Iterative Coding for Network Coding

Andrea Montanari*, Vish Rathi† and Rüdiger Urbanke†

*Stanford, †EPFL

March 26, 2008

Outline

Outline

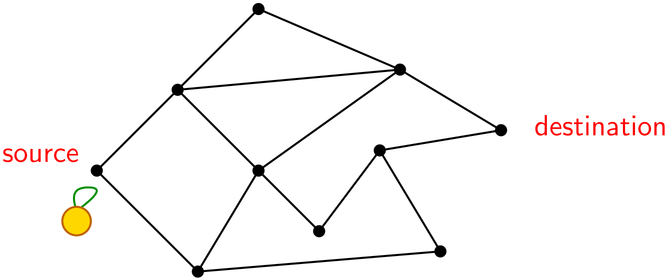
Outline

Outline

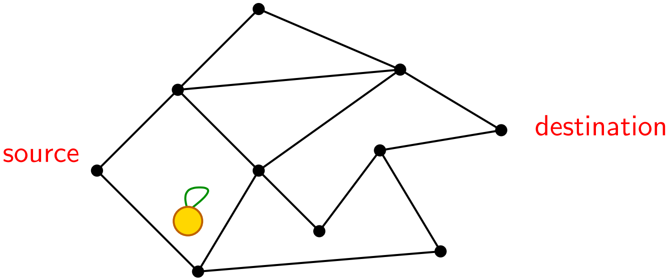
Outline

Information is not oranges

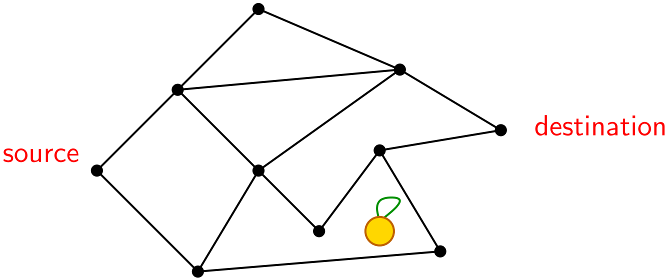
Current approach to communication networks



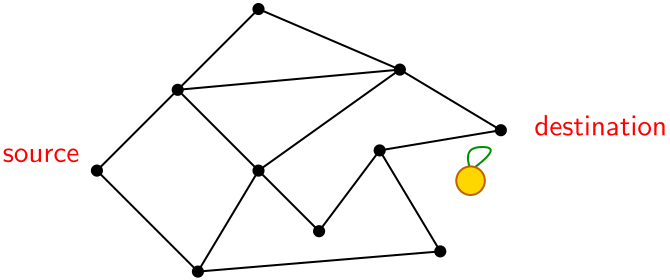
Current approach to communication networks



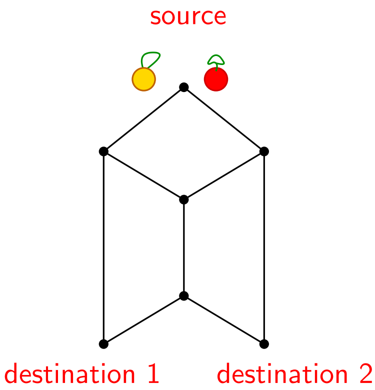
Current approach to communication networks



Current approach to communication networks

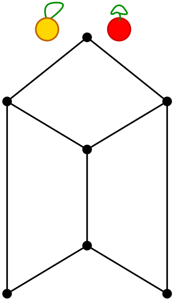


What are we losing? The butterfly example

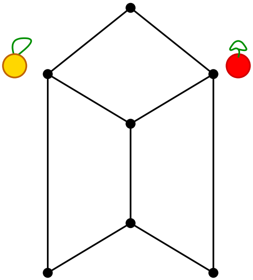


[Ahlswede,Cai,Li,Yeung, 2000]

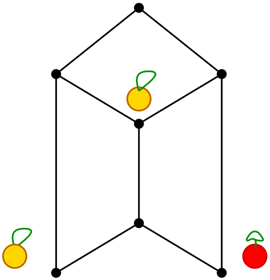
The butterfly example: Routing



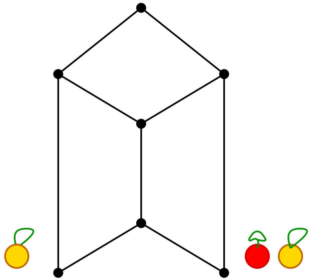
The butterfly example: Routing



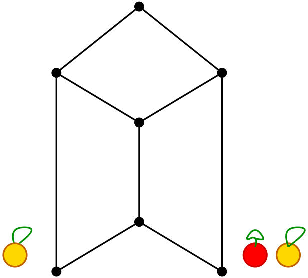
The butterfly example: Routing



The butterfly example: Routing

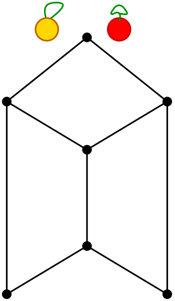


The butterfly example: Routing

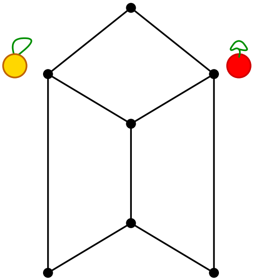


1.5 bits per cycle

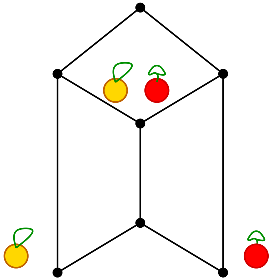
The butterfly example: Network Coding



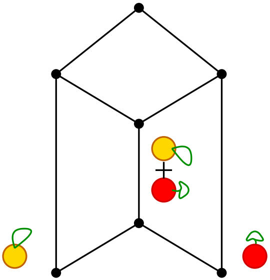
The butterfly example: Network Coding



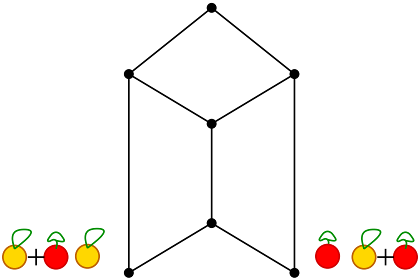
The butterfly example: Network Coding



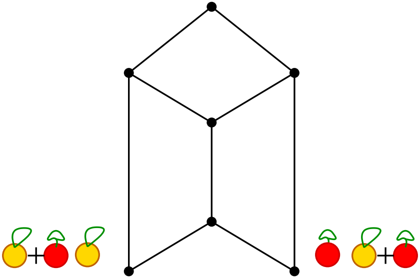
The butterfly example: Network Coding



The butterfly example: Network Coding



The butterfly example: Netwok Coding



2 bits per cycle

Practical network coding

Problem

No one knows the network structure.

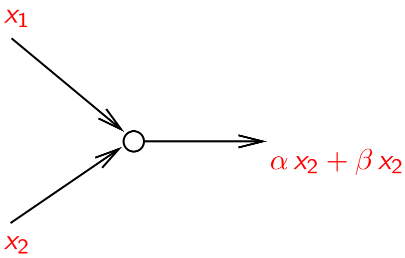
Source/destination do not control intermediate nodes.

Problem

No one knows the network structure.

Source/destination do not control intermediate nodes.

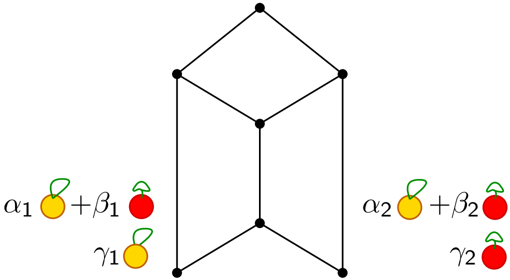
Idea



Forward random combinations

[Chou, Wu, Jain/ Ho, Kötter, Medard, Karger, Effros 2003]

How can that possibly work?



Wait a minute. . .

How am I supposed to figure out α, β, γ?

Wait a minute. . .

How am I supposed to figure out α, β, γ?

Idea: Header

Input:

 $= [1 \quad 0 | \cdots\cdots x_1 \cdots\cdots]$

 $= [0 \quad 1 | \cdots\cdots x_2 \cdots\cdots]$

Idea: Header

Output:

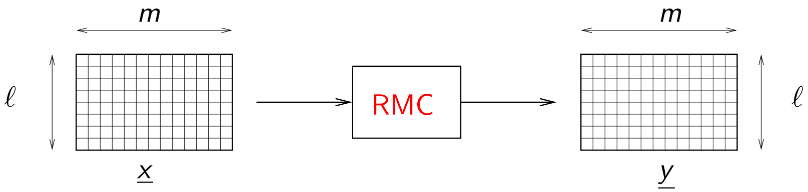
$$? \; + \; ? \; = [\alpha \quad \gamma | \cdots \alpha x_1 + \gamma x_2 \cdots]$$

$$? \; + \; ? \; = [\delta \quad \beta | \cdots \delta x_1 + \beta x_2 \cdots]$$

Noisy network coding

Rank Metric Channel (Symmetric Network Channel)

(Gabidulin, 1985)



$$\underline{y} = \underline{x} \oplus \underline{z},$$

$\underline{z}$ uniformly random with $\mathrm{rank}(\underline{z}) = \ell\omega$

Asymptotics, Rate, Capacity

$$\ell = N\lambda,\ m = N(1-\lambda),\ N \to \infty$$

$$R = \frac{\log_2 |\mathrm{Code}|}{m\ell},$$

$$C(\lambda, \omega) = \frac{1-\lambda-\omega+\lambda\omega^2}{1-\lambda}.$$

Asymptotics, Rate, Capacity

$$\ell = N\lambda,\ m = N(1-\lambda),\ N \to \infty$$

$$R = \frac{\log_2 |\mathrm{Code}|}{m\ell},$$

$$C(\lambda,\omega) = \frac{1-\lambda-\omega+\lambda\omega^2}{1-\lambda}.$$

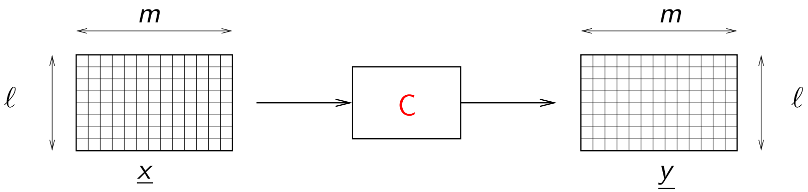
Asymptotics, Rate, Capacity

$\ell = N\lambda,\ m = N(1-\lambda),\ N \to \infty$

$$R = \frac{\log_2 |\mathrm{Code}|}{m\ell},$$

$$C(\lambda,\omega) = \frac{1-\lambda-\omega+\lambda\omega^2}{1-\lambda}.$$

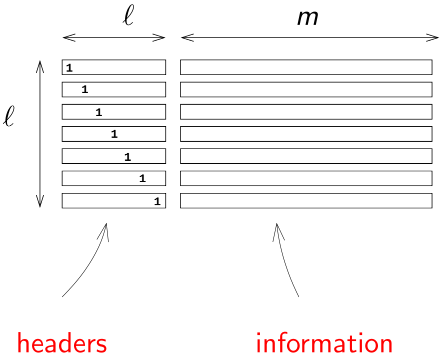
Matrix channels



$$\underline{x} = \{x_{ij}\} \in \mathbb{F}_2^{m \times \ell}$$

Network coding???

(Kötter, Kschischang, 2007)



$$\equiv \left[\ \underline{1}\ \middle|\ \ \underline{x}\ \ \right]$$

(Chou, Wu, Jain, 2003)

Reliable network

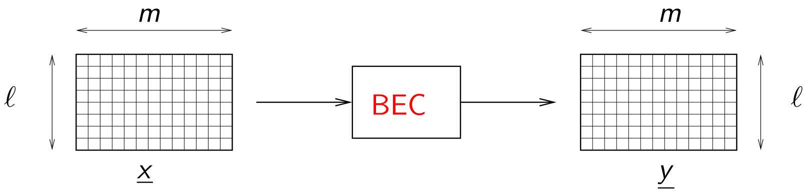
$$\left[\ \underline{1}\ \middle|\ \underline{x}\ \right] \longrightarrow \boxed{\text{NET}} \longrightarrow \left[\ G\ \middle|\ G\underline{x}\ \right] \longrightarrow \boxed{G^{-1}} \longrightarrow \left[\ \underline{1}\ \middle|\ \underline{x}\ \right]$$

Faulty network

$$\left[\ \underline{1}\ \middle|\ \underline{x}\ \right] \longrightarrow \boxed{\text{NET}} \longrightarrow \left[\ G\ \middle|\ G\underline{x}+\underline{z}'\ \right] \longrightarrow \boxed{G^{-1}} \longrightarrow \left[\ \underline{1}\ \middle|\ \underline{x}+G^{-1}\underline{z}'\ \right]$$

Binary Erasure Channel

(Elias, 1954)



$$y_{ij} = \begin{cases} x_{ij} & \text{with prob. } \epsilon, \\ * & \text{with prob. } 1-\epsilon. \end{cases}$$

independently

Asymptotics, Rate, Capacity

$\ell = N\lambda$, $m = N(1-\lambda)$, $N \to \infty$

$$R = \frac{\log_2 |\mathrm{Code}|}{m\ell},$$

$$C(\epsilon) = 1 - \epsilon.$$

Asymptotics, Rate, Capacity

$\ell = N\lambda,\ m = N(1-\lambda),\ N \to \infty$

$$R = \frac{\log_2 |\mathrm{Code}|}{m\ell},$$

$$C(\epsilon) = 1 - \epsilon.$$

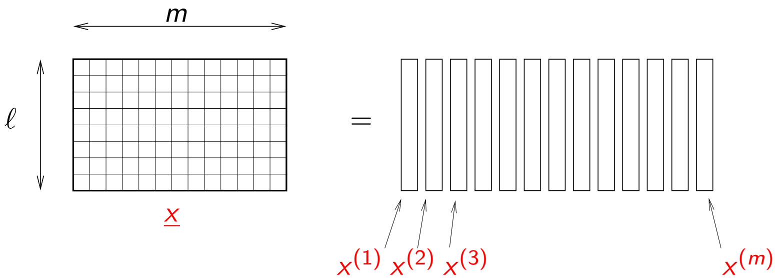
Asymptotics, Rate, Capacity

$\ell = N\lambda$, $m = N(1-\lambda)$, $N \to \infty$

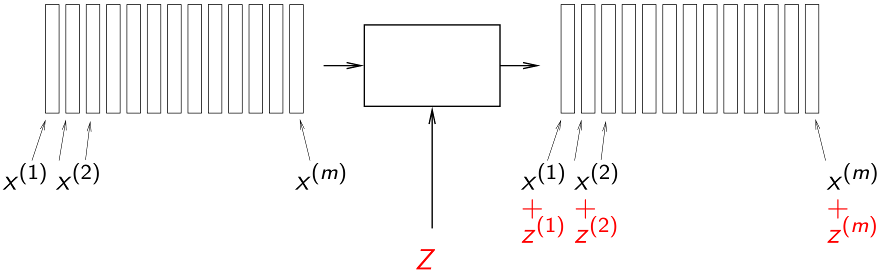
$$\begin{aligned} R &= \frac{\log_2 |\mathrm{Code}|}{m\ell}\,, \\ C(\epsilon) &= 1-\epsilon\,. \end{aligned}$$

Construction and decoding algorithm

Equivalent descripton of the channel

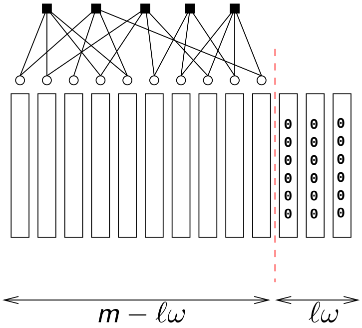


Equivalent descripton of the channel



$Z \equiv$ uniformly random subspace $\subseteq \mathbb{F}_2^{\ell}$
$z^{(1)}, \ldots, z^{(m)} \in Z$

Code

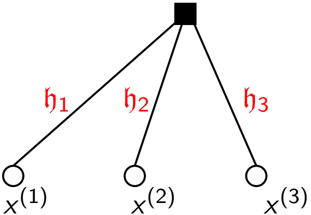


$m - \ell\omega$ 'symbols' $\longrightarrow$ LDPC

$\ell\omega$ 'symbols' $\longrightarrow$ learn the error space Z

LDPC: Check nodes

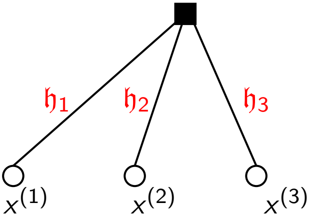
$$\mathfrak{h}_1 x^{(1)} + \mathfrak{h}_2 x^{(2)} + \mathfrak{h}_3 x^{(3)} = 0$$



'Edge labels' $\mathfrak{h}_i \in \mathbb{F}_2^{\ell \times \ell}$: $\ell \times \ell$ matrices

LDPC: Check nodes

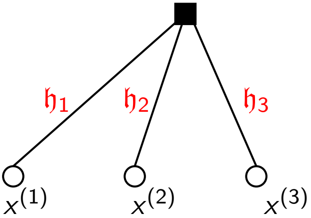
$$\mathfrak{h}_1 x^{(1)} + \mathfrak{h}_2 x^{(2)} + \mathfrak{h}_3 x^{(3)} = 0$$



'Edge labels' $\mathfrak{h}_i \in \mathbb{F}_2^{\ell \times \ell}$: $\ell \times \ell$ matrices

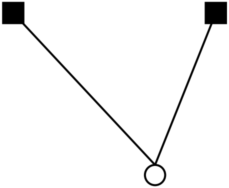
LDPC: Check nodes

$$\mathfrak{h}_1 x^{(1)} + \mathfrak{h}_2 x^{(2)} + \mathfrak{h}_3 x^{(3)} = 0$$



'Edge labels' $\mathfrak{h}_i \in \mathbb{F}_2^{\ell\times\ell}$: $\ell \times \ell$ matrices

LDPC: Variable nodes



$$x^{(i)} \in \{z^{(i)} + Z\}$$

Degree $= 2$!

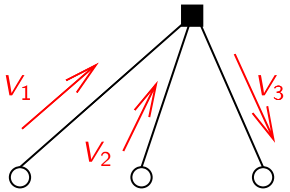
Message passing decoder

Messages $\longrightarrow$ Affine subspaces $V_{i\to a} \subseteq \mathbb{F}_2^{\ell}$

Operations $\longrightarrow$ Subspace intersections/sums

Message passing decoder: Check nodes

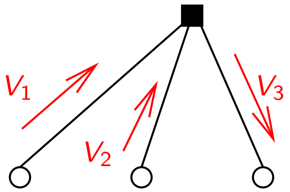
$$\mathfrak{h}_1 x^{(1)} + \mathfrak{h}_2 x^{(2)} + \mathfrak{h}_3 x^{(3)} = 0$$



$$V_3 = \mathfrak{h}_3^{-1}(\mathfrak{h}_1 V_1 + \mathfrak{h}_2 V_2)$$

Message passing decoder: Check nodes

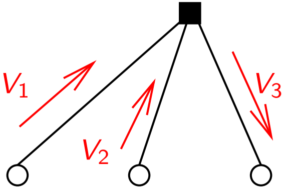
$$\mathfrak{h}_1 x^{(1)} + \mathfrak{h}_2 x^{(2)} + \mathfrak{h}_3 x^{(3)} = 0$$



$$V_3 = \mathfrak{h}_3^{-1}(\mathfrak{h}_1 V_1 + \mathfrak{h}_2 V_2)$$

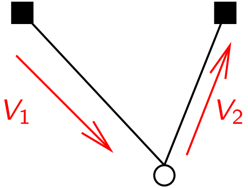
Message passing decoder: Check nodes

$$\mathfrak{h}_1 x^{(1)} + \mathfrak{h}_2 x^{(2)} + \mathfrak{h}_3 x^{(3)} = 0$$



$$V_3 = \mathfrak{h}_3^{-1} \left(\mathfrak{h}_1 V_1 + \mathfrak{h}_2 V_2 \right)$$

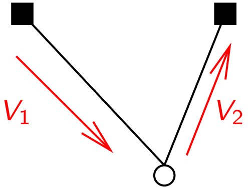
Message passing decoder: Variable nodes



$$x^{(i)} \in \{z^{(i)} + Z\}$$

$$V_2 = V_1 \cap \{z^{(i)} + X\}$$

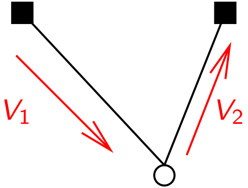
Message passing decoder: Variable nodes



$$x^{(i)} \in \{z^{(i)} + Z\}$$

$$V_2 = V_1 \cap \{z^{(i)} + X\}$$

Message passing decoder: Variable nodes



$$x^{(i)} \in \{z^{(i)} + Z\}$$

$$V_2 = V_1 \cap \{z^{(i)} + X\}$$

Achieving capacity

Capacity achieving ensemble

Variable degree:

$$2$$

Check degree:

$$P_i^{(k)} = \frac{2k(k-1)}{i(i-1)(i-2)}.$$

Not the soliton!

Capacity achieving ensemble

Variable degree:

$$2$$

Check degree:

$$P_i^{(k)} = \frac{2k(k-1)}{i(i-1)(i-2)}.$$

Not the soliton!

Capacity achieving ensemble

Variable degree:

$$2$$

Check degree:

$$P_i^{(k)} = \frac{2k(k-1)}{i(i-1)(i-2)}.$$

Not the soliton!

Capacity achieving ensemble

Variable degree:

$$2$$

Check degree:

$$P_i^{(k)} = \frac{2k(k-1)}{i(i-1)(i-2)}\,.$$

Not the soliton!

Capacity achieving ensemble

Theorem

If $\omega = 1/k$, then the ensemble $(2, P^{(k)})$ has rate equal to the capacity of the rank metric channel and achieves vanishing error probability under message passing decoding.

Further, it achieves vanishing error probability over the erasure channel.

Capacity achieving ensemble

Theorem

If $\omega = 1/k$*, then the ensemble* $(2, P^{(k)})$ *has rate equal to the capacity of the rank metric channel and achieves vanishing error probability under message passing decoding.*
Further, it achieves vanishing error probability over the erasure channel.

Encoding complexity	$O(m\ell^2)$
Decoding complexity	$O(m\ell^2)$
Error probability	$\exp[-\Omega(\gamma^{\mathrm{iter}})]$, $\exp(-\Omega(m,\ell))$

Realistic example (from Chou et al.):

$$\ell \approx 50\,, \qquad m \approx 1700 \qquad (\text{over } \mathbb{F}_{2^8})$$

Encoding complexity	$O(m\ell^2)$
Decoding complexity	$O(m\ell^2)$
Error probability	$\exp[-\Omega(\gamma^{\text{iter}})]$, $\exp(-\Omega(m,\ell))$

Realistic example (from Chou et al.):

$$\ell \approx 50\,, \qquad m \approx 1700 \qquad\qquad (\text{over } \mathbb{F}_{2^8})$$

The magic

1. Fix number of iterations.
2. For large m, message V_i uniformly random conditional on dimension.
3. For large ℓ, output dimension determined by input dimension.
4. For $\omega = 1/k$, only dimension $\ell\omega$ or 0 is possible.

The magic

1. Fix number of iterations.
2. For large m, message V_i uniformly random conditional on dimension.
3. For large ℓ, output dimension determined by input dimension.
4. For $\omega = 1/k$, only dimension $\ell\omega$ or 0 is possible.

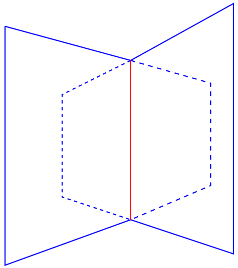
The magic

1. Fix number of iterations.
2. For large m, message V_i uniformly random conditional on dimension.
3. For large ℓ, output dimension determined by input dimension.
4. For $\omega = 1/k$, only dimension $\ell\omega$ or 0 is possible.

The magic

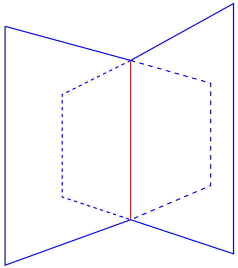
1. Fix number of iterations.
2. For large m, message V_i uniformly random conditional on dimension.
3. For large ℓ, output dimension determined by input dimension.
4. For $\omega = 1/k$, only dimension $\ell\omega$ or 0 is possible.

"For large ℓ, output dimension determined by input dimension"



$$d_{1\cap 2} \approx \max(d_1 + d_2 - d_{\mathrm{amb}}, 0)\,.$$

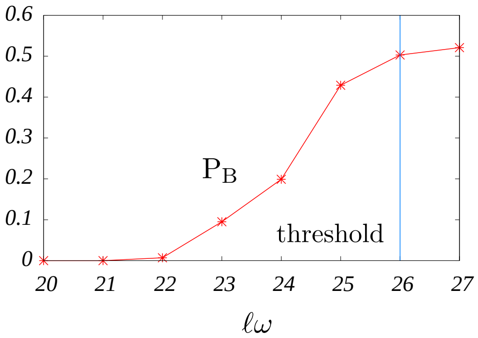
"For large ℓ, output dimension determined by input dimension"



$$d_{1\cap 2} \approx \max(d_1 + d_2 - d_{\mathrm{amb}}, 0)\,.$$

Simulations at small packet sizes

$m = 42$, $\ell = 136$ *(LP optimized degree sequence)*



Conclusion 1

q-ary LDPC's (Davey, MacKay/ Burshtein, Miller/ Rathi, Urbanke)
Mixed outcomes

Exact density evolution for large q

Capacity achieving ensembles

Conclusion 1

q-ary LDPC's (Davey, MacKay/ Burshtein, Miller/ Rathi, Urbanke)
Mixed outcomes

Exact density evolution for large q

Capacity achieving ensembles

Conclusion 2

LDPC codes achieve capacity (under message passing decoding) over the erasure channel (Luby et al. 97) ...

...and the rank metric channel

Conclusion 2

LDPC codes achieve capacity (under message passing decoding) over the erasure channel (Luby et al. 97) . . .

. . . and the rank metric channel

Conclusion 2

LDPC codes achieve capacity (under message passing decoding) over the erasure channel (Luby et al. 97) . . .

. . . and the rank metric channel