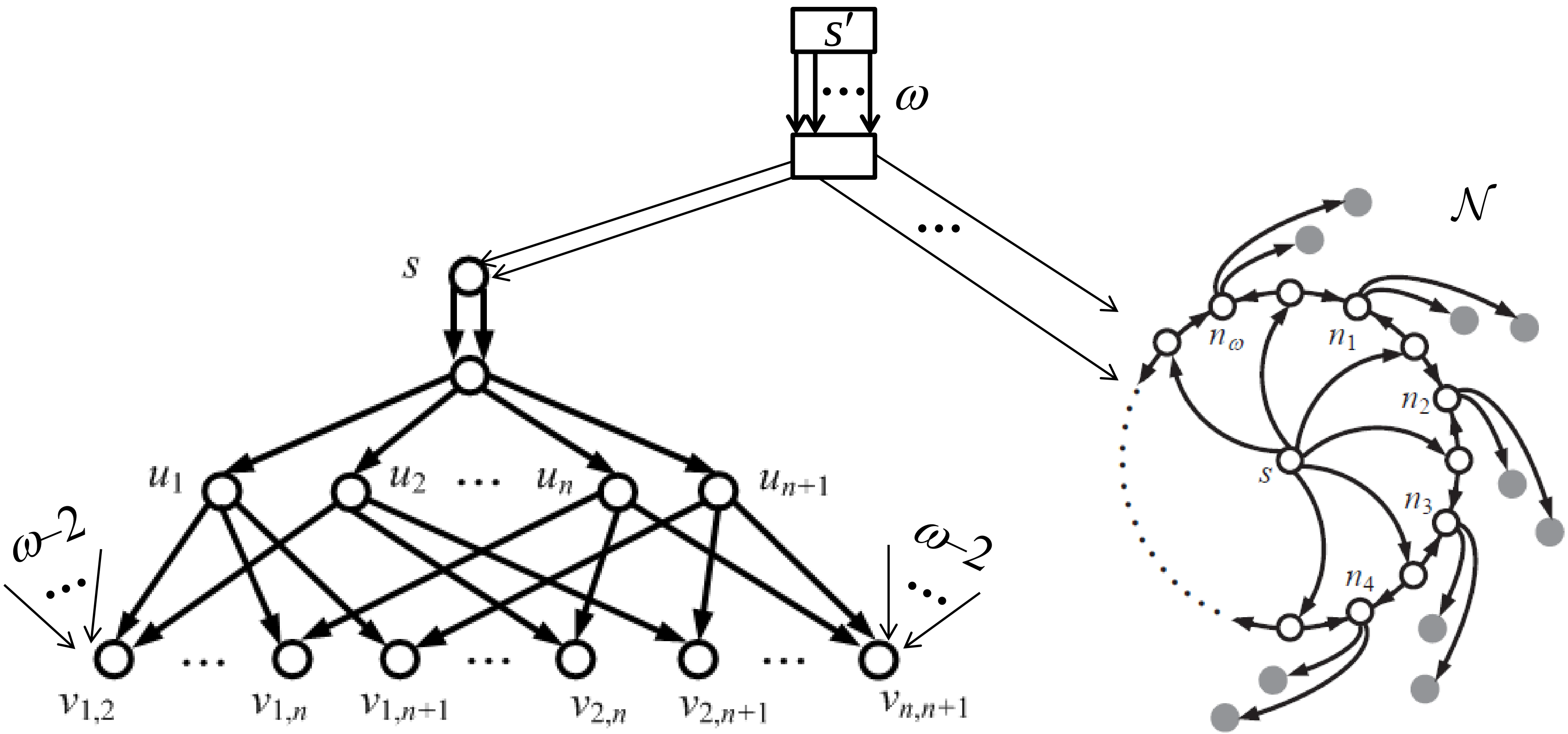
(n+1, 2)-Combination Network



- ∃ a *vector* linear solution over $GF(q)^L$ *iff* $q^L \geq n$.
- ∃ a *scalar* linear solution over $GF(q)^L$ *iff* $q^L \geq n$.

Verification of Conjecture 2

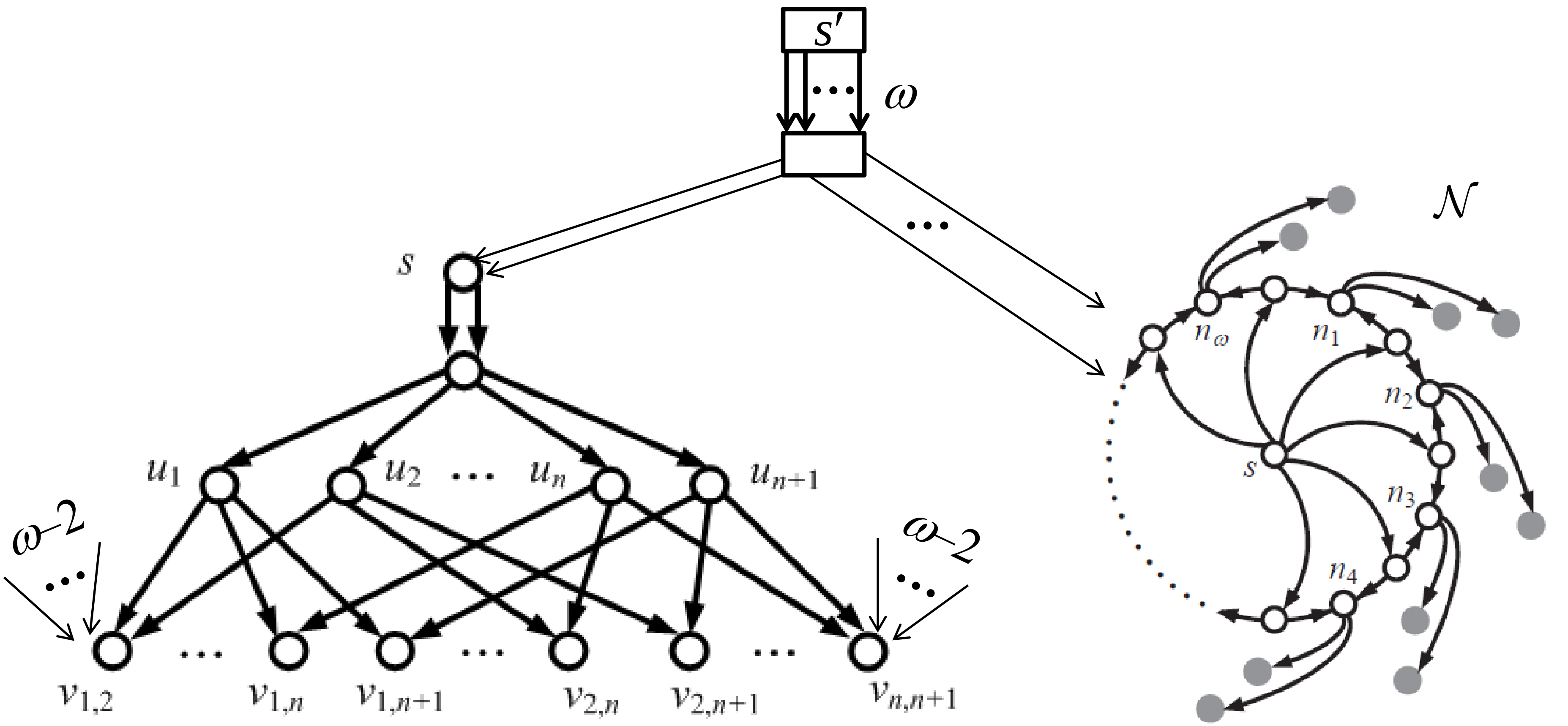
- Let $\mathcal{N}$ be an *arbitrary* multicast network that has a vector linear solution over GF$(q)^L$ but no scalar linear solution over GF(q^L).



(q^L+1, 2)-combination network

Verification of Conjecture 2

Theorem. The multicast network has a vector linear solution over $\mathrm{GF}(q)^L$ but no scalar linear solution over $\mathrm{GF}(q')$ for any $q' \leq q^L$.



(q^L+1, 2)-combination network

Vector vs. scalar LNC on multicast networks

Vector LNC outperforms scalar LNC in terms of alphabet size to yield a solution:

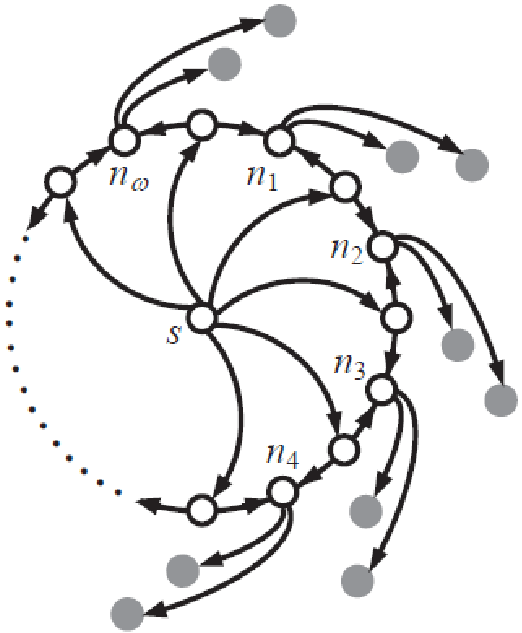
- Scalar linearly solvable over $GF(q^{L_1})$, …, $GF(q^{L_m})$ may not be so over $GF(q^{L_1+\dots+L_m})$.
  Vector linearly solvable over GF(q) of dimensions L_1, …, L_m must be so over GF(q) of dimensions $L_1+ \dots +L_m$
- There is a multicast network that has a vector linear solution over $GF(q)^L$ but no scalar linear solution over GF(q') for any $q' \leq q^L$.

Scalar LNC may also outperform vector LNC in terms of alphabet size to yield a solution too.

Vector vs. scalar LNC on multicast networks

Scalar LNC may also outperform vector LNC in terms of alphabet size to yield a solution too.

- Vector LNC can set base field = GF(2) in advance, and then merely increase L to yield a solution.
- $\exists$ multicast networks scalar linearly solvable over GF(q) but *not* vector linearly solvable over $GF(2)^L$ with $2^L > q$.



Scalar linearly solvable over GF(5), but not over $GF(2^p)$

Whether vector linearly solvable over $GF(2)^p$?

Vector linear solvability of Swirl network

- The Swirl network is *scalar* linearly solvable over GF(q)

  iff $\exists\, a_1, \ldots, a_\omega \in \mathrm{GF}(q)\backslash\{0, 1\}$, $b \in \mathrm{GF}(q)\backslash\{0\}$ s.t.

  $$b + m_1 \cdot m_2 \ldots m_\omega \neq 0,\ \forall\, m_j \in \{1, a_j\}$$

  $G \subset \mathrm{GF}(q)^\times \cong \mathbb{Z}_{q'-1}$ Assign $a_1, \ldots, a_\omega \in G\backslash\{1\}$, $b \in \mathrm{GF}(q)^\times\backslash G$

  iff $\exists$ a proper subgroup G of $\mathrm{GF}(q)^\times$ with $|G| \geq 2$.

- The Swirl network is *vector* linearly solvable over $\mathrm{GF}(q)^L$ *iff*

  $\exists$ invertible matrices $\mathbf{A}_1, \ldots, \mathbf{A}_\omega$, $\mathbf{B}$ over GF(q) of size $L \times L$ s.t.

  General Linear Group of degree L

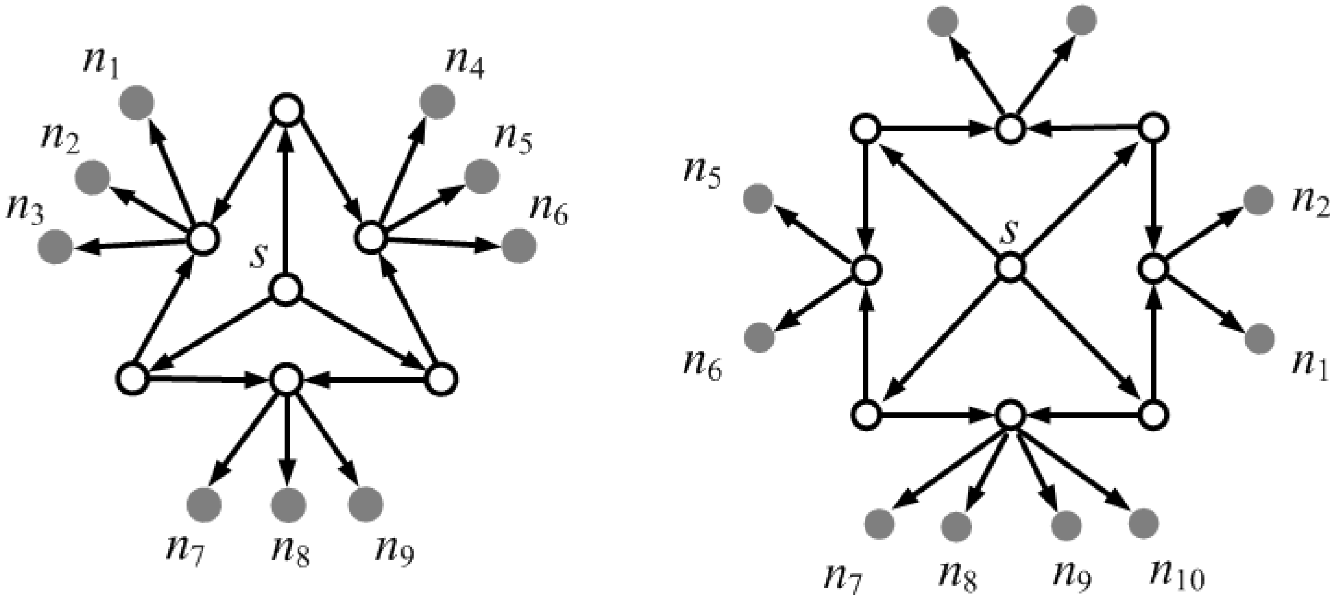
  $$rank(\mathbf{I} - \mathbf{A}_j) = L \quad \forall\, j$$

  $$rank(\mathbf{B} + \mathbf{M}_1 \cdot \mathbf{M}_2 \ldots \mathbf{M}_\omega) = L,\ \forall\, \mathbf{M}_j \in \{\mathbf{I}, \mathbf{A}_j\}$$

☹ Haven't found a good way to further analyze the equivalent conditions.

Vector vs. scalar LNC on multicast networks

- When $\omega \geq 6$, the Swirl network is *scalar* linearly solvable over GF(5), but *not vector* linearly solvable over $GF(2)^3$.



(a) (b)

Scalar linearly solvable over GF(7) but not over GF(8).

Not vector linearly solvable over $GF(2)^3$ either.

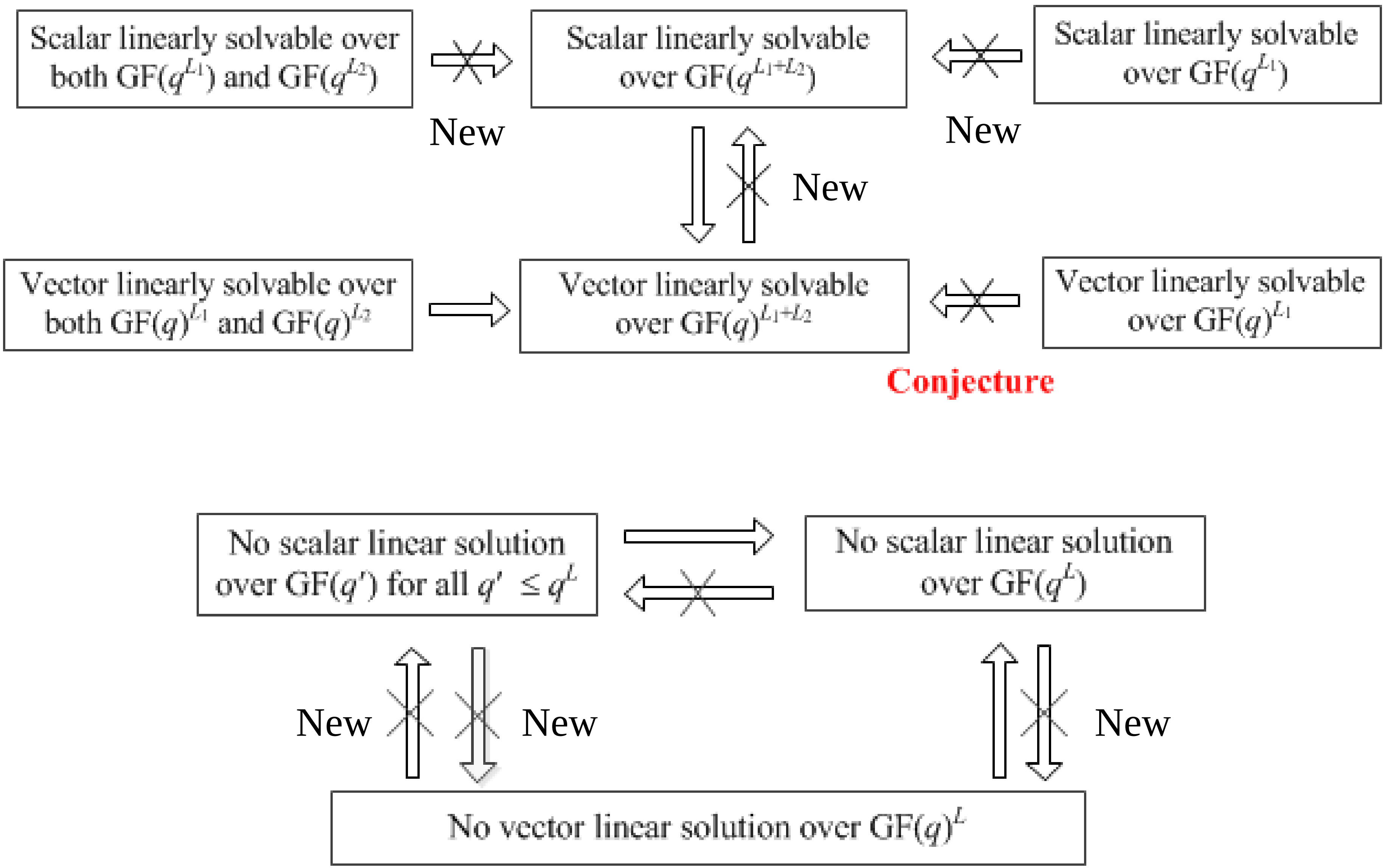
Vector vs. scalar LNC on multicast networks

Vector LNC outperforms scalar LNC in terms of alphabet size to yield a solution:

- Scalar linearly solvable over GF(q^{L_1}), …, GF(q^{L_m}) may not be so over GF($q^{L_1+\dots+L_m}$).
  Vector linearly solvable over GF(q) of dimensions L_1, …, L_m must be so over GF(q) of dimensions $L_1+\dots+L_m$
- There is a multicast network that has a vector linear solution over GF(q)^L but no scalar linear solution over GF(q') for any $q' \leq q^L$.

Scalar LNC may also outperform vector LNC in terms of alphabet size to yield a solution too.

Summary (on multicast networks)



Thanks!

Have a Prosperous Year of Sheep!