Linear Network Coding Over Ring Alphabets

Joe Connelly

University of California, San Diego

Final Defense
April 4th, 2018

Supported by NSF

www.connelly.fyi

Prior work:

Linear network coding over fields

(presented with *citation*)

Field: commutative *ring* with multiplicative inverses

Novel results:

Linear network coding over rings

- Which rings are best?
- When are rings better than fields?

(presented as *theorems*)

Outline

- ## Solvability over Commutative Rings

  "Linear Network Coding over Rings, Part I: Scalar Codes and Commutative Alphabets,"

  IEEE Transactions on Information Theory, Jan 2018

- ## Solvability over Non-Commutative Rings

  "Linear Network Coding over Rings, Part II: Vector Codes and Non-Commutative Alphabets,"

  IEEE Transactions on Information Theory, Jan 2018

- ## Non-Linear Solvability

  "A Class of Non-Linearly Solvable Networks,"

  IEEE Transactions on Information Theory, Jan 2017

- ## Capacity

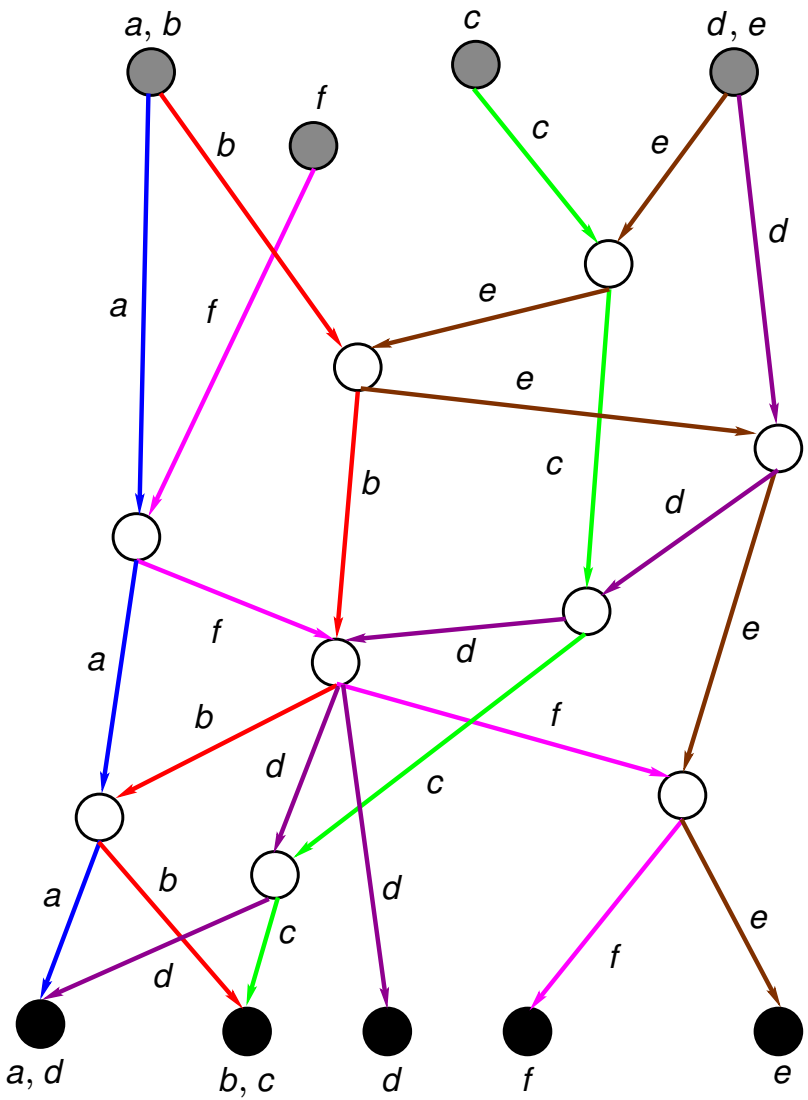
  "Capacity and Achievable Rate Regions for Linear Network Coding over Ring Alphabets,"

  submitted to *IEEE Transactions on Information Theory*

Joint work with Ken Zeger

Network Coding:
Motivation and Definitions

Why Study Networks?



Connected Devices:

2017: 15 billion

2021: 25 billion

(Cisco 2017)

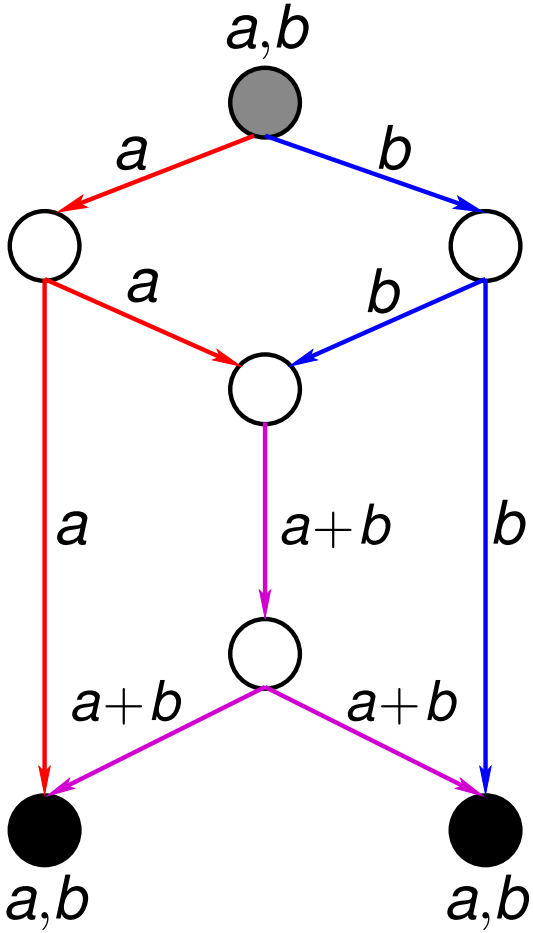
Network:

DAG with *senders* and *receivers*

Routing:

Users *relay* certain inputs

Butterfly Network



(Ahlswede, Cai, Li, Yeung 2000)

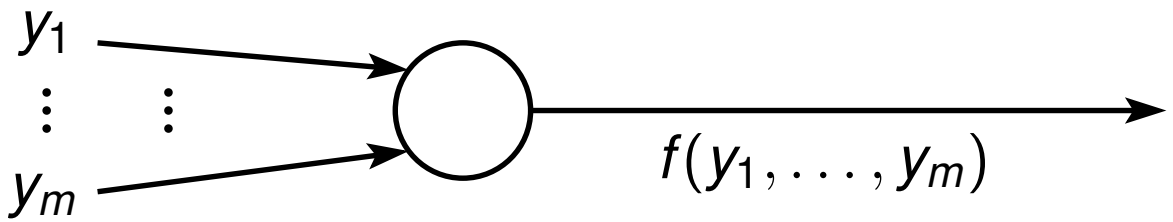
- No routing solution

  Coding solution (over any ring):

  $a = (a + b) - b$

  $b = (a + b) - a$

- *Network coding:* Nodes transmit *functions* of inputs



Code over $\mathcal{A}$ for network $\mathcal{N}$:

- Messages and edge symbols $\in \mathcal{A}$
- *Edge functions:* map inputs to symbol in $\mathcal{A}$

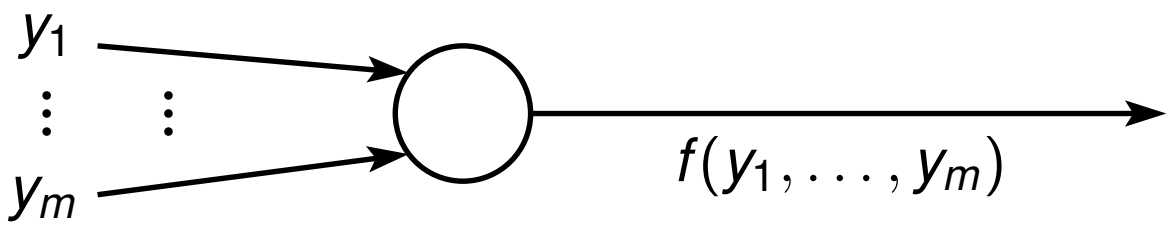
$$f : \mathcal{A}^m \to \mathcal{A}$$

$\mathcal{N}$ is *solvable*: $\exists$ code in which receivers recover demands

Ring alphabet:

- Set R with $+$ and $*$ operations
  - not all elements have multiplicative inverses
  - multiplication not always commutative
- Examples:
  - $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ with mod n arithmetic
  - $n \times n$ matrices over a field with matrix arithmetic

Special case: $\mathbb{F}_{p^k}$ = the *field* with p^k elements



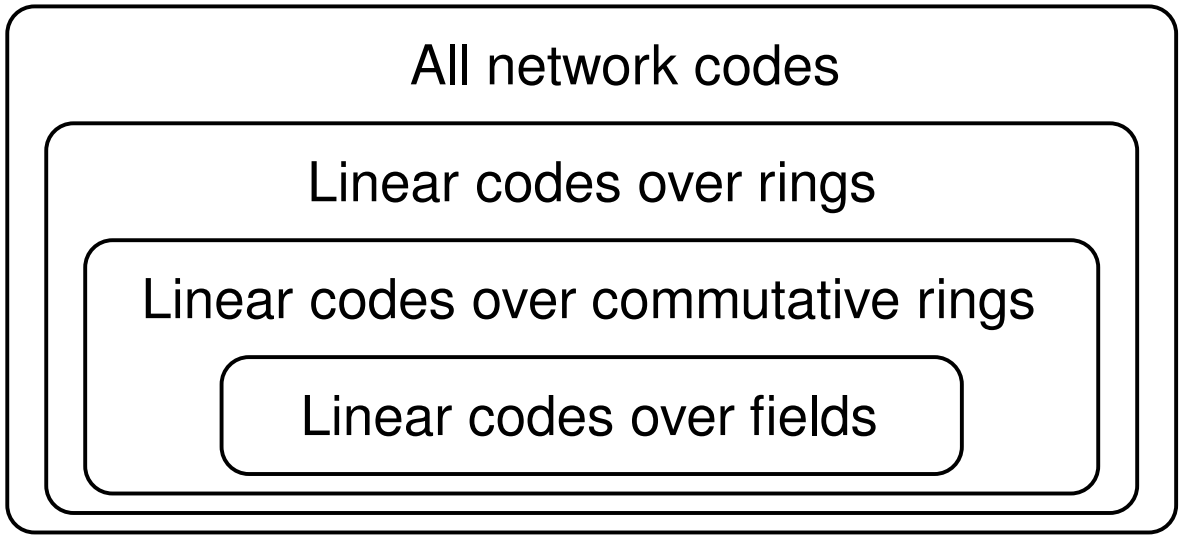
Linear code over the ring R:

- Messages and edge symbols $\in R$
- Edge functions *linear* over R

$$f(y_1, \ldots, y_m) = (A_1 * y_1) + \cdots + (A_m * y_m)$$

for some constants $A_1, \ldots, A_m \in R$

Why Linear Codes?



- More feasible analysis
- Lower implementation complexity
- Linear codes over fields have been a major area of study
- Linear codes over rings:
  - Previously not well studied
  - Potential advantages over fields

Solvability:

- *What is the "best" ring of a given size?*
- *What is the "best" ring for a given network?*
- *What field results extend to rings?*
- *Can $\mathcal{N}$ be linearly solvable only over non-field rings?*

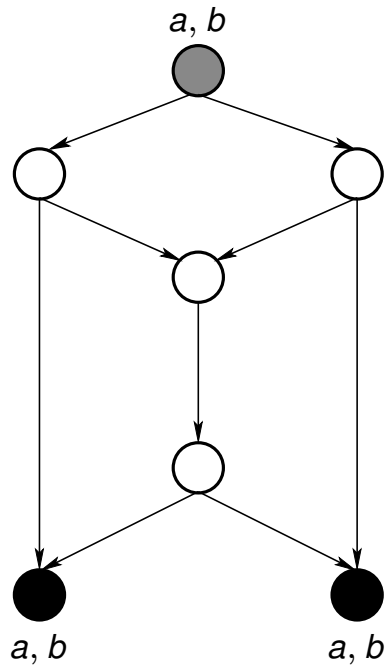
Capacity:

Are higher linear capacities attainable using non-field rings?

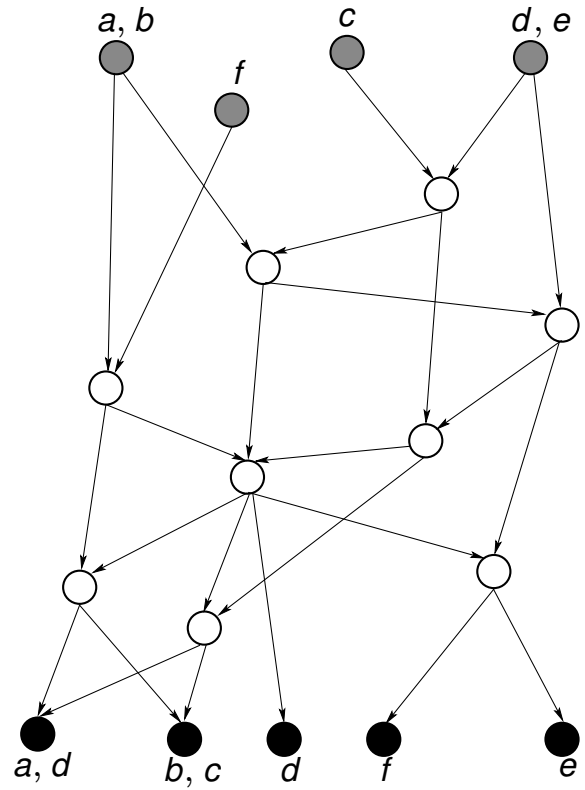
- ***Linear Solvability***
  - ***Fields***
  - Commutative Rings
  - Rings
- Capacity & Non-Linear Codes

Multicast network:

single source node, receivers demand all messages



Multicast Network



Non-Multicast Network

Multicast network:

single source node, receivers demand all messages

- Solvable
  $\Longrightarrow$ linearly solvable over every sufficiently large field
  (Li, Yeung, Cai 2003)
- Polynomial-time algorithms for linear solutions over fields
  (Jaggi et al. 2005)

General networks: not known whether solvability is decidable

(1) For network $\mathcal{N}$, $\exists$ collection of polynomials $\mathcal{P}$ such that:

$\mathcal{N}$ linearly solvable over $\mathbb{F} \iff \mathcal{P}$ has mutual root in $\mathbb{F}$

(Koetter, Médard 2003)

(2) For finite $\mathcal{P}$, $\exists$ network $\mathcal{N}$ such that:

$\mathcal{N}$ linearly solvable over $\mathbb{F} \iff \mathcal{P}$ has mutual root in $\mathbb{F}$

(Dougherty, Freiling, Zeger 2008)

Examples of (2):

$\mathcal{P}_1 = \{2x + 1\}$ has root in $\mathbb{F} \iff \text{char}(\mathbb{F}) \neq 2$

$\mathcal{P}_2 = \{2\}$ has root in $\mathbb{F} \iff \text{char}(\mathbb{F}) = 2$

$\mathcal{P}_3 = \{2, x^2+x+1\}$ has root in $\mathbb{F} \iff |\mathbb{F}| = 4^n$

- ***Linear Solvability***
  - Fields
  - ***Commutative Rings***
  - Rings
- Capacity & Non-Linear Codes

Unique field with p^k elements

Number of commutative rings $\sim p^{k^3}$ *(Poonen 2008)*

How do we identify "good" rings of size p^k?

Ring R *dominates* ring S:
$\forall \mathcal{N}$, $\mathcal{N}$ linearly solvable over S
$\implies$ $\mathcal{N}$ linearly solvable over R

Quasi-order on commutative rings of size m:

- reflexive and transitive
- not always anti-symmetric $(R \equiv S \not\Rightarrow R \cong S)$

R is *maximal* under dominance:

R is not *strictly* dominated by any commutative ring of size $|R|$

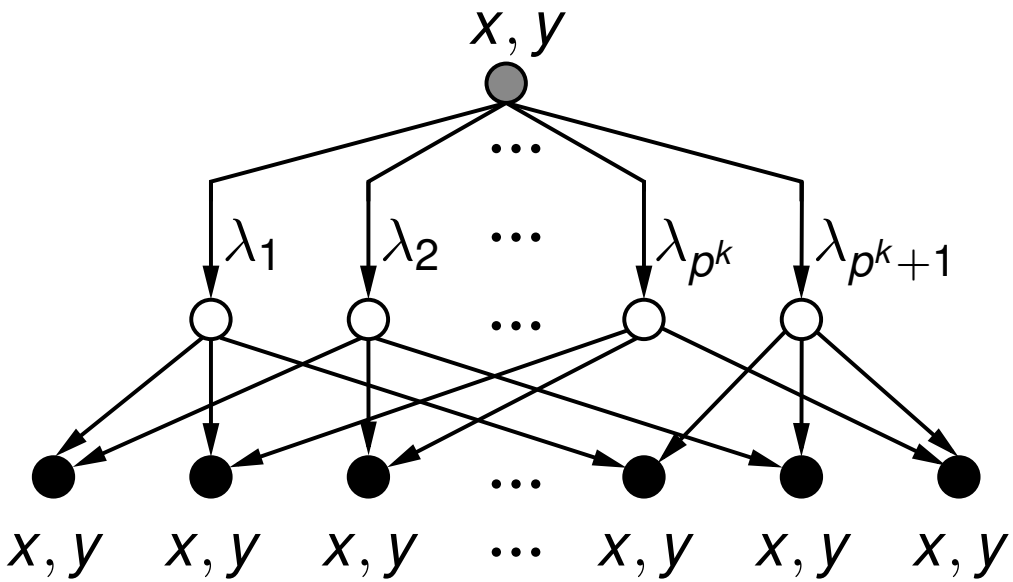
Maximal rings: "best" commutative rings of a given size

Theorem:

R is maximal $\iff \exists\, \mathcal{N}$ linearly solvable over R but no other commutative ring of size $|R|$

What are the maximal rings of a given size?

$(p^k + 1)$-Choose-Two Network



Theorem:
Linearly solvable over $\mathbb{F}_{p^k}$ but no other ring of size p^k

Is $\mathbb{F}_{p^k}$ the only maximal ring of size p^k ?

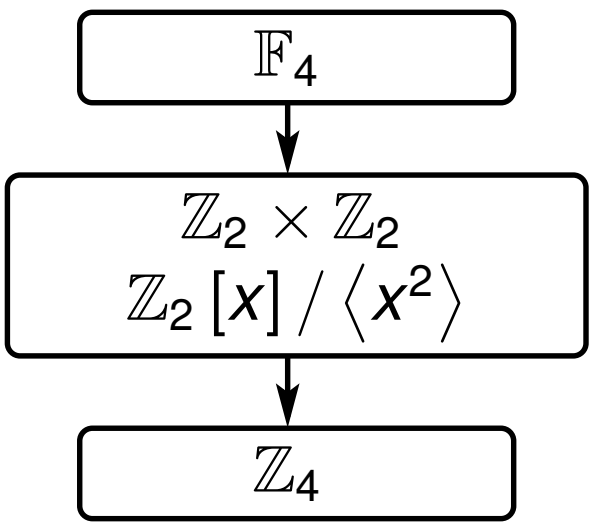
Example 1:

Four rings of size 4 (with multiplicative identity):

$$\mathbb{F}_4, \quad \mathbb{Z}_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_2[x] / \langle x^2 \rangle$$

Theorem:

Hasse Diagram under dominance:



$\therefore$ *all* other rings of size 4 are *strictly* dominated by $\mathbb{F}_4$

True for all prime powers?

Example 2:

$(x^3+x+1)(x^2+x+1)$ has roots in $\mathbb{F}_8$ and $\mathbb{F}_4$ but not $\mathbb{F}_{32}$

$\implies$ $\exists$ network linearly solvable over $\mathbb{F}_8 \times \mathbb{F}_4$ but not $\mathbb{F}_{32}$

> ***Theorem:***
> $\mathbb{F}_{32}$ and $\mathbb{F}_8 \times \mathbb{F}_4$ are both maximal of size 32

$\therefore$ no "best" ring of size 32

How does this generalize?

Theorem:

$\mathbb{F}_{p^k}$ is the only maximal ring of size p^k
$\iff k \in \{1, 2, 3, 4, 6\}$

Corollary:

$\exists$ network linearly solvable over some commutative ring of size p^k but not over $\mathbb{F}_{p^k} \iff k = 5$ or $k \geq 7$

What if $|R|$ is not a prime power?

Theorem:

Let $|R| = p_1^{k_1} \cdots p_t^{k_t}$. R is maximal if and only if R is a direct product of maximal rings of sizes $p_1^{k_1}, \ldots, p_t^{k_t}$

Example 1: Size $12 = (4)(3)$ maximal ring:

$$\mathbb{F}_4 \times \mathbb{F}_3$$

Example 2: Size $96 = (32)(3)$ maximal rings:

$$\mathbb{F}_{32} \times \mathbb{F}_3 \quad \text{and} \quad \mathbb{F}_8 \times \mathbb{F}_4 \times \mathbb{F}_3$$

Commutative Solvability Conclusions

- *Ring dominance*: method of comparing ring alphabets
- *Maximal rings*: "best" commutative rings
- $\mathbb{F}_{p^k}$ is the unique maximal ring of size p^k
  $\iff k \in \{1, 2, 3, 4, 6\}$
- Non-power-of-prime size maximal rings:
  direct products of prime-power size maximal rings

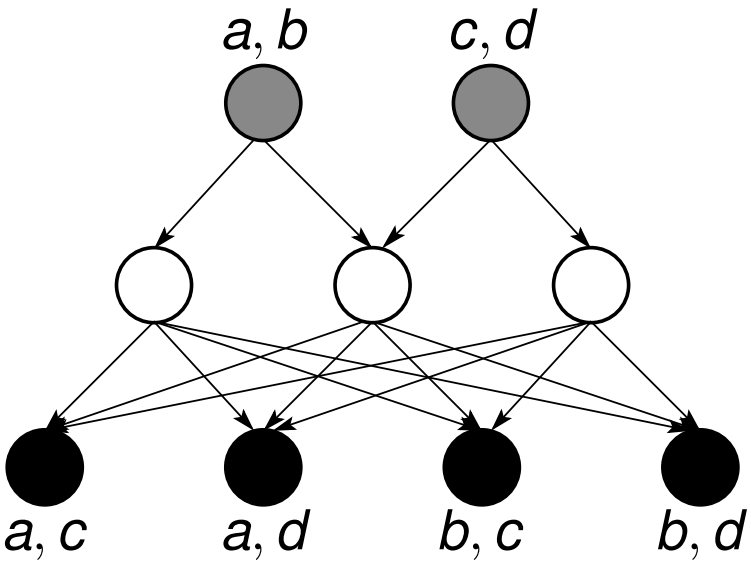
- ***Linear Solvability***
  - Fields
  - Commutative Rings
  - ***Rings***
- Capacity & Non-Linear Codes

Theorem:
$\mathcal{N}$ linearly solvable over some commutative ring
$\iff$ $\mathcal{N}$ linearly solvable over some field

Does this result hold for general rings?

Theorem:
If $\mathcal{N}$ is linearly solvable over non-commutative ring R but not over any commutative ring, then $|R| \geq 16$

Is this bound tight?



M Network

(Médard, Effros, Ho, Karger 2003)

- Not linear solvable over any field

Theorem:

Linearly solvable over the ring of binary 2×2 matrices but not over any commutative ring

Recall:

Multicast network $\mathcal{N}$ is solvable

$\Longrightarrow$ $\mathcal{N}$ linearly solvable over every sufficiently large $\mathbb{F}$

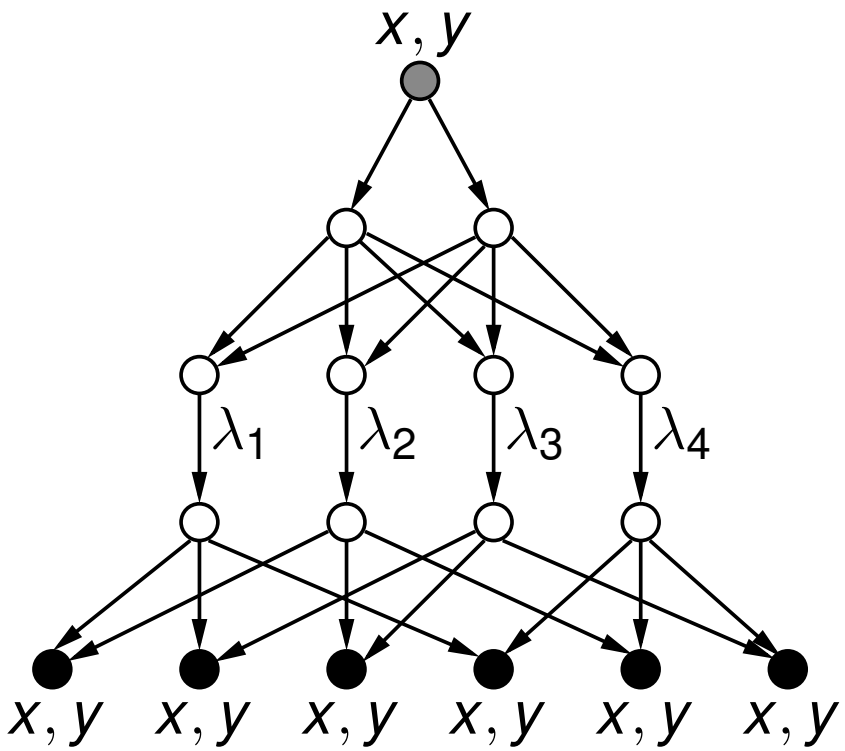
(Li, Yeung, Cai 2003)

Does this result hold for general rings?

Lemma:

If $|R| = 2 \bmod 4$, then $\mathbb{F}_2$ dominates R

Two-Six Network



Theorem:
Linearly solvable over *some* ring of size m
$\iff m \neq 2 \bmod 4$

Solvable over $\mathcal{A} \iff |\mathcal{A}| \notin \{2, 6\}$

(Dougherty, Freiling, Zeger 2004)

Euler's conjecture on ***Orthogonal Latin Squares***

(Bose, Shrikhande, Parker 1960)

What is the "best" ring for a given network?

- Larger alphabet $\longrightarrow$ higher complexity at nodes
- Minimizing alphabet size is an important problem in network coding, e.g.

  (Langberg et al. 2006), *(Jaggi et al. 2005)*, *(Wachter-Zeh, Etzion 2018)*

k-dimensional vector linear code over R:

- messages and edge symbols $\in R^k$
- edge functions:

$$(\mathbf{A_1} y_1) + \cdots + (\mathbf{A_n} y_n)$$

where $\mathbf{A_1}, \ldots, \mathbf{A_n}$ are $k \times k$ matrices over R

What is the "best" ring for a given network?

Theorem:
Vector linear codes over fields minimize alphabet size needed for a linear solution

(even when more general linearity is allowed)

k-dimensional vector linear code over R:

- messages and edge symbols $\in R^k$
- edge functions:

$$(\mathbf{A_1} y_1) + \cdots + (\mathbf{A_n} y_n)$$

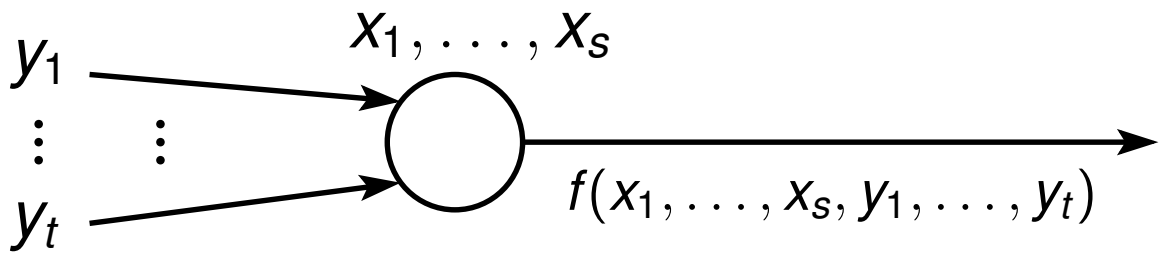
where $\mathbf{A_1}, \ldots, \mathbf{A_n}$ are $k \times k$ matrices over R

Ring Solvability Conclusions

- Linear solvability over some ring
  $\not\Rightarrow$ linear solvability over some commutative ring
- Multicast network is solvable
  $\not\Rightarrow$ linearly solvable over every sufficiently large ring
- *Vector* linear codes over fields minimize alphabet size

- Linear Solvability
  - Fields
  - Commutative Rings
  - Rings

- ***Capacity & Non-Linear Codes***



(k,n) fractional code over $\mathcal{A}$:

- Messages: $x_i \in \mathcal{A}^k$
- Edge symbols: $y_i \in \mathcal{A}^n$
- ***Rate:*** $r = \dfrac{k}{n}$

Capacity of $\mathcal{N}$ over $\mathcal{A}$:

$$\sup\{r \in \mathbb{Q} \,:\, r \text{ achievable over } \mathcal{A}\}$$

Finding network capacities is an open problem

- Not known whether capacity is computable
- Capacities related to characterization of entropy functions *(Chant, Grant 2007)*
- Non-Shannon information inequalities may be needed *(Dougherty, Freiling, Zeger 2007)*
- Capacity is independent of alphabet size *(Cannons, et al. 2006)*

(k,n) fractional linear code over R:

- Messages $\in R^k$ and edge symbols $\in R^n$
- Edge functions *linear* over R:

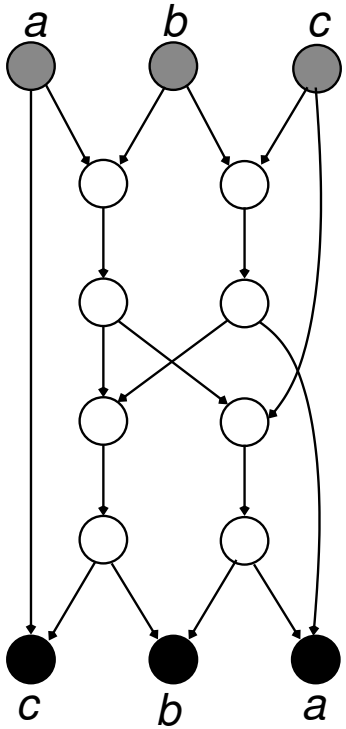
$$(\mathbf{A_1}\, y_1) + \cdots + (\mathbf{A_m}\, y_m)$$

where y_i's are input vectors and $\mathbf{A_i}$'s are matrices

Linear Capacity of $\mathcal{N}$ over R:

$$\mathcal{C}(\mathcal{N}, R) = \sup\{r \in \mathbb{Q} : r \text{ linearly achievable over } R\}$$

Linear Capacities over Fields Example



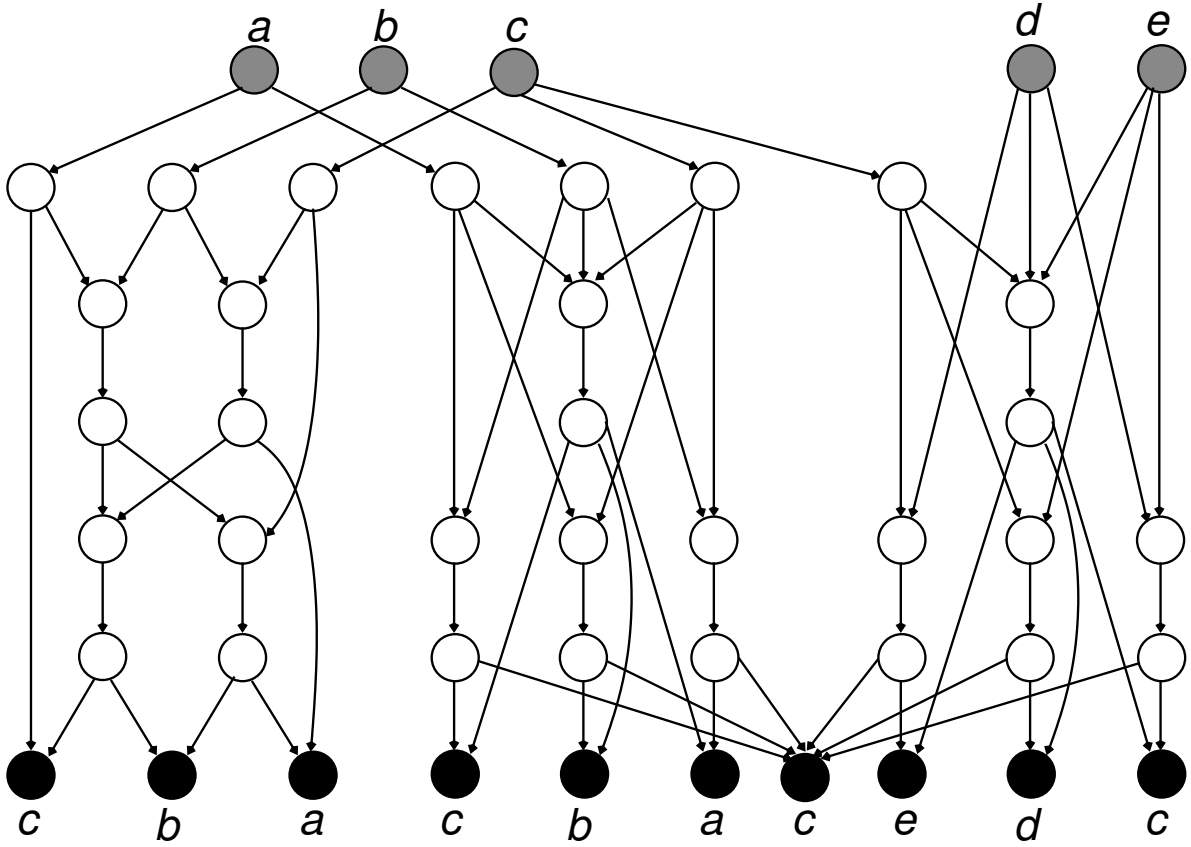
The linear capacity of the *Fano Network* over $\mathbb{F}$ is

- 1 if $\text{char}(\mathbb{F}) = 2$
- $4/5$ if $\text{char}(\mathbb{F}) \neq 2$

(Dougherty, Freiling, Zeger 2005)

Linear Codes Insufficient

(Dougherty, Freiling, Zeger 2005)



- Non-linearly solvable over size 4 alphabet
- Not linearly solvable over any ring
- Capacity $>$ linear capacity over any field

Theorem:
$\exists$ infinite class of **non-linearly** solvable networks with capacities $>$ linear capacities over fields

- Linear codes over fields cannot approximate capacity to any constant factor
  (Blasiak, Kleinberg, Lubetzky 2011) *(Lovett 2014)*

Big Question:

Are higher linear capacities attainable using non-field rings?

Theorem:

Let R be a ring and $\mathbb{F}$ a field. $\exists$ network $\mathcal{N}$ such that

$$\mathcal{C}(\mathcal{N}, R) > \mathcal{C}(\mathcal{N}, \mathbb{F})$$

if and only if $\gcd(|R|, |\mathbb{F}|) = 1$

Corollary:

If $|R| = |\mathbb{F}|$, then for any network, any rate linearly achievable over R is linearly achievable over $\mathbb{F}$

Corollary:

Let $\mathbb{F}$ and $\mathbb{K}$ be fields. $\mathcal{C}(\mathcal{N}, \mathbb{F}) = \mathcal{C}(\mathcal{N}, \mathbb{K})$ for each $\mathcal{N}$ **if and only if** $\text{char}(\mathbb{F}) = \text{char}(\mathbb{K})$

Recall: linear functions over R are of the form:

$$(A_1 * y_1) + \cdots + (A_m * y_m)$$

If R is non-commutative, then *two-sided linear functions*

$$\begin{aligned}(A_{1,1} * y_1 * B_{1,1}) \ + \cdots + \ (A_{1,n} * y_1 * B_{1,n}) + \\ \vdots \\ + (A_{m,1} * y_m * B_{m,1}) + \cdots + (A_{m,n} * y_m * B_{m,n})\end{aligned}$$

are a broader class of functions

Example:
Let R be the ring of all 2×2 binary matrices and let

$$f\left(\begin{bmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{bmatrix}\right) = \begin{bmatrix} x_{1,1} & 0 \\ 0 & x_{2,2} \end{bmatrix}$$

$f(\mathbf{X})$ is not of the form $\mathbf{AXB}$, but

$$f(\mathbf{X}) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \mathbf{X} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \mathbf{X} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

What if we allow two-sided linear functions over rings?

Theorem:

Even allowing two-sided linear functions,

$$\mathcal{C}(\mathcal{N}, R) \leq \mathcal{C}(\mathcal{N}, \mathbb{F})$$

for all $\mathcal{N}$, whenever $\gcd(|R|, |\mathbb{F}|) \neq 1$.

Higher capacities *cannot* be attained using non-field rings

Conclusions
Linear Codes over Rings

Ring Linearity Conclusions

- Linear coding over non-power-of-prime alphabet sizes
- Rings offer some specific solvability advantages
- "Best" alphabets: vector codes over prime fields
- Higher linear capacities *cannot* be attained using non-field rings
- $\exists$ networks with capacities $>$ linear capacities over fields, rings, and even modules

Future: Low-complexity, mathematically-tractable class of codes that outperform linear codes over fields?

References

- R. Ahlswede, N. Cai, S.-Y.R. Li, and R.W. Yeung,
"Network information flow,"
IEEE Transactions on Information Theory, July 2000.
- A. Blasiak, R. Kleinberg,and E. Lubetzky,
"Lexicographic products and the power of non-linear network coding,"
IEEE Symposium on Foundations of Computer Science (FOCS), 2011.
- J. Cannons, R. Dougherty, C. Freiling, and K. Zeger,
"Network routing capacity,"
IEEE Transactions on Information Theory, March 2006.
- *Cisco Visual Networking Index: Forecast and Methodology, 2016–2021*,
June 2017.
- R. Dougherty, C. Freiling, and K. Zeger,
"Linearity and solvability in multicast networks,"
IEEE Transactions on Information Theory, October 2004.
- R. Dougherty, C. Freiling, and K. Zeger,
"Insufficiency of linear coding in network information flow,"
IEEE Transactions on Information Theory, August 2005.
- R. Dougherty, C. Freiling, and K. Zeger,
"Networks, matroids, and non-Shannon information inequalities,"
IEEE Transactions on Information Theory, June 2007.
- R. Dougherty, C. Freiling, K. Zeger,
"Linear network codes and systems of polynomial equations',"
IEEE Transactions on Information Theory, May 2008.

References (cont)

- R. Dougherty, E. Freiling, and K. Zeger,
"Characteristic-dependent linear rank inequalities with applications to network coding,"
IEEE Transactions on Information Theory, May 2015.
- S. El Rouayheb, A. Sprintson, and C. Georghiades,
"On the index coding problem and its relation to network coding and matroid theory,"
IEEE Transactions on Information Theory, July 2010.
- T. Etzion and A. Wachter-Zeh,
"Vector network coding based on subspace codes outperforms scalar linear network coding,"
to appear *IEEE Transactions on Information Theory*.
- T. Ho, M. Médard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong,
"A random linear network coding approach to multicast,"
IEEE Transactions on Information Theory, October 2006.
- S. Jaggi, P. Sanders, P. Chou, M. Effros, S. Egner, K. Jain, and L. Tolhuizen,
"Polynomial time algorithms for multicast network code construction,"
IEEE Transactions on Information Theory, June 2005.
- R. Koetter and M. Médard,
"An algebraic approach to network coding,"
IEEE/ACM Transactions on Networking, October 2003.
- P. Krishnan and B.S. Rajan,
"A matroidal framework for network-error correcting codes,"
IEEE Transactions on Information Theory, February 2015.
- M. Langberg, A. Sprintson and J. Bruck,
"The encoding complexity of network coding,"
IEEE Transactions on Information Theory, June 2006.

References (cont)

- S.-Y.R. Li, R.W. Yeung, and N. Cai,
  "Linear network coding,"
  IEEE Transactions on Information Theory, February 2003.
- S. Lovett,
  "Linear codes cannot approximate the network capacity within any constant factor,"
  Electronic Colloquium on Computational Complexity, 2014.
- M. Médard, M. Effros, T. Ho, and D. Karger,
  "On coding for non-multicast networks,"
  Conference on Communication Control and Computing, October 2003.
- B. Poonen,
  "The moduli space of commutative algebras of finite rank,"
  Journal of the European Mathematical Society, October 2008.
- B.K. Rai and B.K. Dey,
  "On network coding for sum-networks,"
  IEEE Transactions on Information Theory, January 2012.
- A. Rasala Lehman and E. Lehman,
  "Complexity classification of network information flow problems,"
  ACM-SIAM Symposium on Discrete algorithms, 2004.
- S. Riis,
  "Linear versus nonlinear boolean functions in network flow,"
  Conference on Information Sciences and Systems (CISS), March 2004.
- Q. Sun, X. Yin, Z. Li, and K. Long,
  "Multicast network coding and field sizes,"
  IEEE Transactions on Information Theory, November 2015.