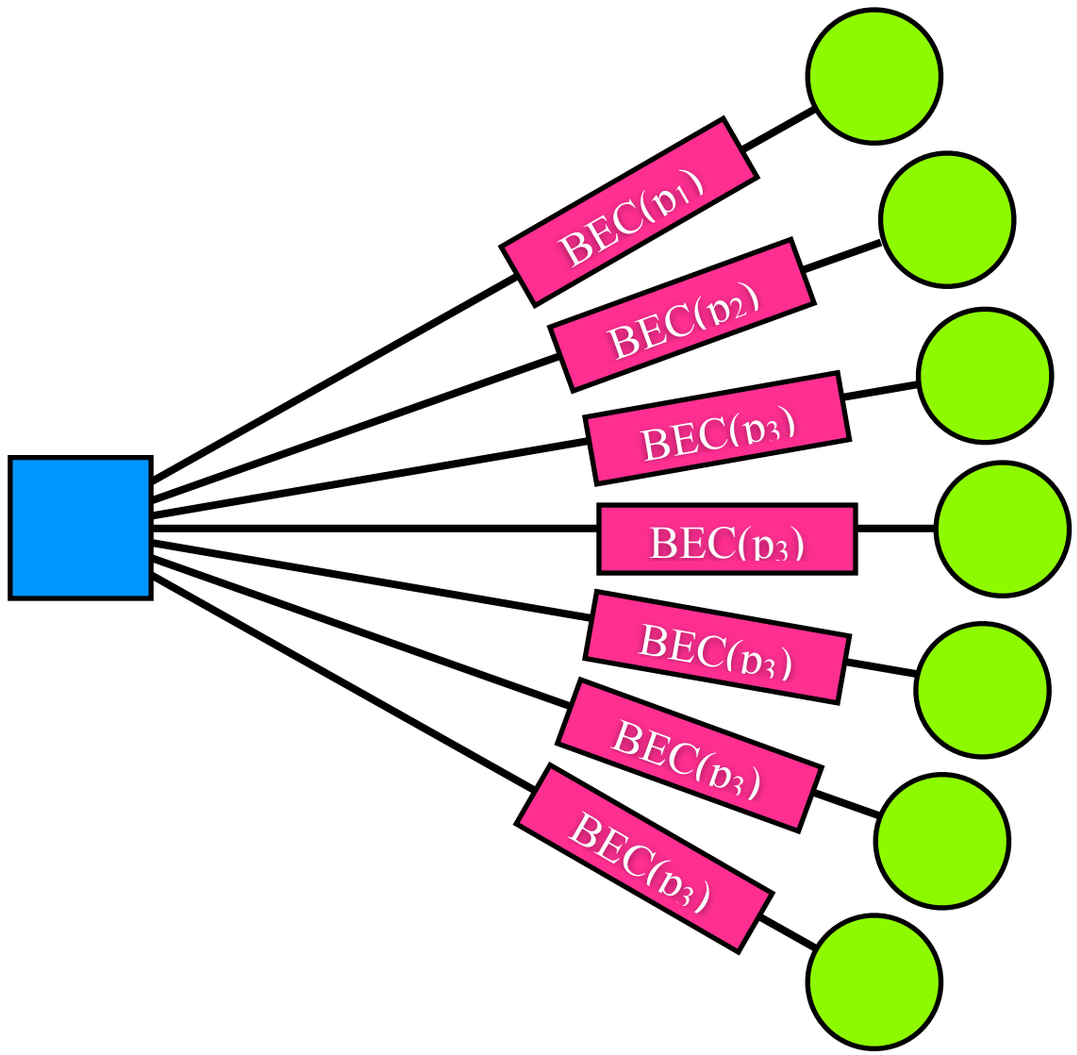
Fountain Codes on Symmetric Channels

Amin Shokrollahi
EPFL

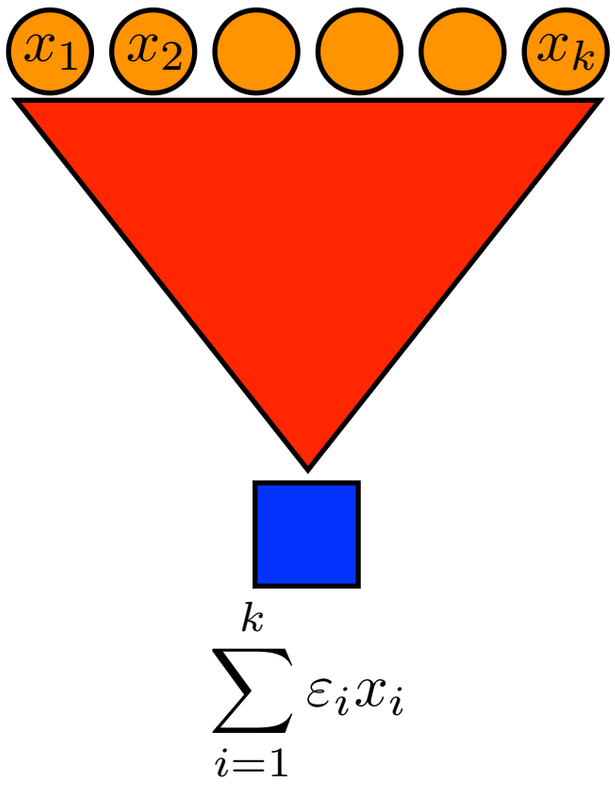
WCS-2009• Dublin

Fountain Codes

Originally designed for transmission on erasure channels with *unknown* probability.



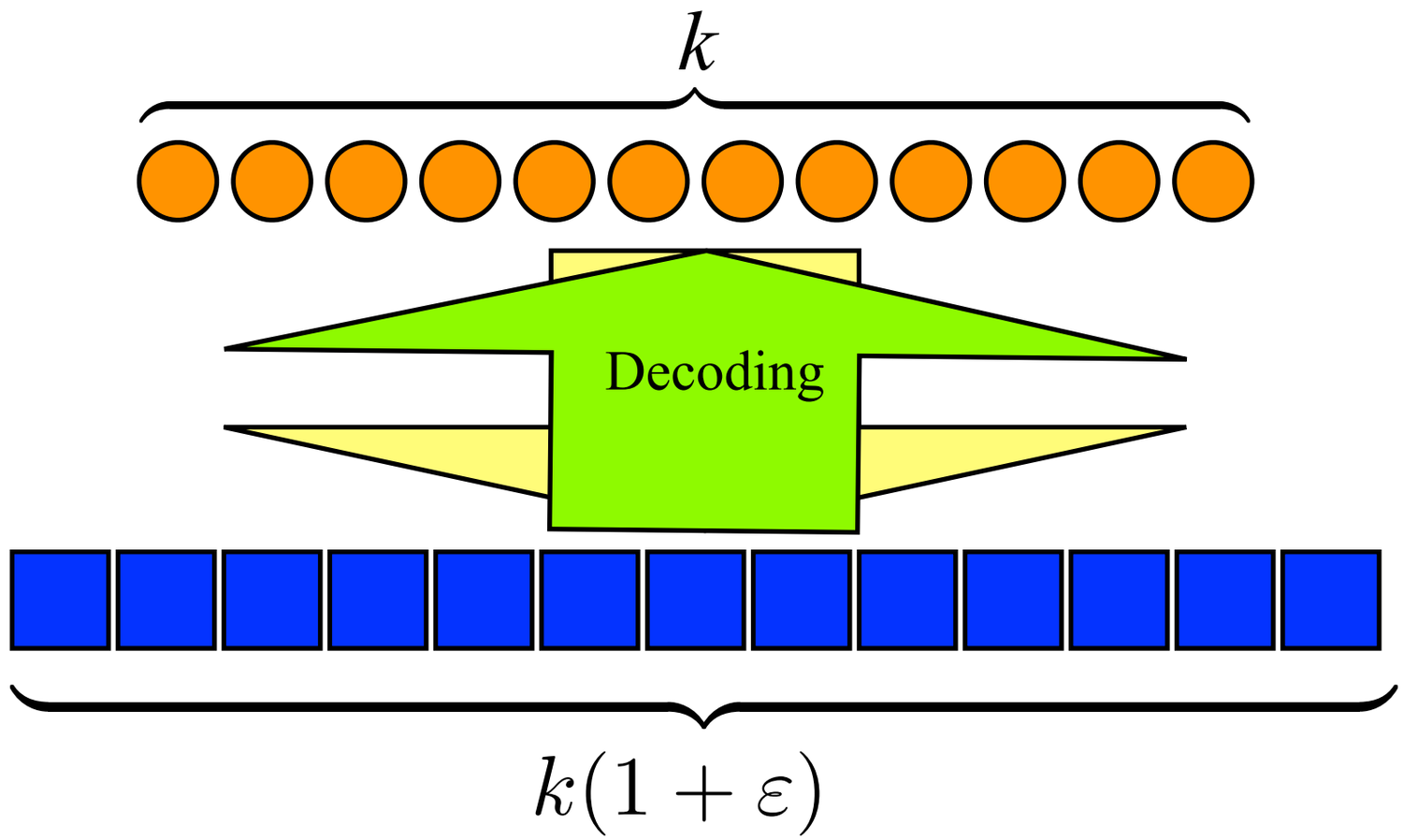
Fountain Codes



$\mathcal{D}$ distribution on $\mathbb{F}_2^k$

$\longrightarrow (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k) \in \mathbb{F}_2^k$

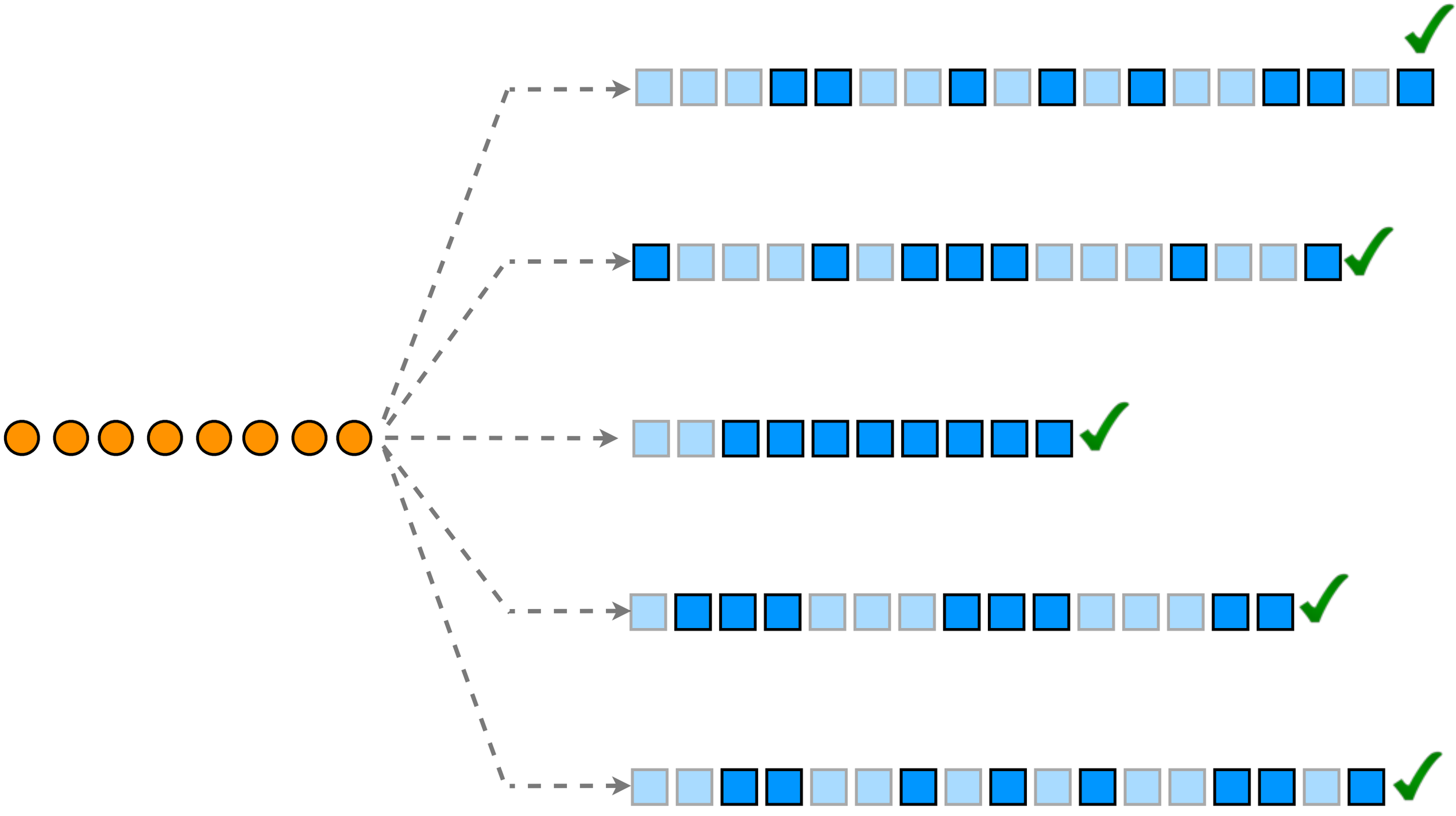
Fountain Codes



Fountain Codes (1998, Luby et al.)

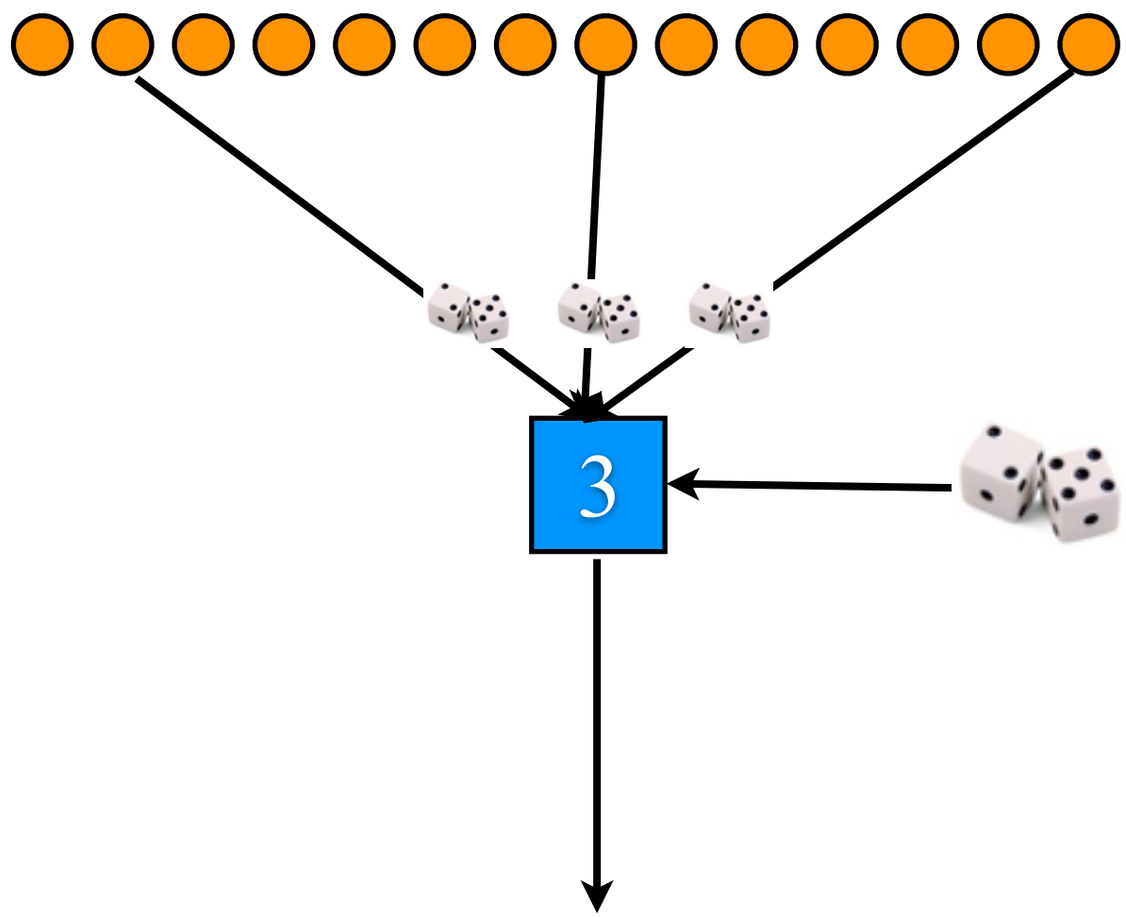
- Output symbols are generated *independently.*
- The k original symbols can be recovered from *any* set of $k(1+\varepsilon)$ output symbols with high probability.

Broadcast with Fountain Codes



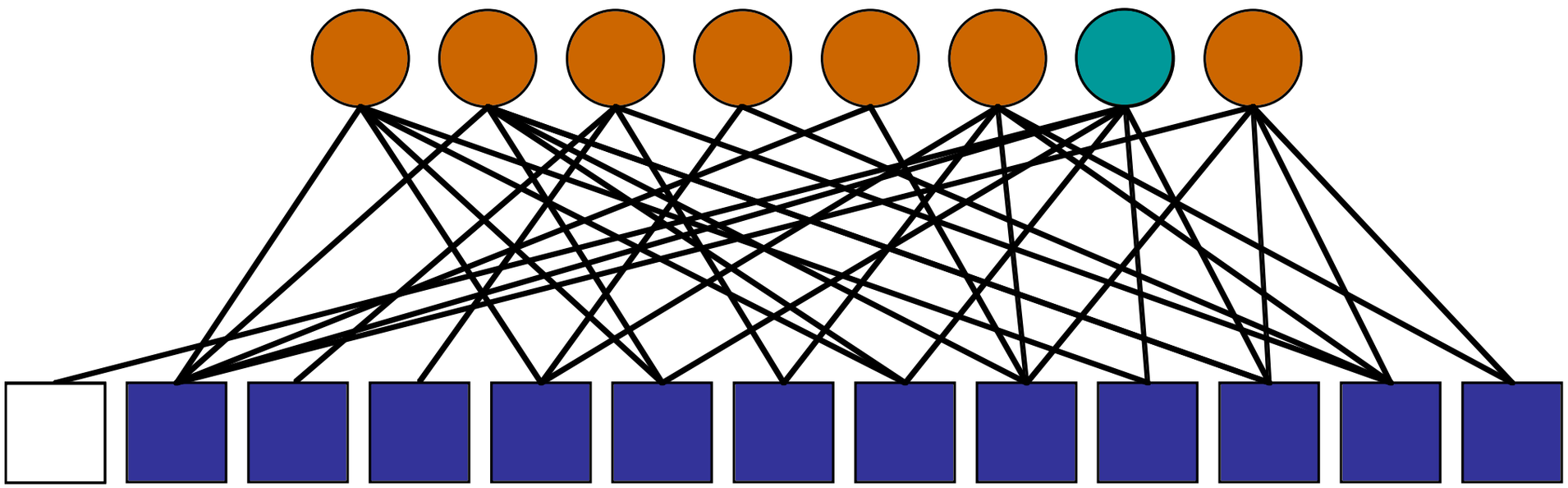
LT-Codes: Encoding (Luby, 1998)

$\Omega_1, \Omega_2, \ldots, \Omega_k$ distribution on $\{1, \ldots, k\}$

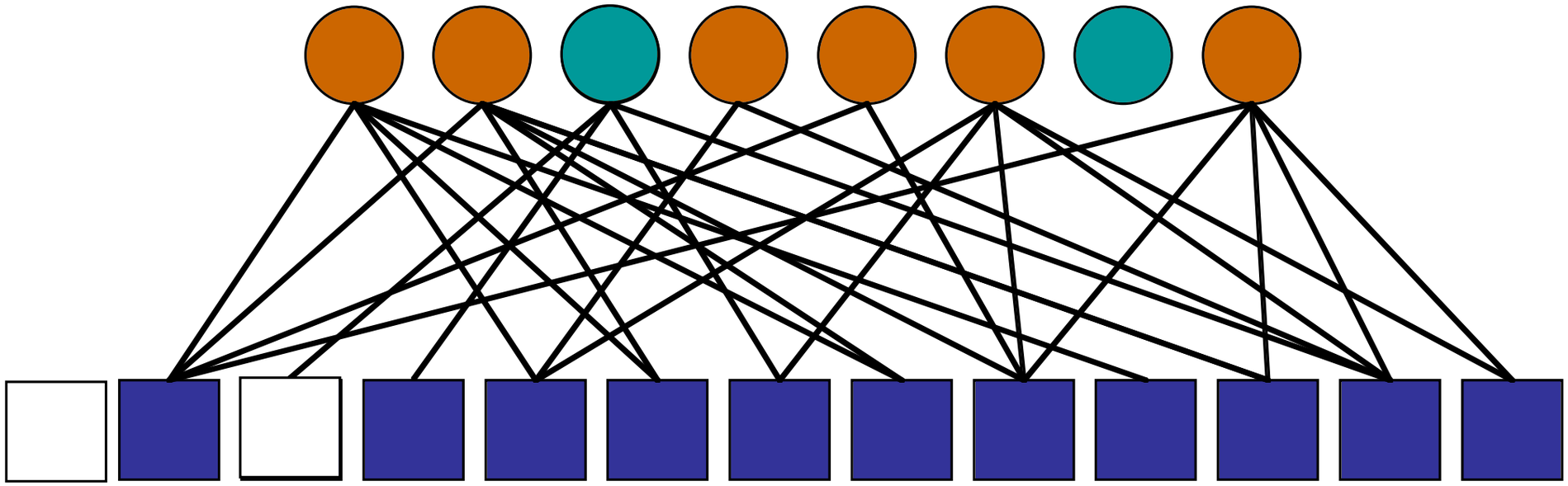


1	Ω_1
2	Ω_2
$\vdots$	$\vdots$
k	Ω_k

LT-Codes: Decoding (Belief Propagation)

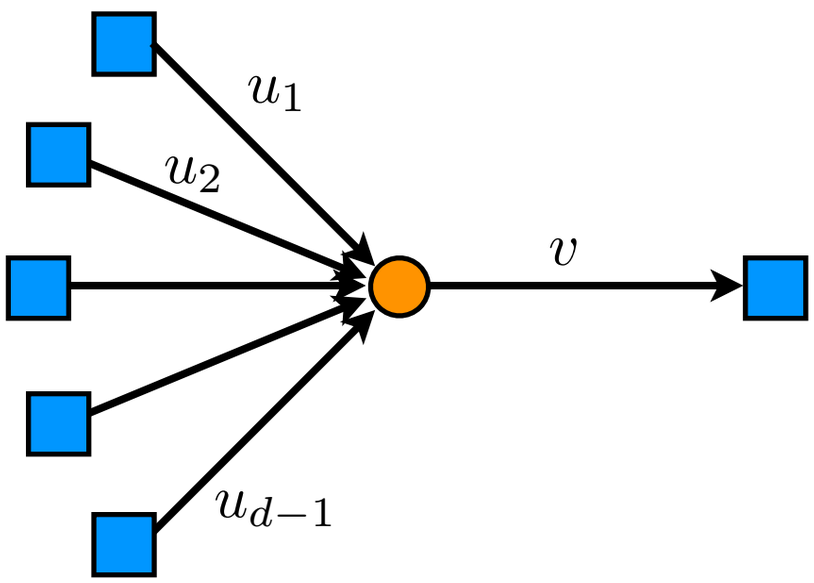


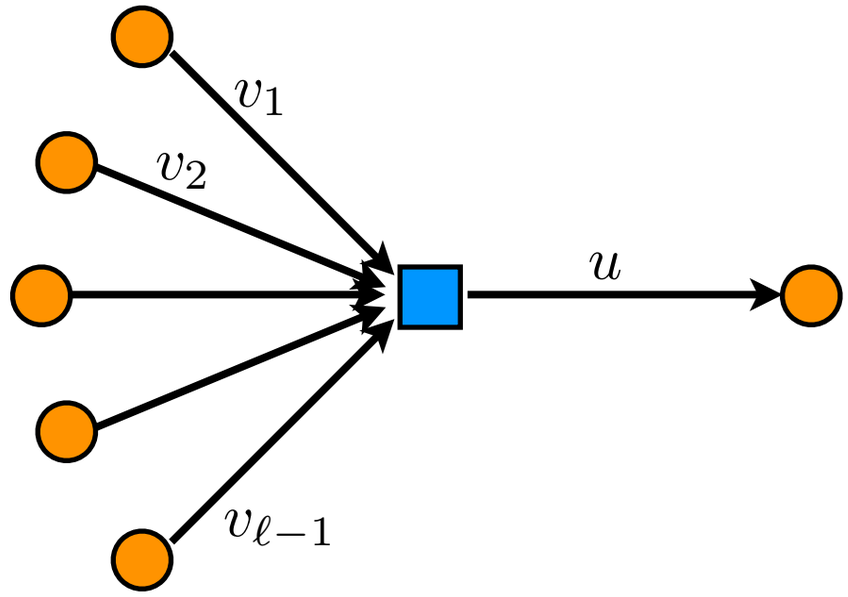
LT-Codes: Decoding (Belief Propagation)



Etc

Belief Propagation





$$v = 1 \iff \exists i\colon\ u_i = 1$$

$$u = 1 \iff \forall i\colon\ v_i = 1$$

Analysis

$$\Omega(x) = \sum_i \Omega_i x^i$$

$$\mathrm{e}^{-(1+\varepsilon)\Omega'(x)} < 1 - x$$

$x = 0$: start of the process
$x = 1$: end of the process

Stability: Start of Decoding

Derivative at 0 of $\mathrm{e}^{-(1+\varepsilon)\Omega'(x)} - 1 + x$ should be negative

$$1 < (1+\varepsilon)\Omega''(0) = (1+\varepsilon)2\Omega_2$$

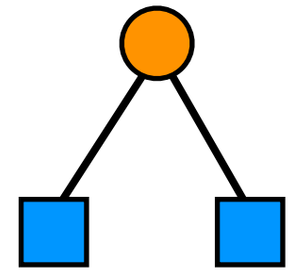
$$\Omega_2 > \frac{1}{2(1+\varepsilon)}$$

$$\Omega_2 \geq \frac{1}{2}$$

Achieving Capacity: Threshold Phenomenon

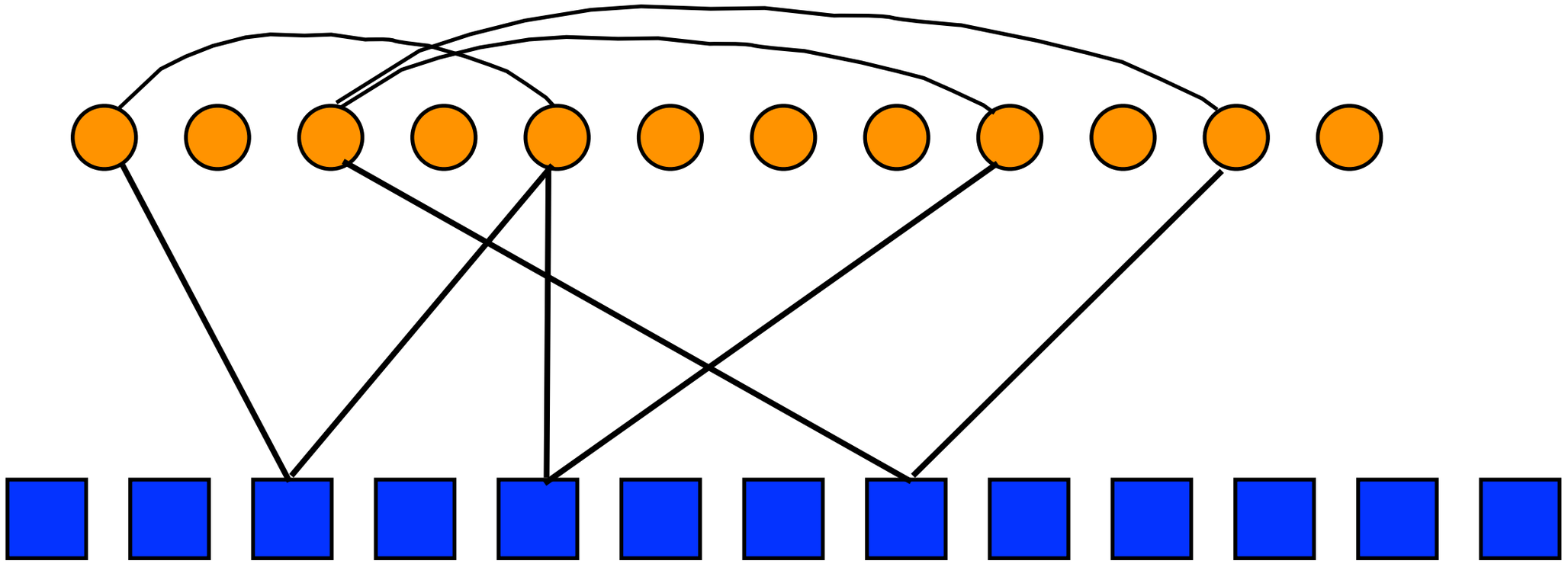
Decoding is possible from any set of $k(1+\varepsilon)$ output symbols.
$\varepsilon \sim 0$

Ω_1 has to go to zero, because information loss otherwise.



Achieving Capacity: Threshold Phenomenon

Induced graph



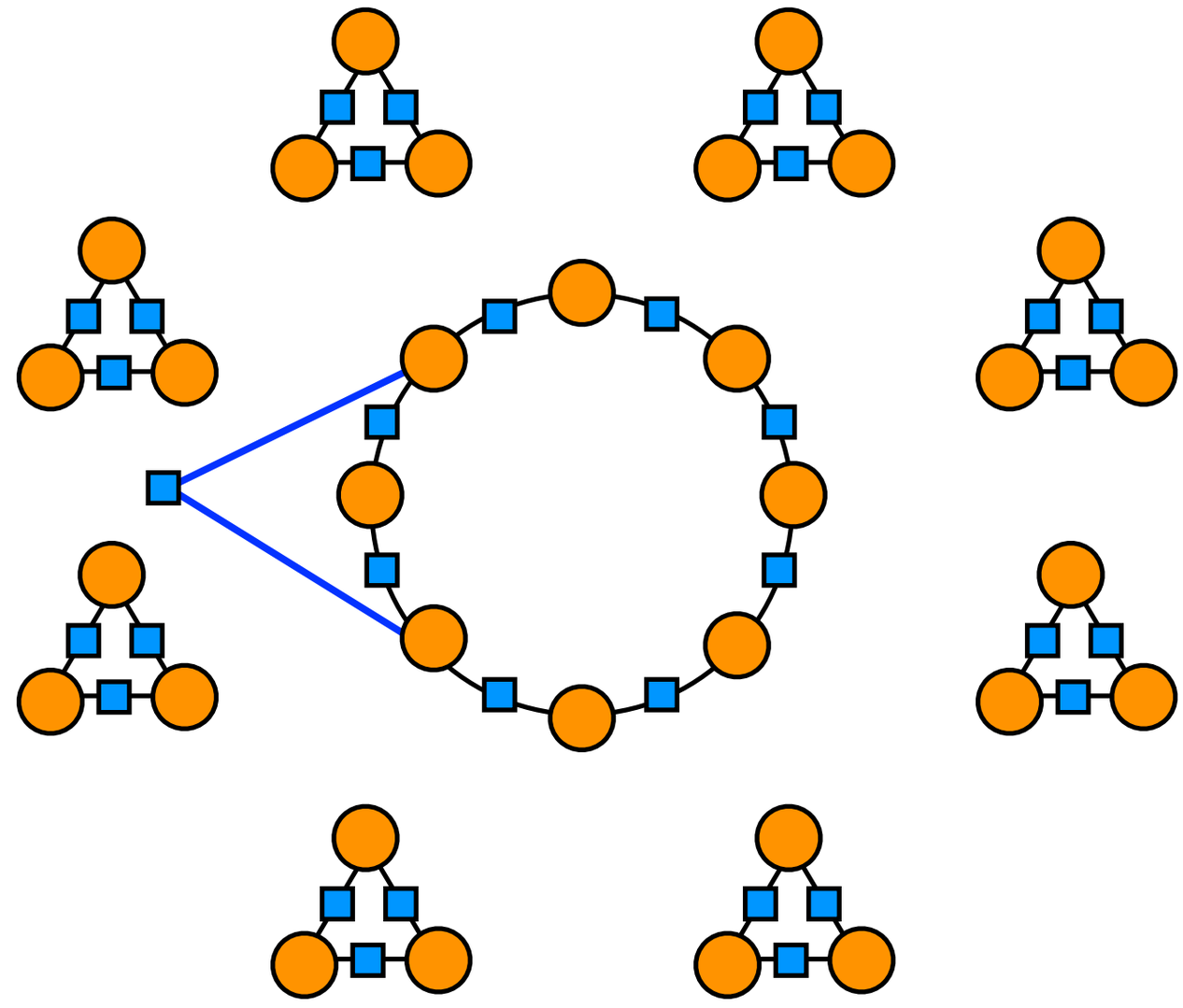
Achieving Capacity: Threshold Phenomenon

Ω_2 should be less than $\frac{1}{2}$

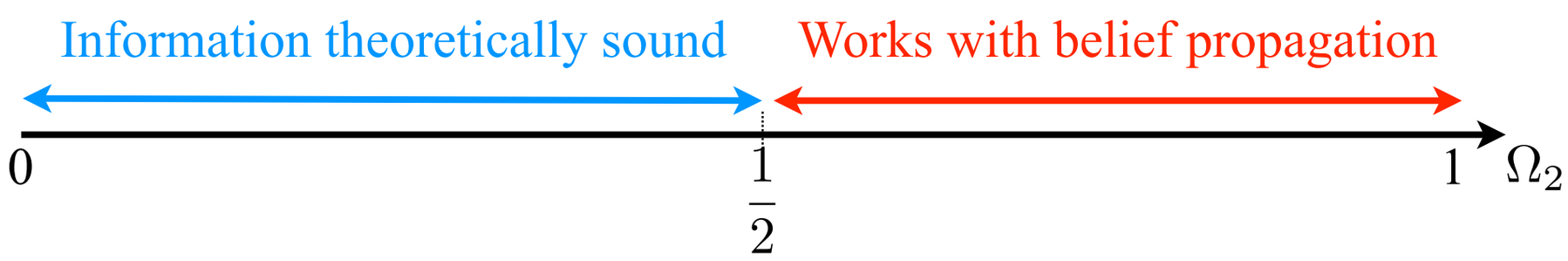
If graph has giant component, then new output symbol of degree 2 has both its neighbors in the component with constant probability.

Hence, information loss.

Giant component appears iff average degree is > 1.



Phase Transition for Ω_2



Achieving Capacity

BP

$$\mathrm{e}^{-\Omega'(x)} = 1 - x$$

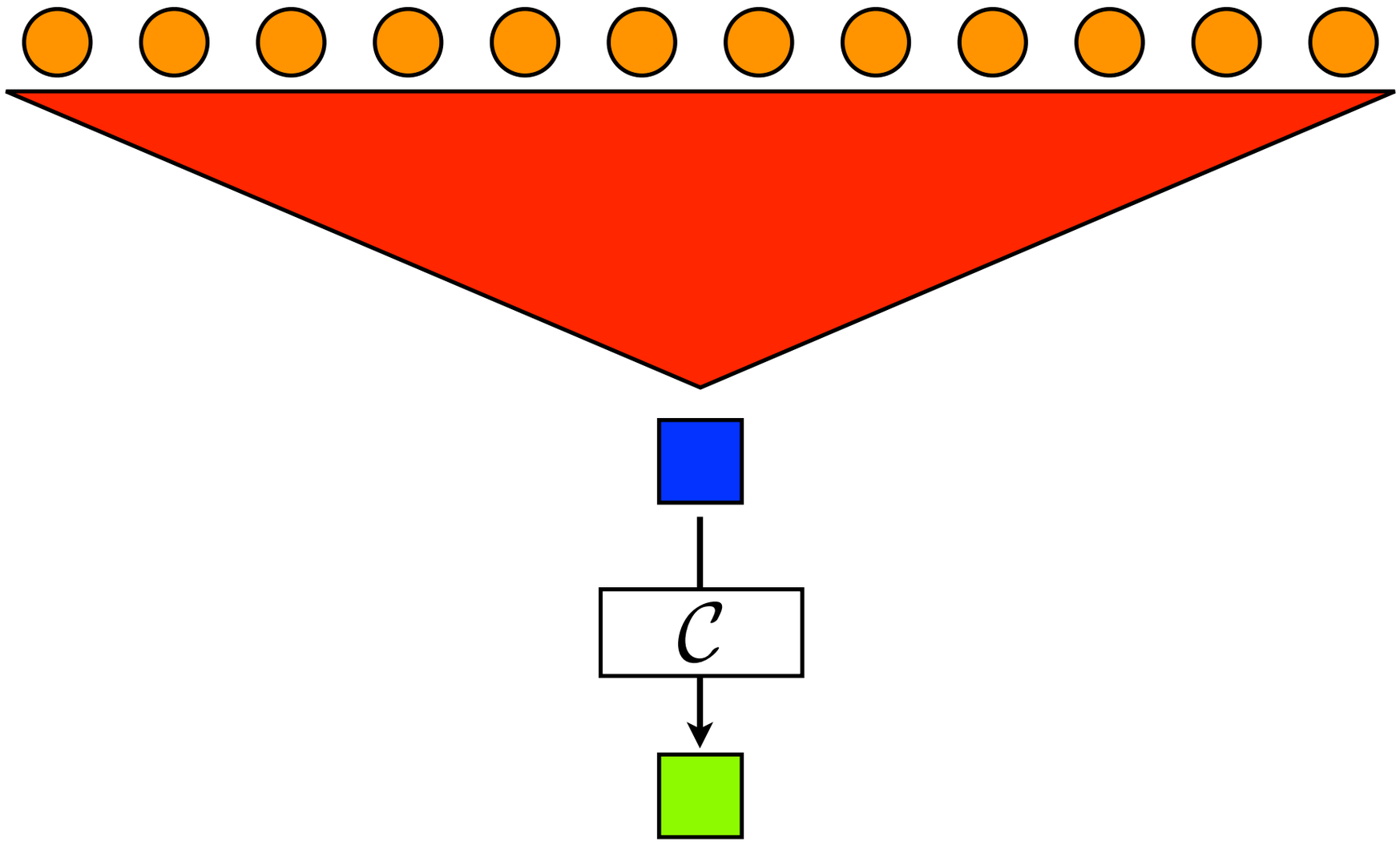
Information Theory

$$\forall \alpha > 0 \colon \frac{\mathrm{d}}{\mathrm{d}x} \Omega(\alpha + (1-\alpha)x)\big|_{x=0} = 1$$

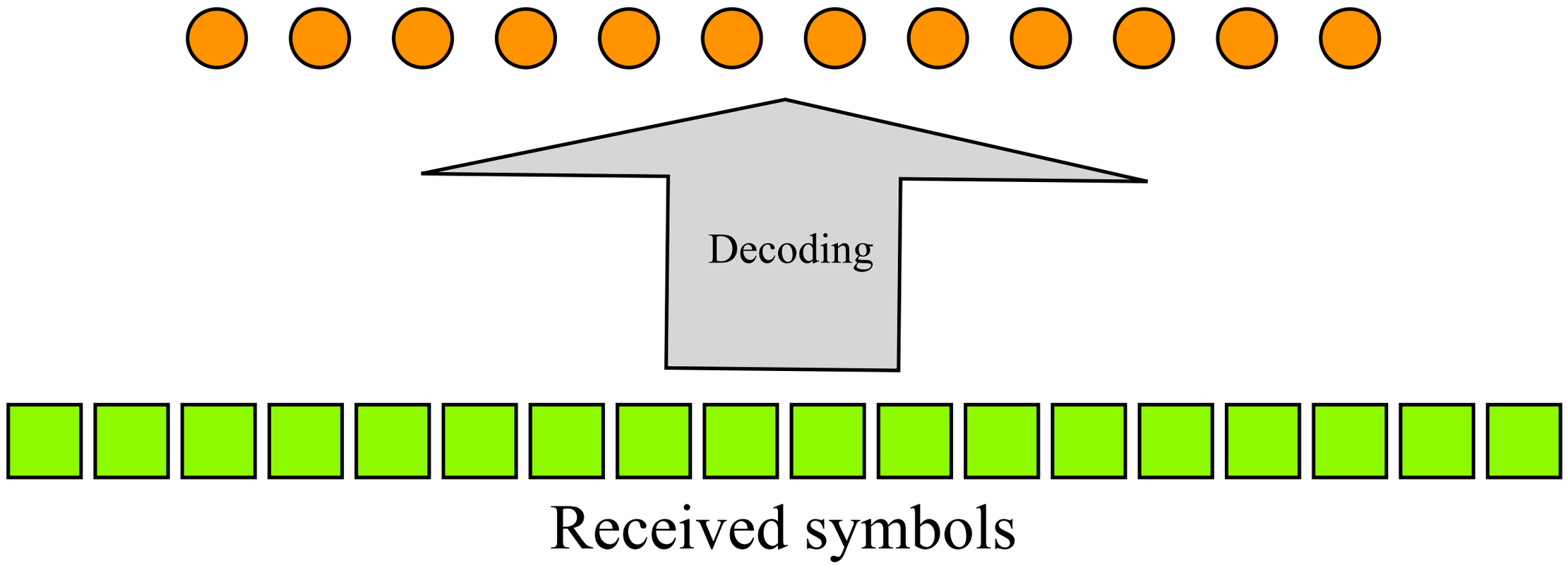
$$\Omega(x) = \frac{x^2}{1 \cdot 2} + \frac{x^3}{2 \cdot 3} + \cdots$$

Symmetric Channels

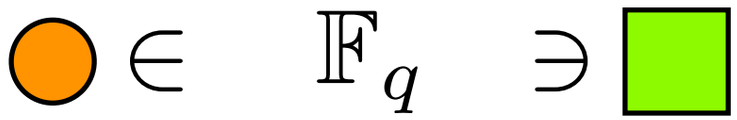
$\mathcal{C}$ symmetric channel



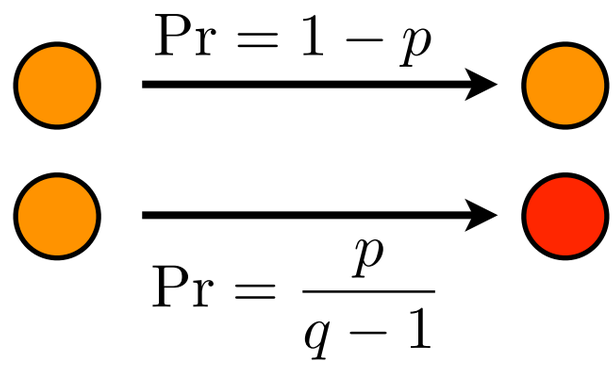
Decoding



Large Alphabet



q large



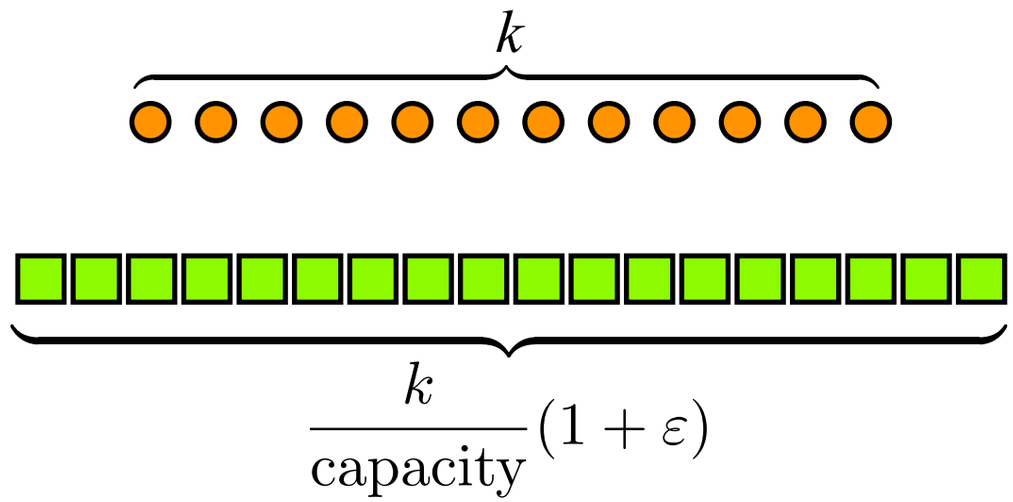
q-ary symmetric channel

Capacity

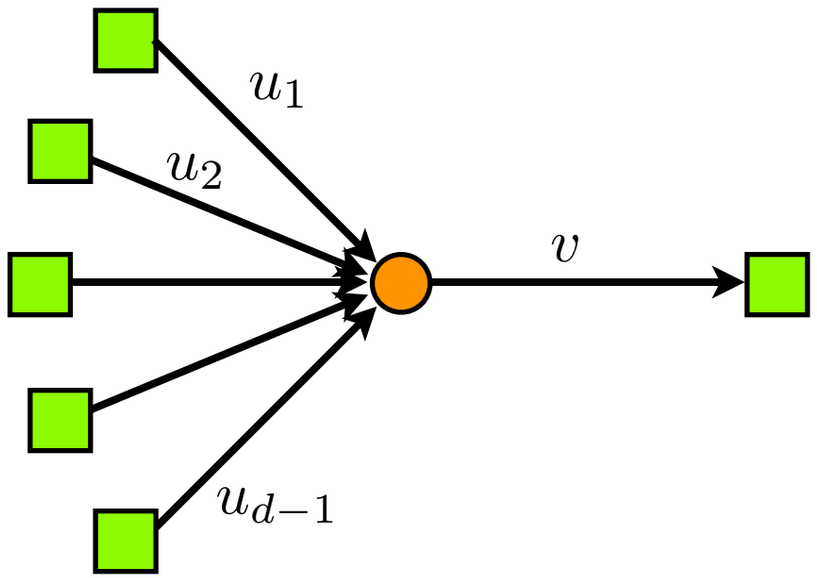
The capacity of this channel is

$$1 + p\log_q(p) + (1-p)\log_q(1-p) - p\log_q(q-1)$$

$$\sim 1 - p$$

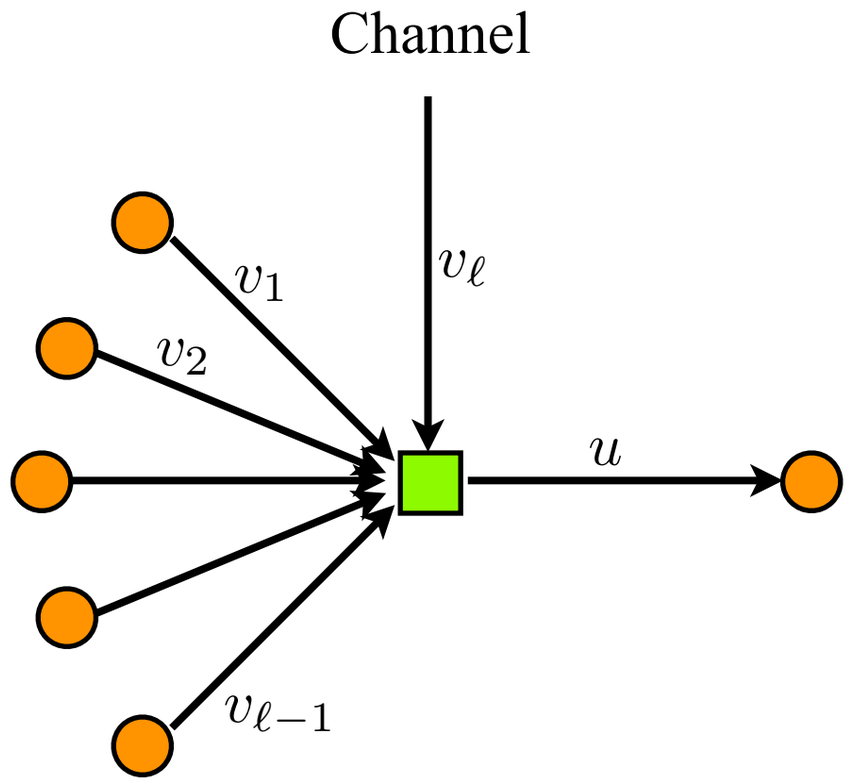


Simple Double Verification



$$v = \begin{cases} \alpha & \text{if } \exists i, j : \alpha = u_i = u_j \\ \text{erasure} & \text{otherwise.} \end{cases}$$

Simple Double Verification



$$u = \begin{cases} \sum_{i=1}^{\ell} v_i & \text{if } \forall i\colon v_i \neq \text{erasure} \\ \text{erasure} & \text{otherwise.} \end{cases}$$

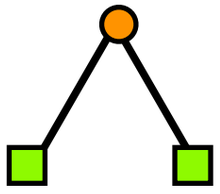
Simple Double Verification

(Karp-Luby-S, 05)

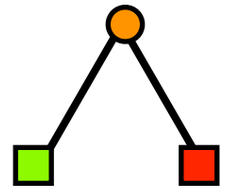
Asymptotically, the overhead ε of this algorithm is

$$2 + \frac{1}{\mathrm{e}} - \frac{\mathrm{e}}{2} \simeq 1.00873$$

Combinatorial View



Verified

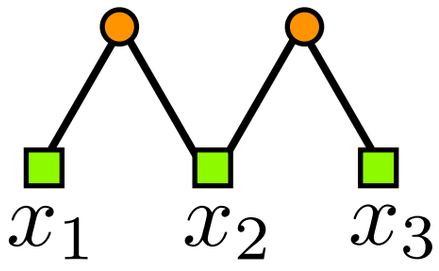


Unverified

To verify ●, it needs to be connected to two correctly transmitted ■.

Remove verified ● from the graph, and continue.

More Sophisticated Versions



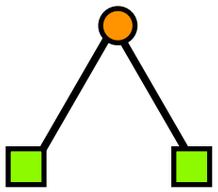
$x_1 + x_2 + x_3 = 0$?

Verified path of length 4

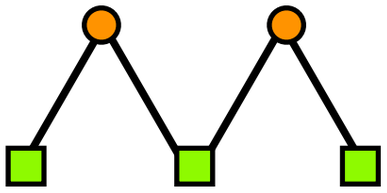
Find a verified path of length 4 and remove it from graph.

Need three correctly transmitted ■ per two ●. Overhead is roughly 3/2-1 = 1/2.

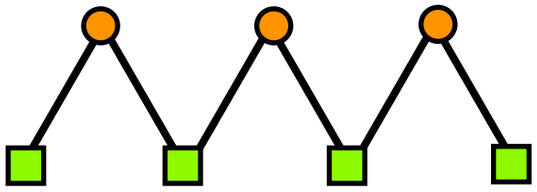
More Sophisticated Versions



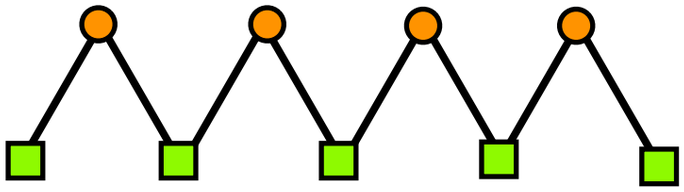
Verified path of length 2



Verified path of length 4



Verified path of length 6



Verified path of length $2n$

Advanced Double Verification

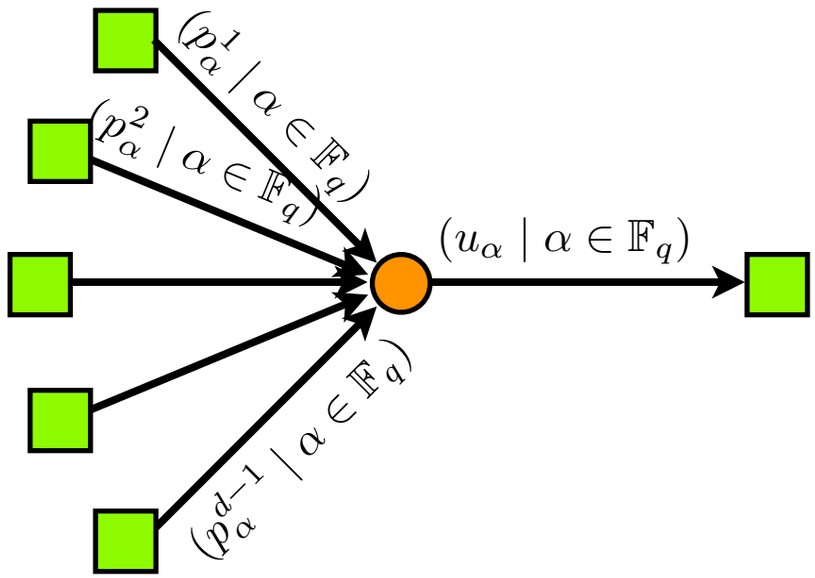
Want lots of verified paths in the graph.

Graph on correctly transmitted output symbols of degree 2 must have a giant component.

Ω_2 is equal to $\frac{1}{2}$ in the limit.

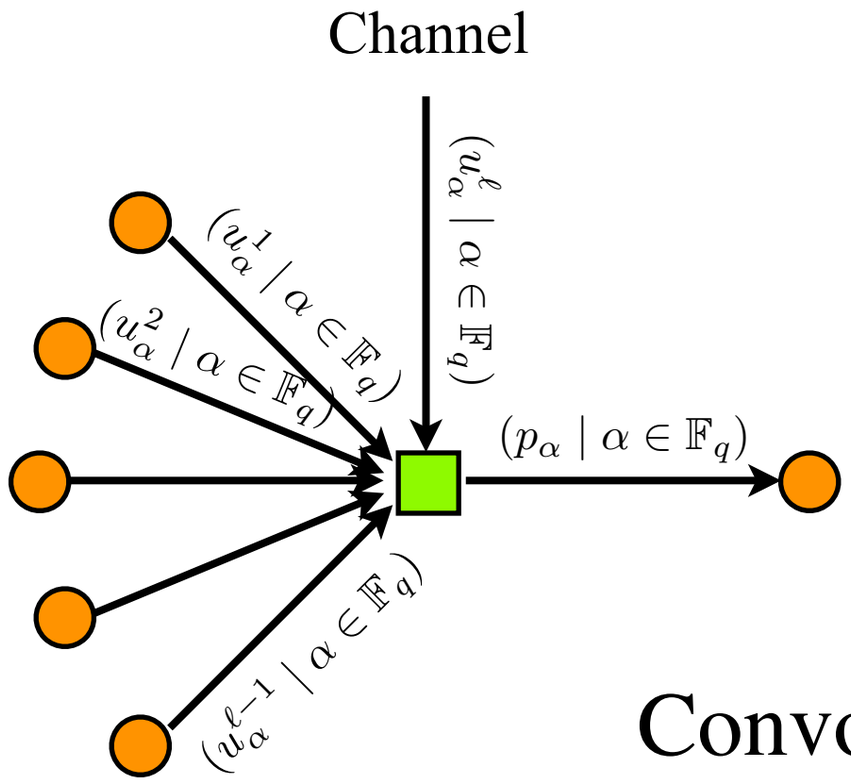
Same capacity-achieving distribution as in the case of the erasure channel.

Belief Propagation



$$u_\alpha = \frac{\prod_{i=1}^{d-1} p_\alpha^i}{\sum_\alpha \prod_{i=1}^{d-1} p_\alpha^i}$$

Belief Propagation



Convolution

$$(p_\alpha \mid \alpha \in \mathbb{F}_q) = \bigotimes_{i=1}^{\ell} (u_\alpha^i \mid \alpha \in \mathbb{F}_q)$$

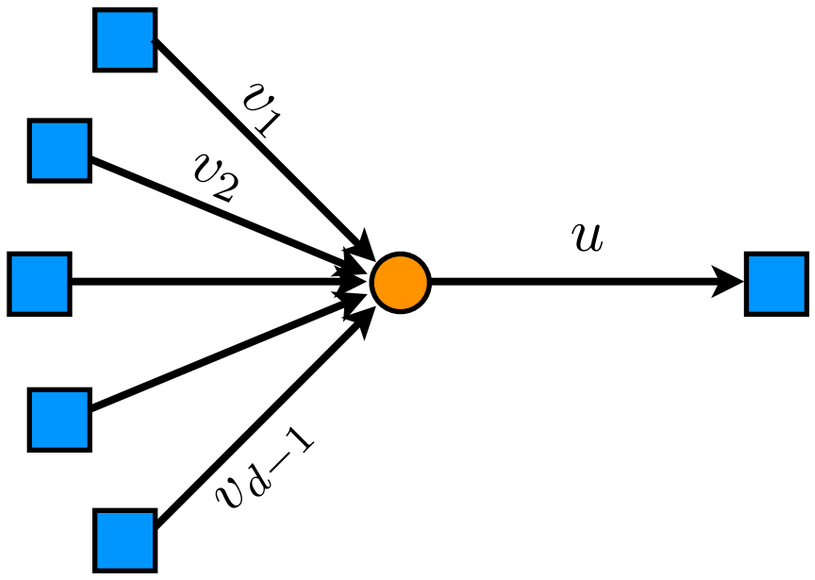
Large Alphabets

Belief propagation is computationally inefficient for large alphabets, in part because of the convolutions.

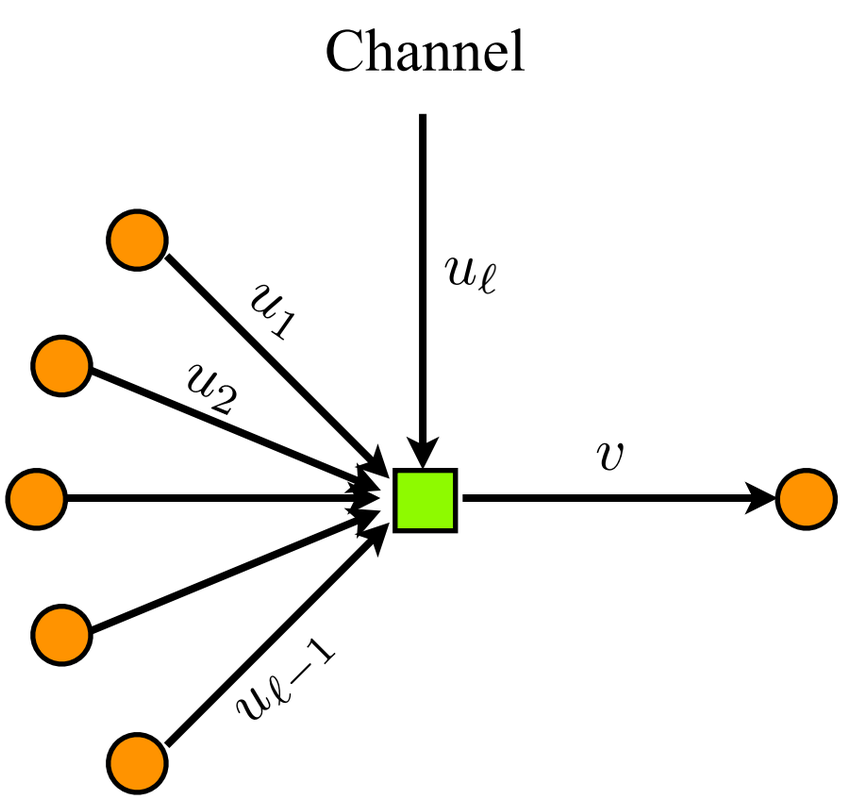
More efficient approximations have been proposed, but for large alphabets, they are not competitive with double verification type algorithms.

How about small alphabets (binary)?

Binary Alphabet

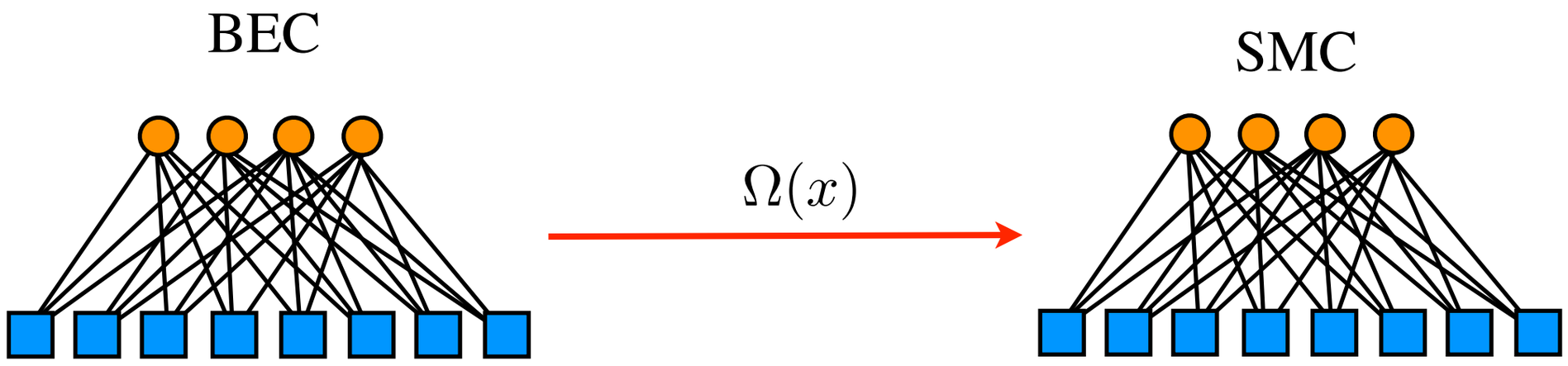


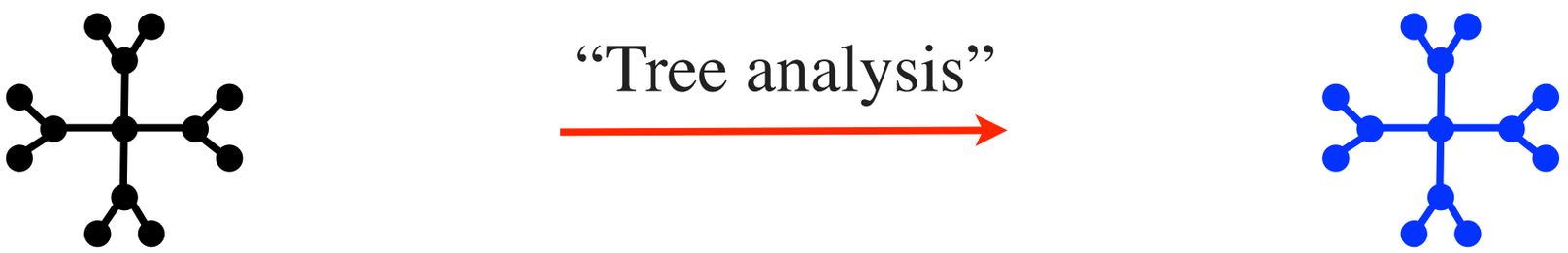
$$u = \sum_{i=1}^{d-1} v_i$$



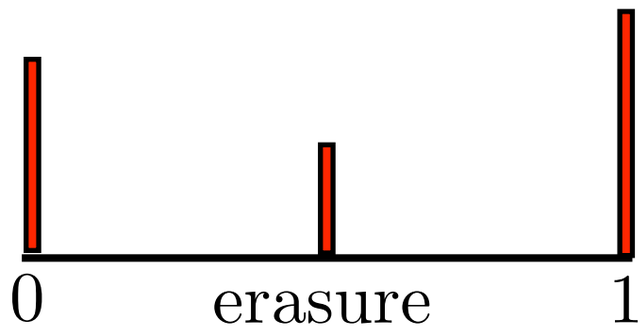
$$\tanh(v/2) = \prod_{i=1}^{\ell} \tanh(u_i)$$

A lot Carries Over from the Erasure Case

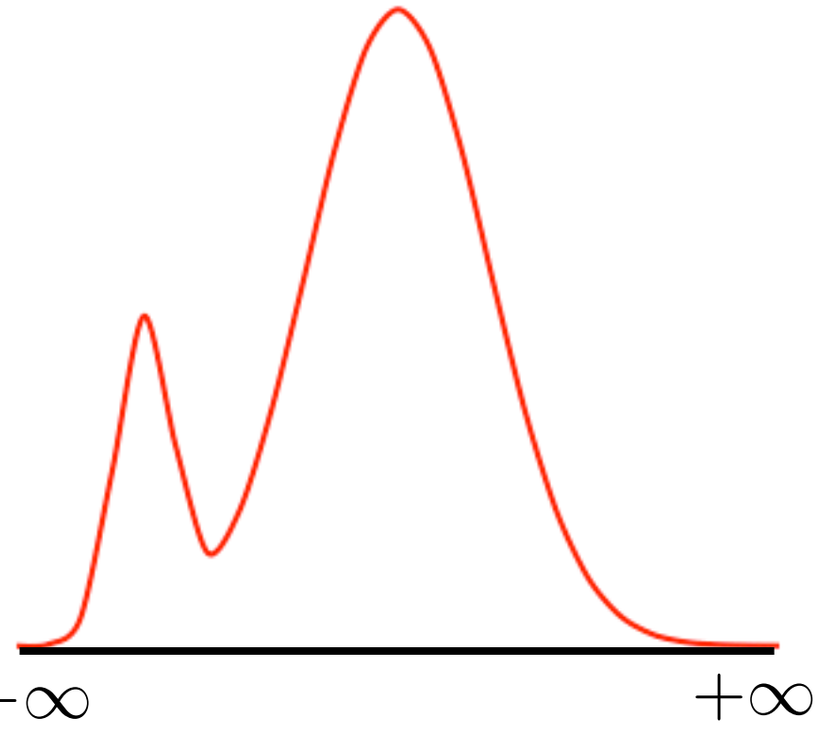




Message Passing Analysis



BEC



SMC

"Density" of messages passed

Density Evolution

$$p_{i+1} = \mathrm{e}^{-(1+\varepsilon)\Omega'(1-p_i)}$$

Probability of erasure at round i

$$f_{i+1} = \Gamma^{-1}\left(\mathrm{e}_{\otimes}^{-(1+\varepsilon)f_0 \otimes \Omega'_{\otimes}(\Gamma(f_i))}\right)$$

Density of messages passed at round i

Stability: Algorithmic

$$p_{i+1} = \mathrm{e}^{-(1+\varepsilon)\Omega'(1-p_i)}$$

Taylor expansion at p=1 gives $\Omega_2 > \dfrac{1}{2(1+\varepsilon)}$

$$f_{i+1} = \Gamma^{-1}\left(\mathrm{e}_{\otimes}^{-(1+\varepsilon)f_0 \otimes \Omega'_{\otimes}(\Gamma(f_i))}\right)$$

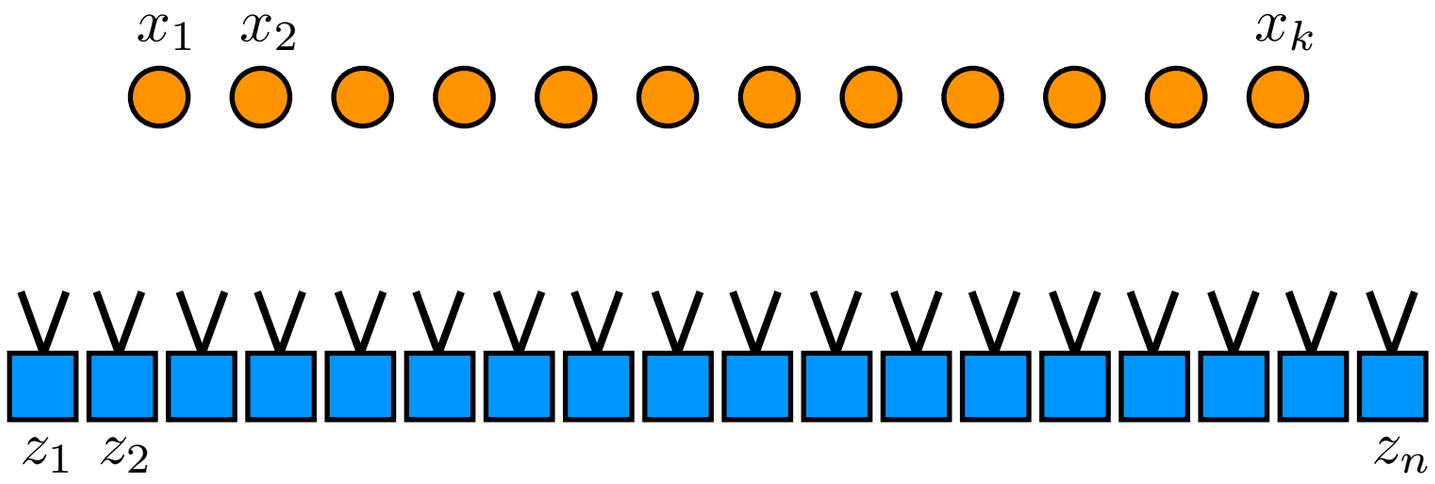
Directional derivative at Δ_0 in direction of channel noise gives

$$\Omega_2 > \frac{1}{2(1+\varepsilon)\Pi(\mathcal{C})}$$

Examples

$\mathcal{C}$	$\Pi(\mathcal{C})$
BEC	1
BSC(p)	$\dfrac{1-h(p)}{(1-2p)^2}$
AWGN $\left(\sqrt{\dfrac{2}{m}}\right)$	$\dfrac{1-\dfrac{1}{2\sqrt{\pi m}}\displaystyle\int_{-\infty}^{\infty}\log_2\left(1+e^{-x}\right)e^{-\frac{(x-m)^2}{4m}}dx}{\dfrac{1}{2\sqrt{\pi m}}\displaystyle\int_{-\infty}^{\infty}\tanh\left(\dfrac{x}{2}\right)e^{-\frac{(x-m)^2}{4m}}dx},$

Stability: Information Theoretic, BEC

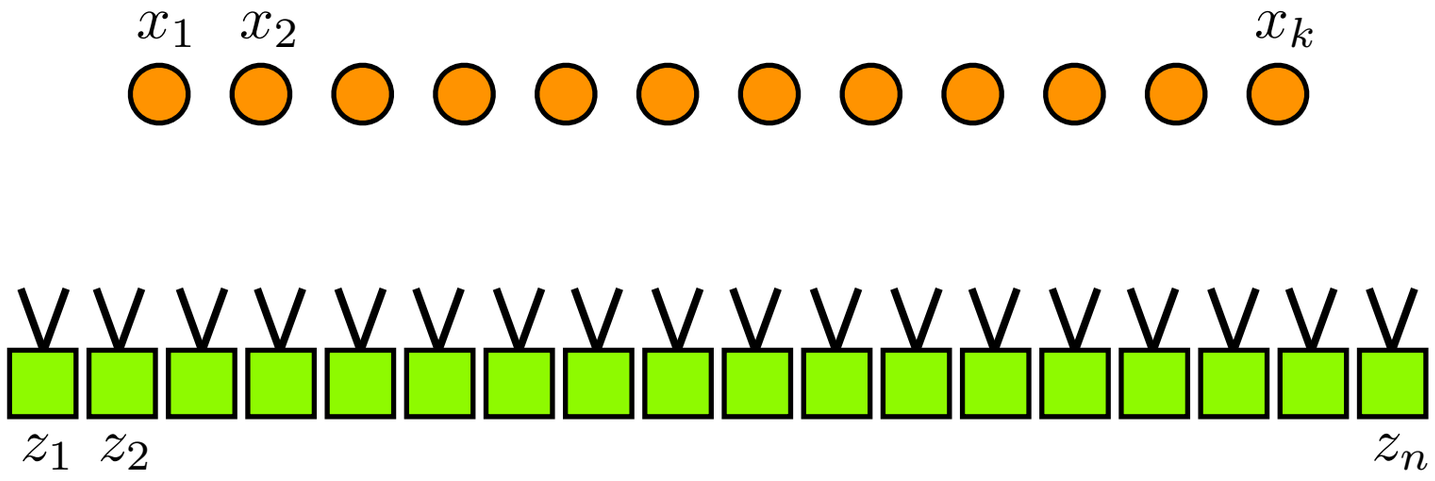


$$I(x;z) \sim n \implies \frac{n}{k} < \frac{1}{2}$$

$$\implies \Omega_2 < \frac{1}{2}$$

Stability: Information Theoretic, SMC

Etessami-S, 06



$$I(x;z) \sim n\mathrm{Cap}(\mathcal{C}) \implies \frac{n}{k} < \frac{1}{2\Pi(\mathcal{C})}$$

$$\implies \Omega_2 < \frac{1}{2\Pi(\mathcal{C})}$$

Achieving Capacity?