Polar Codes

Ruediger Urbanke, EPFL

February 19th, 2010

For the most recent version of these slides visit
http://ipg.epfl.ch/doku.php?id=en:publications:mct

Modern Coding Theory
Cambridge University Press

Polar Codes: Summary

Polar Codes: Summary

Erdal Arikan, ISIT 2007

Polar Codes: Summary

Erdal Arikan, ISIT 2007

very general phenomenon

Polar Codes: Summary

Erdal Arikan, ISIT 2007

very general phenomenon

information theoretic view why codes work

Polar Codes: Summary

Erdal Arikan, ISIT 2007

very general phenomenon

information theoretic view why codes work

first “low complexity” scheme which provably achieves the capacity for a fairly wide array of channels

Polar Codes: Summary

Erdal Arikan, ISIT 2007

very general phenomenon

information theoretic view why codes work

first “low complexity” scheme which provably achieves the capacity for a fairly wide array of channels

many possible variations on the theme

Polar Codes: Summary

Erdal Arikan, ISIT 2007

very general phenomenon

information theoretic view why codes work

first “low complexity” scheme which provably achieves the capacity for a fairly wide array of channels

many possible variations on the theme

codes not only good for channel coding; work equally well for source coding and more complicated scenarios

References

arXiv:0807.3917 [ps, pdf, other]

Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels

Erdal Arikan

Comments: 49 pages, 14 figures. Submitted to IEEE Transactions on Information Theory, Oct. 2007

Subjects: **Information Theory (cs.IT)**

arXiv:0807.3806 [ps, pdf, other]

On the Rate of Channel Polarization

Erdal Arikan, Emre Telatar

Comments: 10 pages

Subjects: **Information Theory (cs.IT)**

arXiv:0901.0536 [ps, pdf, other]

Polar Codes: Characterization of Exponent, Bounds, and Constructions

Satish Babu Korada, Eren Sasoglu, Rudiger Urbanke

Comments: Submitted to IEEE Transactions on Information Theory, minor updates

Subjects: **Information Theory (cs.IT)**

arXiv:0901.2207 [ps, pdf, other]

Performance and Construction of Polar Codes

Ryuhei Mori, Toshiyuki Tanaka

Comments: 5 pages, 3 figures, submitted to ISIT2009

Subjects: **Information Theory (cs.IT)**

arXiv:0903.0307 [ps, pdf, other]

Polar Codes are Optimal for Lossy Source Coding

Satish Babu Korada, Rudiger Urbanke

Comments: 15 pages, submitted to Transactions on Information Theory

Subjects: **Information Theory (cs.IT)**

arXiv:0908.0302 [ps, pdf, other]

Polarization for arbitrary discrete memoryless channels

Eren Sasoglu, Emre Telatar, Erdal Arikan

Comments: 12 pages

Subjects: **Information Theory (cs.IT)**

arXiv:0908.0302 [ps, pdf, other]

Polarization for arbitrary discrete memoryless channels

Eren Sasoglu, Emre Telatar, Erdal Arikan

Comments: 12 pages

Subjects: **Information Theory (cs.IT)**

arXiv:0901.2370 [ps, pdf, other]

Polar Codes for Channel and Source Coding

Nadine Hussami, Satish Babu Korada, Rudiger Urbanke

Comments: submitted to ISIT

Subjects: **Information Theory (cs.IT)**

arXiv:1001.2766 [ps, pdf, other]

On the scaling of Polar codes: I. The behavior of polarized channels

S. Hamed Hassani, Rudiger Urbanke

Comments: Submitted to ISIT 2010

Subjects: **Information Theory (cs.IT)**

arXiv:1001.2545 [ps, pdf, other]

Concatenated Polar Codes

Mayank Bakshi, Sidharth Jaggi, Michelle Effros

Subjects: **Information Theory (cs.IT)**

arXiv:1001.0210 [ps, pdf, other]

Achieving the Secrecy Capacity of Wiretap Channels Using Polar Codes

Hessam Mahdavifar, Alexander Vardy

Comments: 5 pages, submitted to the IEEE Symposium on Information Theory

Subjects: **Information Theory (cs.IT)**; Cryptography and Security (cs.CR)

arXiv:1001.2662 [ps, pdf, other]

Channel Polarization on q-ary Discrete Memoryless Channels

Ryuhei Mori, Toshiyuki Tanaka

Comments: 5 pages, submitted to ISIT2010

Subjects: **Information Theory (cs.IT)**

arXiv:1002.0777 [ps, pdf, other]

Polar Codes for the m-User MAC and Matroids

Emmanuel Abbe, Emre Telatar

Subjects: **Information Theory (cs.IT)**; Discrete Mathematics (cs.DM); Combinatorics (m

arXiv:0907.3291 [ps, pdf, other]

The Compound Capacity of Polar Codes

S. Hamed Hassani, Satish Babu Korada, Ruediger Urbanke

Comments: 5 pages

Subjects: **Information Theory (cs.IT)**

References

arXiv:0807.3917 [ps, pdf, other]

Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels

Erdal Arikan

Comments: 49 pages, 14 figures. Submitted to IEEE Transactions on Information Theory, Oct. 2007

Subjects: **Information Theory (cs.IT)**

arXiv:0807.3806 [ps, pdf, other]

On the Rate of Channel Polarizatior

Erdal Arikan, Emre Telatar

Comments: 10 pages

Subjects: **Information Theory (cs.IT)**

arXiv:0901.0536 [ps, pdf, other]

Polar Codes: Characterization of Ex

Satish Babu Korada, Eren Sasoglu, Rudiger Url

Comments: Submitted to IEEE Transactions on Informa

Subjects: **Information Theory (cs.IT)**

arXiv:0901.2207 [ps, pdf, other]

Performance and Construction of P

Ryuhei Mori, Toshiyuki Tanaka

Comments: 5 pages, 3 figures, submitted to ISIT2009

Subjects: **Information Theory (cs.IT)**

arXiv:0903.0307 [ps, pdf, other]

Polar Codes are Optimal for Lossy S

Satish Babu Korada, Rudiger Urbanke

Comments: 15 pages, submitted to Transactions on In

Subjects: **Information Theory (cs.IT)**

arXiv:0908.0302 [ps, pdf, other]

Polarization for arbitrary discrete m

Eren Sasoglu, Emre Telatar, Erdal Arikan

Comments: 12 pages

Subjects: **Information Theory (cs.IT)**

arXiv:0908.0302 [ps, pdf, other]

Polarization for arbitrary discrete memoryless channels

Eren Sasoglu, Emre Telatar, Erdal Arikan

Comments: 12 pages

Subjects: **Information Theory (cs.IT)**

arXiv:0901.2370 [ps, pdf, other]

Polar Codes for Channel and Source Coding

Nadine Hussami, Satish Babu Korada, Rudiger Urbanke

Comments: submitted to ISIT

Subjects: **Information Theory (cs.IT)**

or of polarized channels

ps, pdf, other]

ted Polar Codes

ni, Sidharth Jaggi, Michelle Effros

nation Theory (cs.IT)**

Wiretap Channels Using Polar Codes

on Information Theory

nd Security (cs.CR)

-ary Discrete Memoryless Channels

10

1-User MAC and Matroids

tar

s.IT); Discrete Mathematics (cs.DM); Combinatorics (m

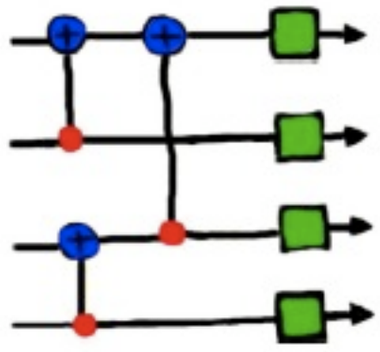
The Compound Capacity of Polar Codes

S. Hamed Hassani, Satish Babu Korada, Ruediger Urbanke

Comments: 5 pages

Subjects: **Information Theory (cs.IT)**

Polar Codes for Channel and Source Coding



Satish Babu Korada

Submitted for the degree of Docteur ès Sciences
Ecole Polytechnique Fédérale de Lausanne

May 20, 2009

Codes from Kronecker Product of G_2

Codes from Kronecker Product of G_2

$$G_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

Codes from Kronecker Product of G_2

$$G_2^{\otimes 2} = \begin{bmatrix} G_2 & 0 \\ G_2 & G_2 \end{bmatrix}$$

Codes from Kronecker Product of G_2

$$G_2^{\otimes 2} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

Codes from Kronecker Product of G_2

$$G_2^{\otimes 3} = \begin{bmatrix} G_2 & 0 & 0 & 0 \\ G_2 & G_2 & 0 & 0 \\ G_2 & 0 & G_2 & 0 \\ G_2 & G_2 & G_2 & G_2 \end{bmatrix}$$

Codes from Kronecker Product of G_2

$$G_2^{\otimes 3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Codes from Kronecker Product of G_2

length $N = 2^m$, $m \in \mathbb{N}$

$$G_2^{\otimes 3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Codes from Kronecker Product of G_2

length $N = 2^m$, $m \in \mathbb{N}$

generator matrix: rows of $G_2^{\otimes m}$

$$G_2^{\otimes 3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

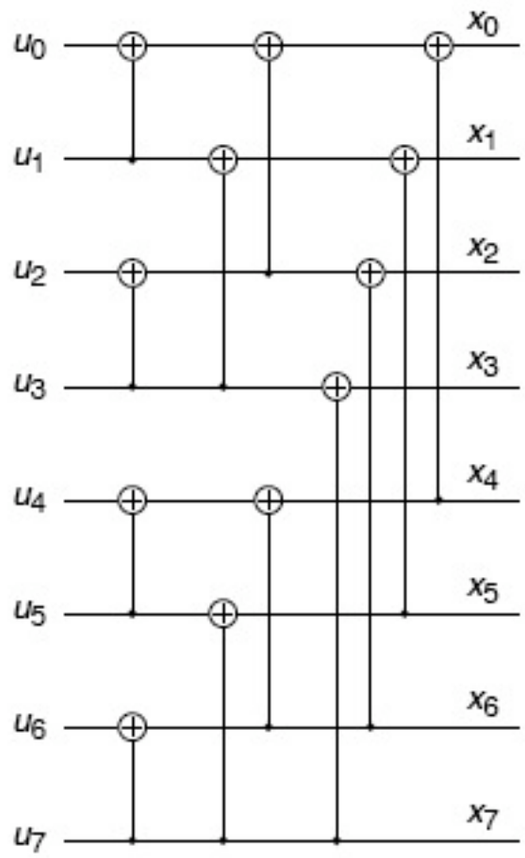
Codes from Kronecker Product of G_2

length $N = 2^m$, $m \in \mathbb{N}$

generator matrix: rows of $G_2^{\otimes m}$

$$G_2^{\otimes 3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\bar{x} = [u_0\ u_1\ u_2\ u_3\ u_4\ u_5\ u_6\ u_7] G_2^{\otimes 3}$$

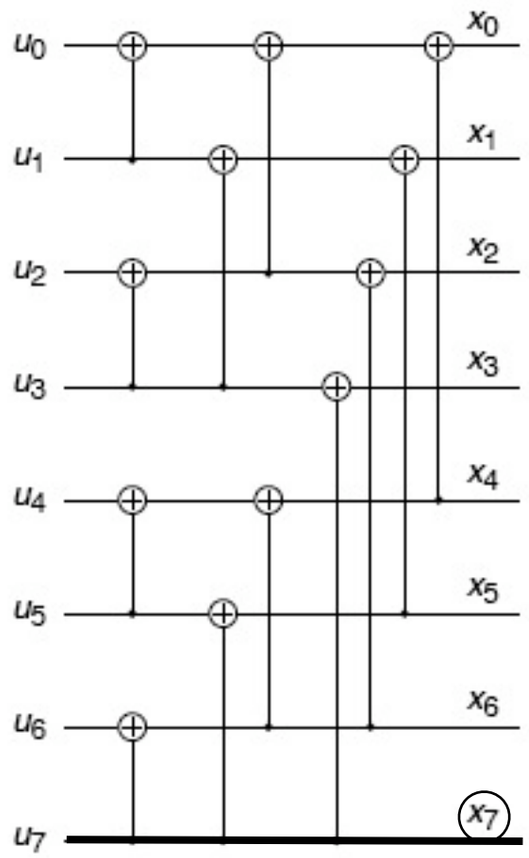


Codes from Kronecker Product of G_2

length $N = 2^m$, $m \in \mathbb{N}$

generator matrix: rows of $G_2^{\otimes m}$

$$G_2^{\otimes 3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & \textcircled{1} \end{bmatrix}$$



$$\bar{x} = [u_0\ u_1\ u_2\ u_3\ u_4\ u_5\ u_6\ u_7]G_2^{\otimes 3}$$

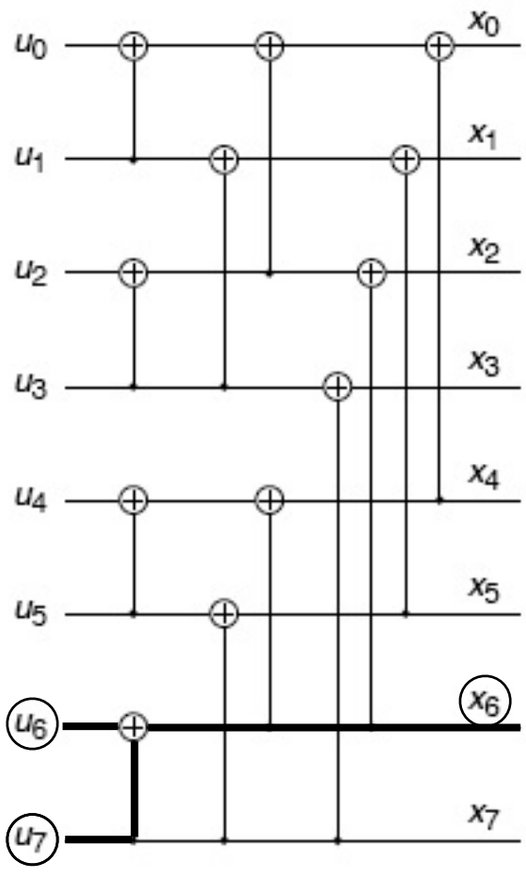
Codes from Kronecker Product of G_2

length $N = 2^m$, $m \in \mathbb{N}$

generator matrix: rows of $G_2^{\otimes m}$

$$G_2^{\otimes 3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & \textcircled{1} & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & \textcircled{1} & 1 \end{bmatrix}$$

$$\bar{x} = [u_0\ u_1\ u_2\ u_3\ u_4\ u_5\ u_6\ u_7] G_2^{\otimes 3}$$



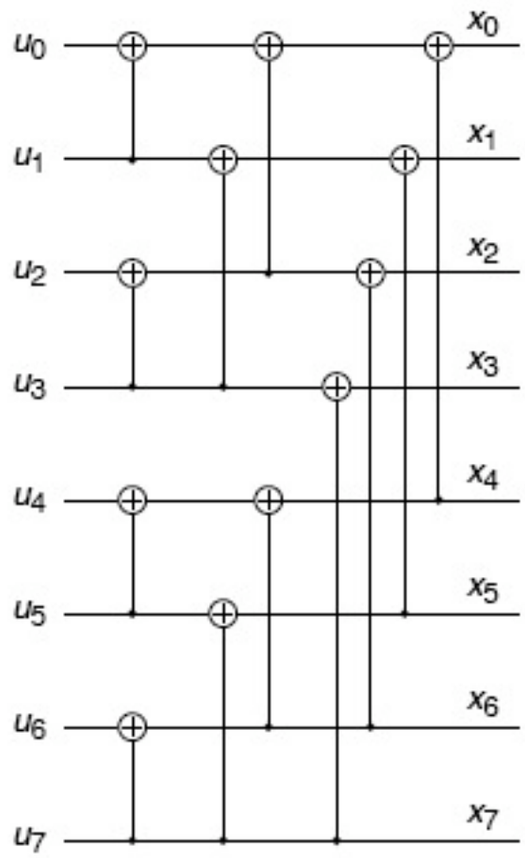
Codes from Kronecker Product of G_2

length $N = 2^m$, $m \in \mathbb{N}$

generator matrix: rows of $G_2^{\otimes m}$

$$G_2^{\otimes 3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\bar{x} = [u_0\ u_1\ u_2\ u_3\ u_4\ u_5\ u_6\ u_7] G_2^{\otimes 3}$$



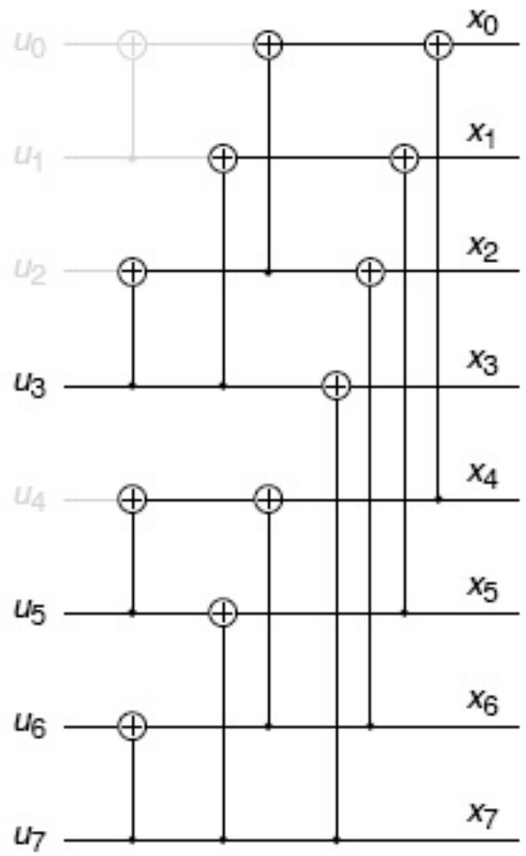
Codes from Kronecker Product of G_2

length $N = 2^m$, $m \in \mathbb{N}$

generator matrix: rows of $G_2^{\otimes m}$

$$G_2^{\otimes 3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\bar{x} = [0\ 0\ 0\ u_3\ 0\ u_5\ u_6\ u_7] G_2^{\otimes 3}$$



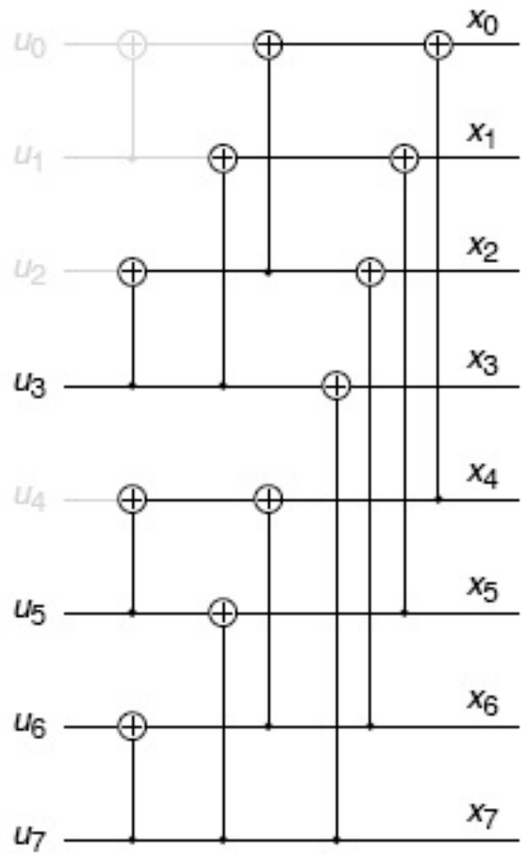
Codes from Kronecker Product of G_2

length $N = 2^m$, $m \in \mathbb{N}$

generator matrix: rows of $G_2^{\otimes m}$

$$G_2^{\otimes 3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\bar{x} = [0\ 0\ 0\ u_3\ 0\ u_5\ u_6\ u_7] G_2^{\otimes 3}$$



How to choose the rows?

Reed-Muller Codes

length $N = 2^m$, $m \in \mathbb{N}$

generator matrix: rows of $G_2^{\otimes m}$

How to choose the rows?

$$G_2^{\otimes 3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\bar{x} = [u_0\ u_1\ u_2\ u_3\ u_4\ u_5\ u_6\ u_7] G_2^{\otimes 3}$$

Reed-Muller Codes

length $N = 2^m$, $m \in \mathbb{N}$

generator matrix: rows of $G_2^{\otimes m}$

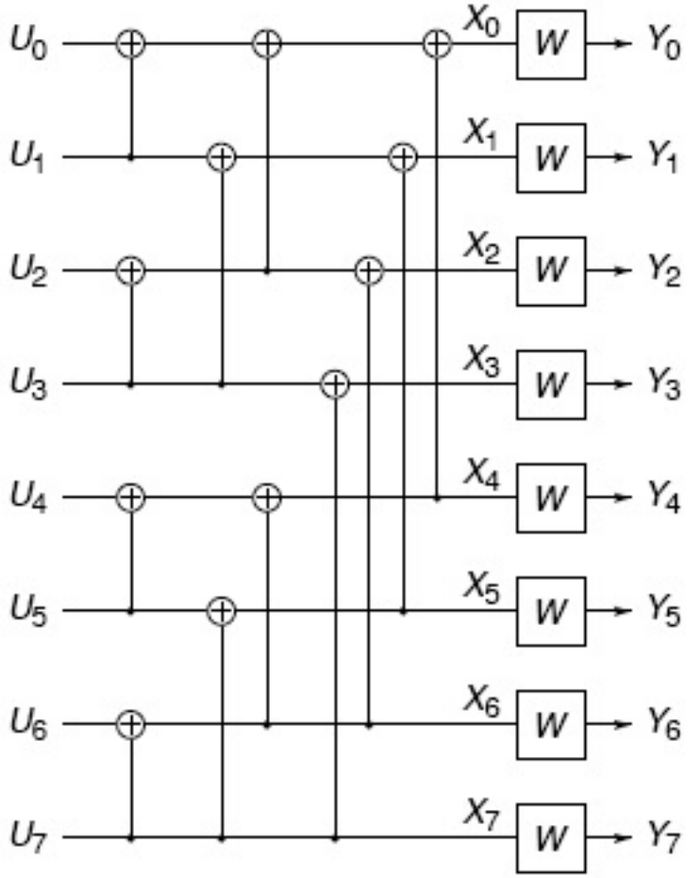
How to choose the rows?

$$G_2^{\otimes 3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\bar{x} = [0\ 0\ 0\ u_3\ 0\ u_5\ u_6\ u_7] G_2^{\otimes 3}$$

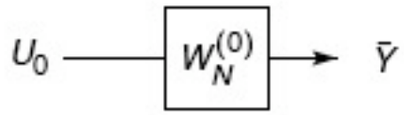
Polar Codes

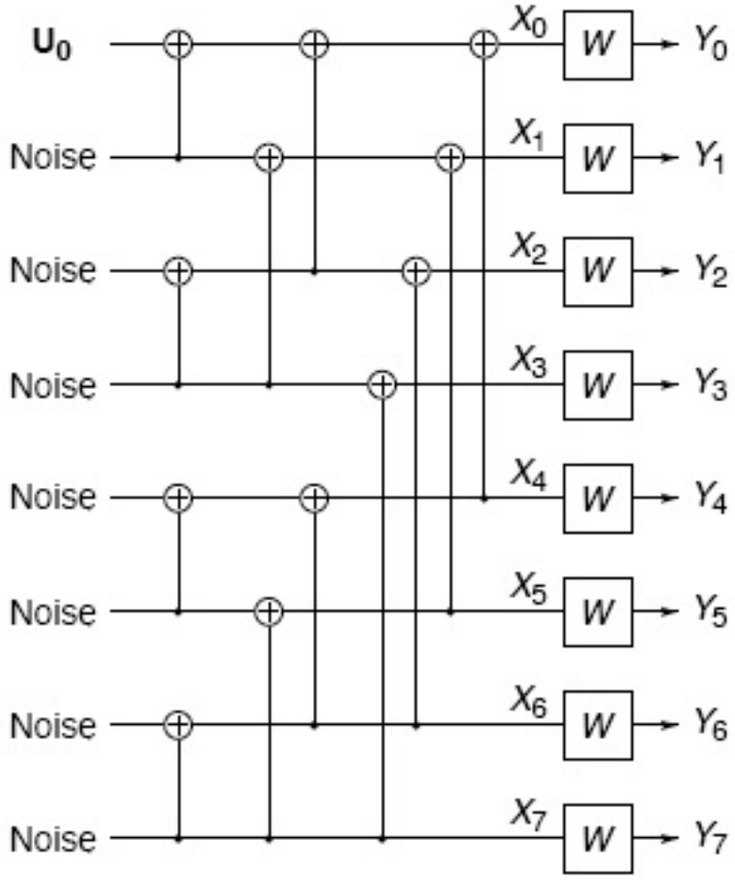
Polar Codes



W -- BMS channel

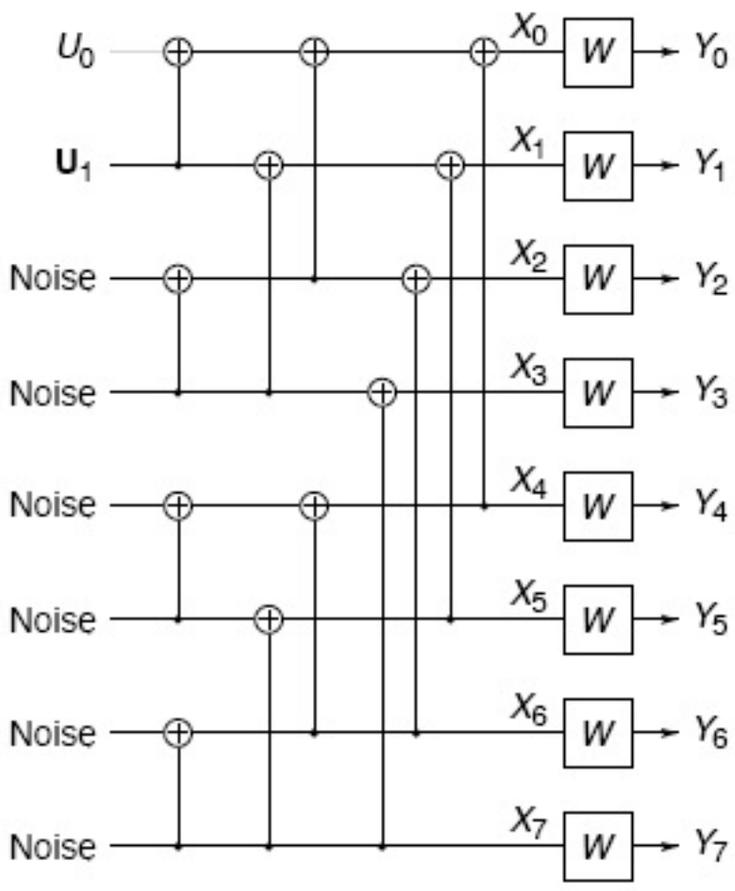
Polar Codes



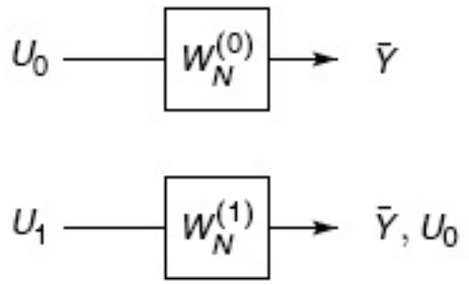


W -- BMS channel

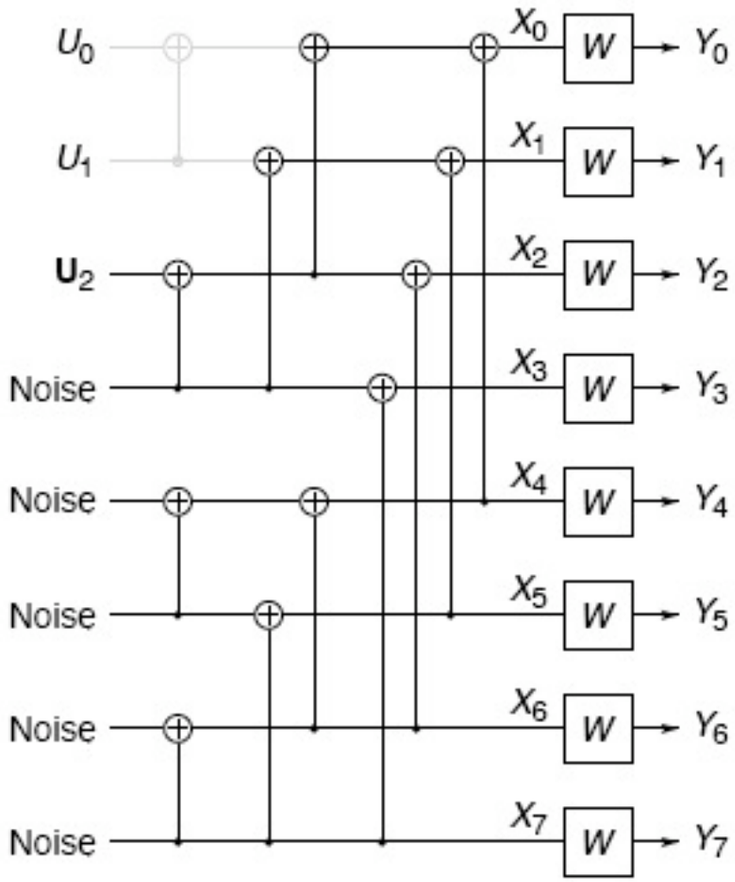
Polar Codes

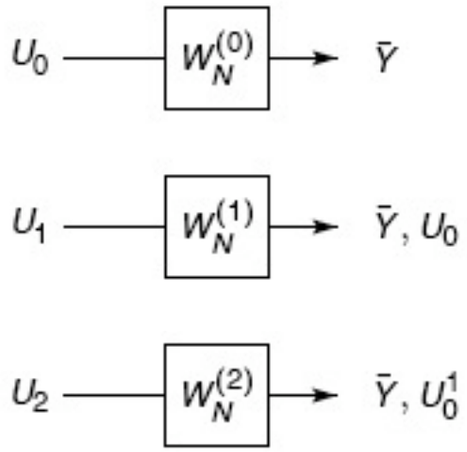


W -- BMS channel



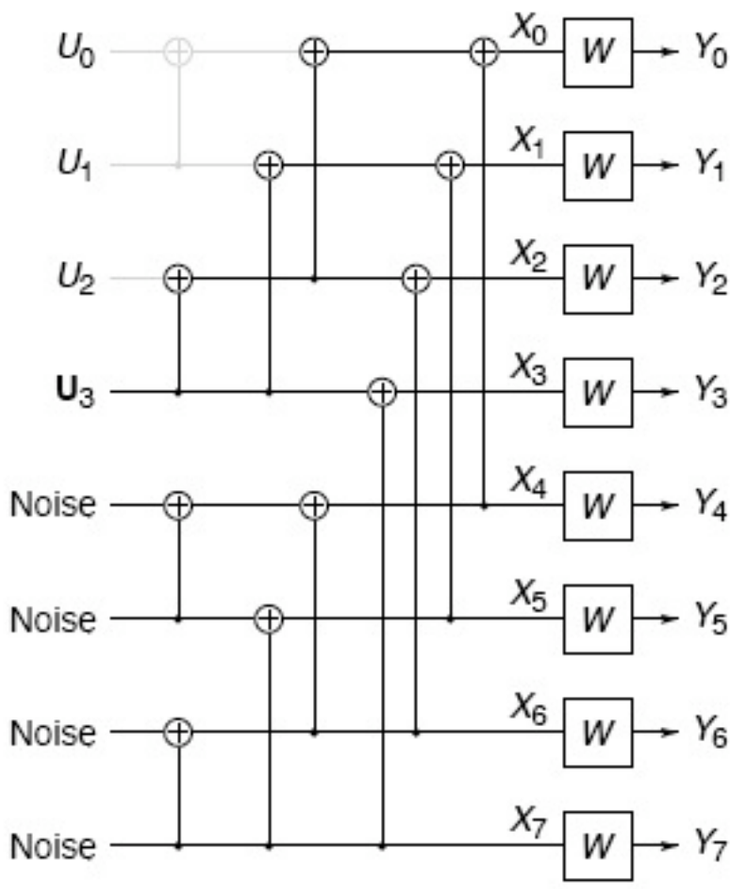
Polar Codes

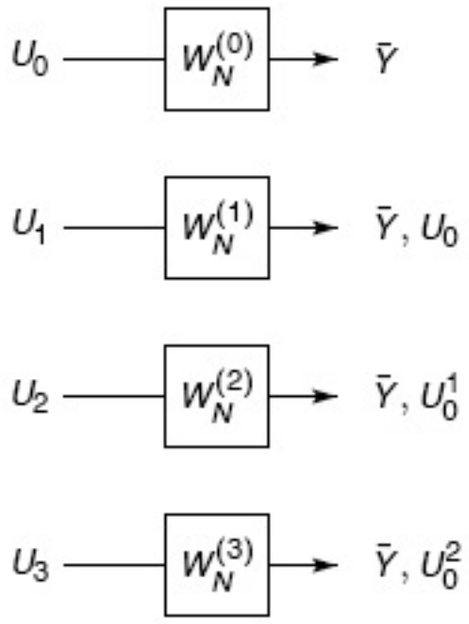




W -- BMS channel

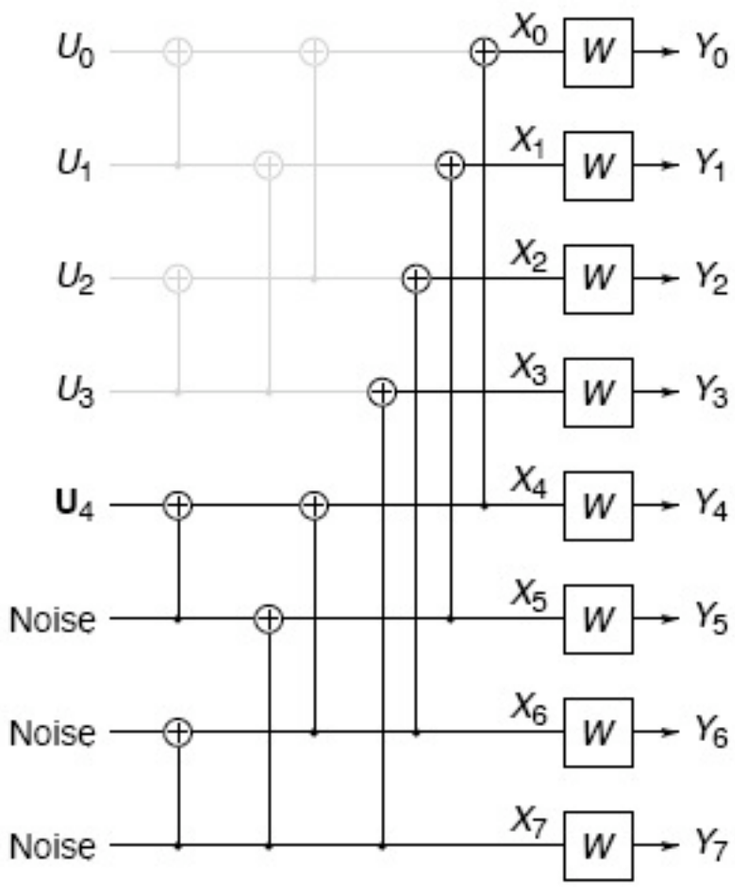
Polar Codes

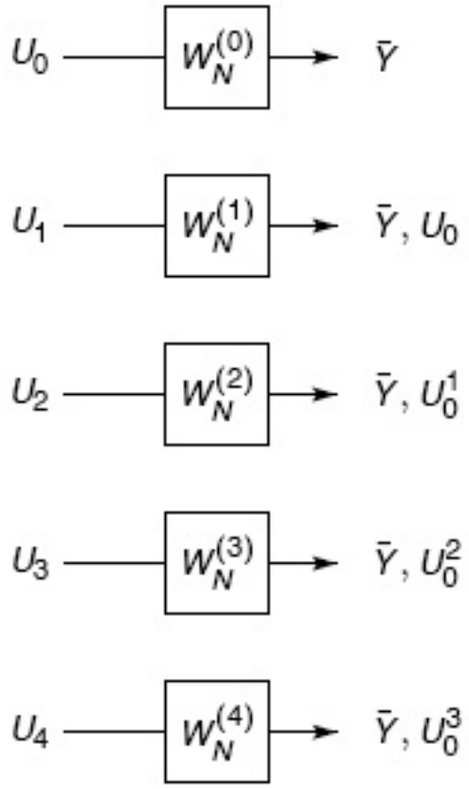




W -- BMS channel

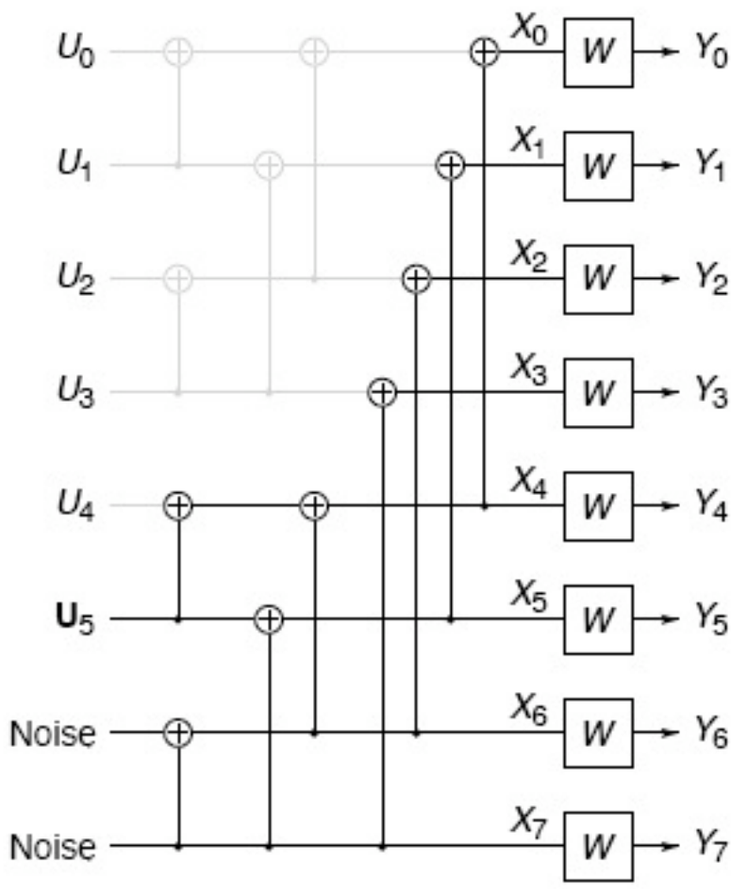
Polar Codes



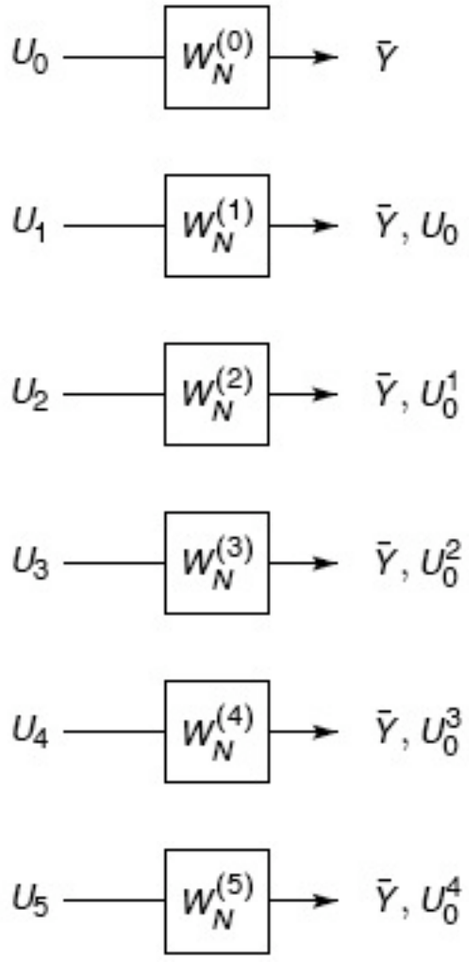


W -- BMS channel

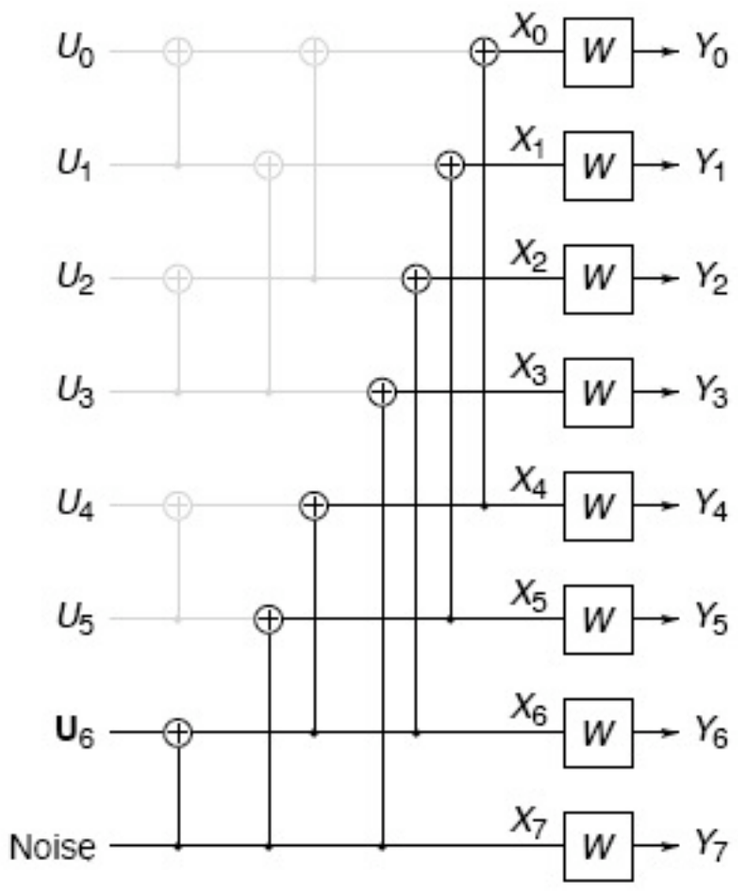
Polar Codes



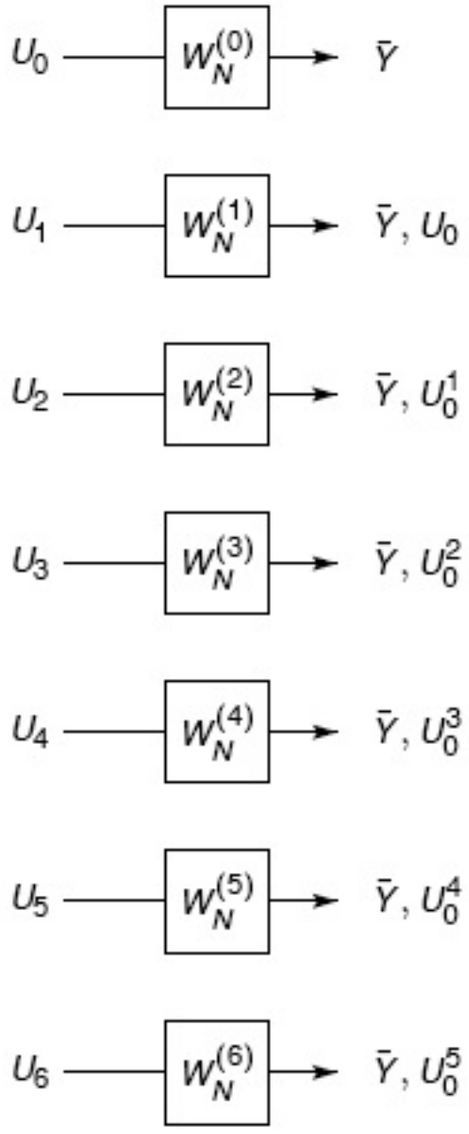
W -- BMS channel



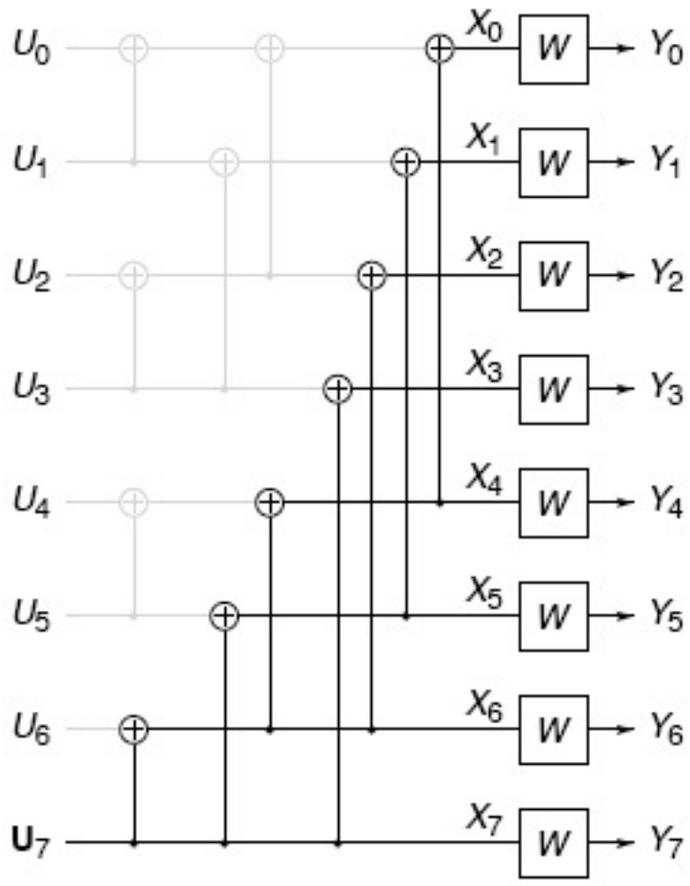
Polar Codes



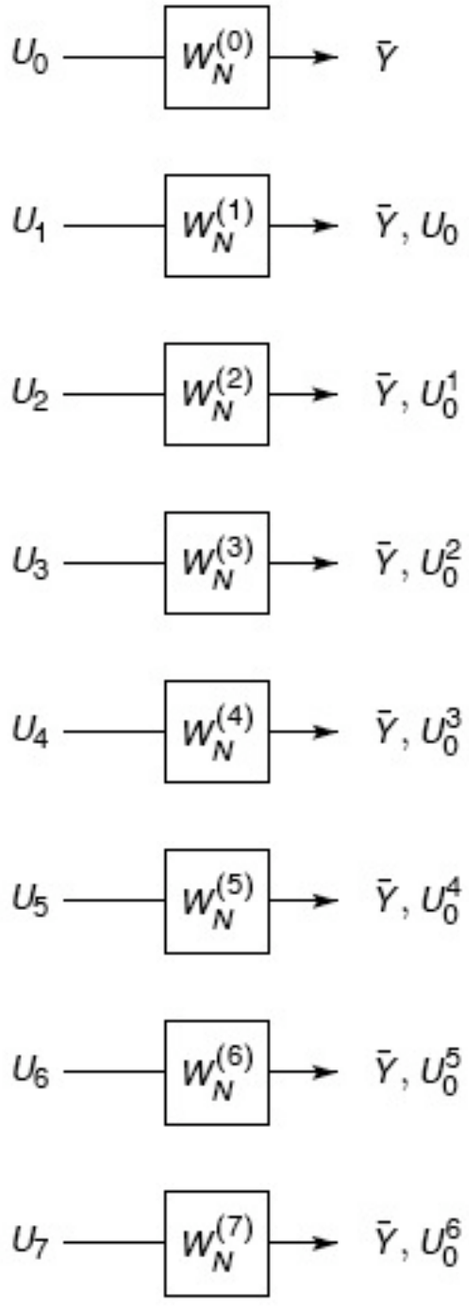
W -- BMS channel



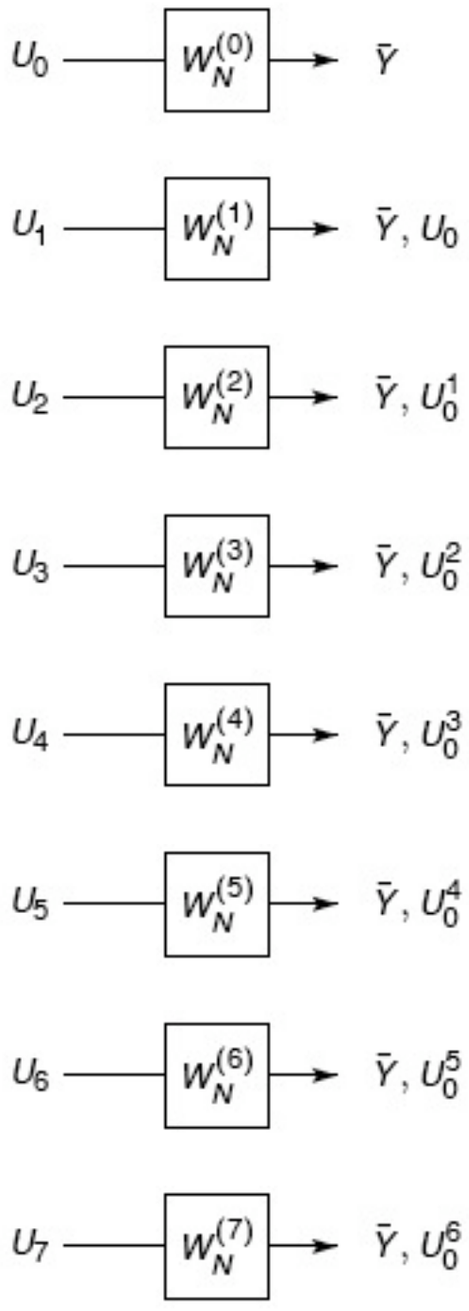
Polar Codes



W -- BMS channel

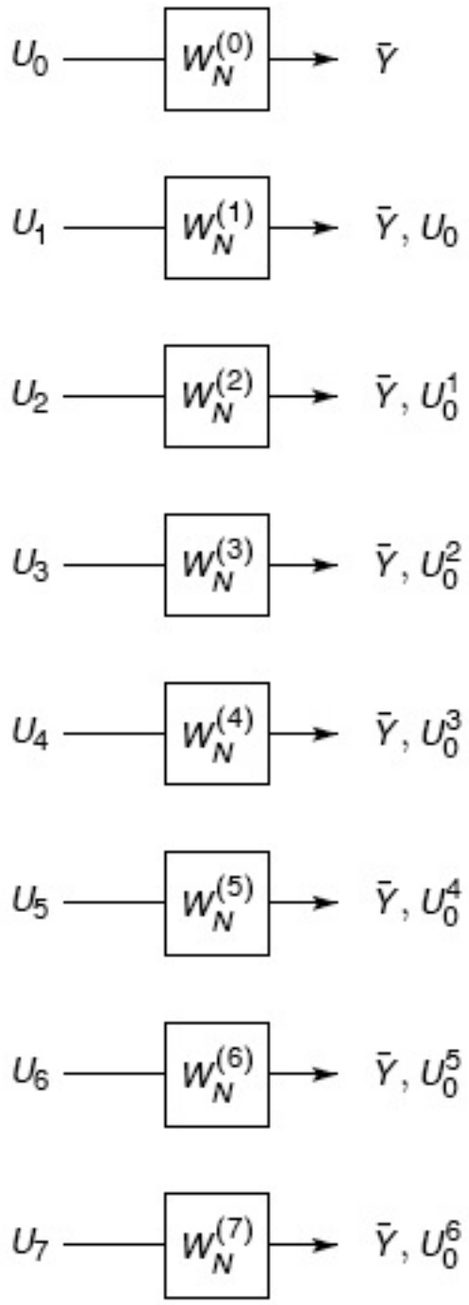


Channel Polarization



Channel Polarization

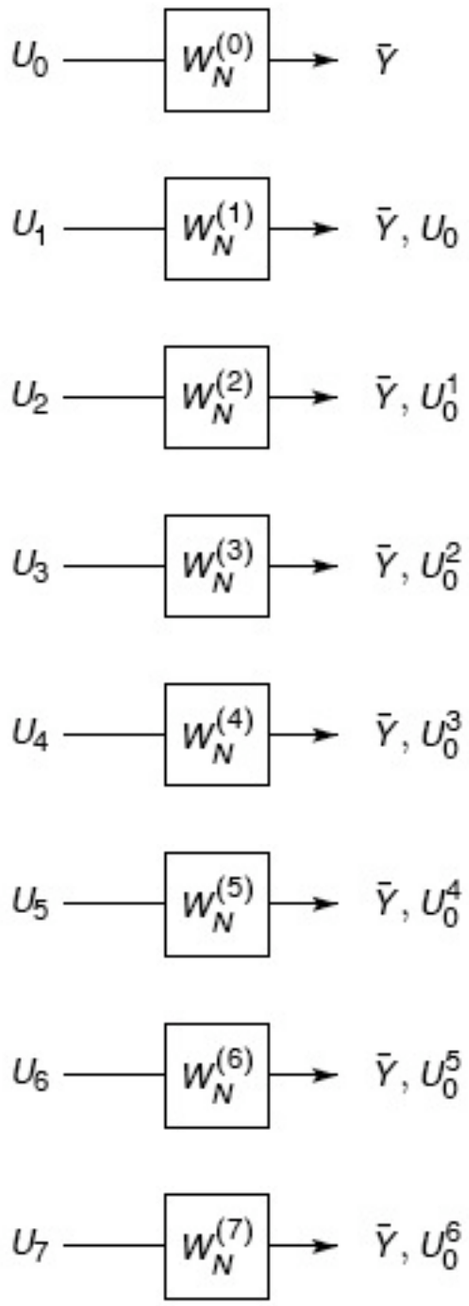
as $N \to \infty$, channels polarize, either completely noisy or noise-free



Channel Polarization

as $N \to \infty$, channels polarize, either completely noisy or noise-free

fraction of good channels approaches capacity $I(W)$

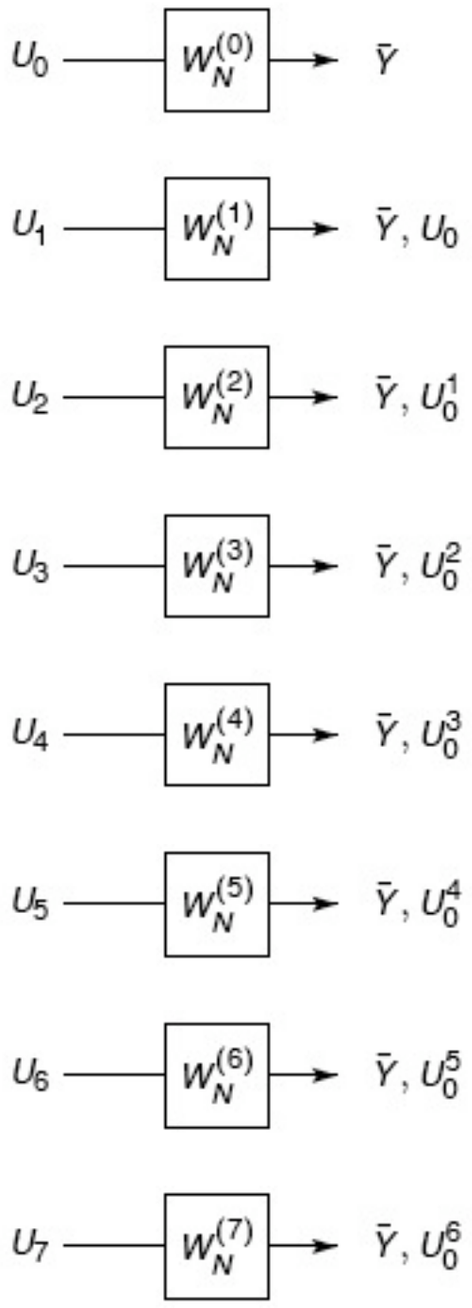


Channel Polarization

as $N \to \infty$, channels polarize, either completely noisy or noise-free

fraction of good channels approaches capacity $I(W)$

fix bad channels and transmit uncoded bits over the good ones

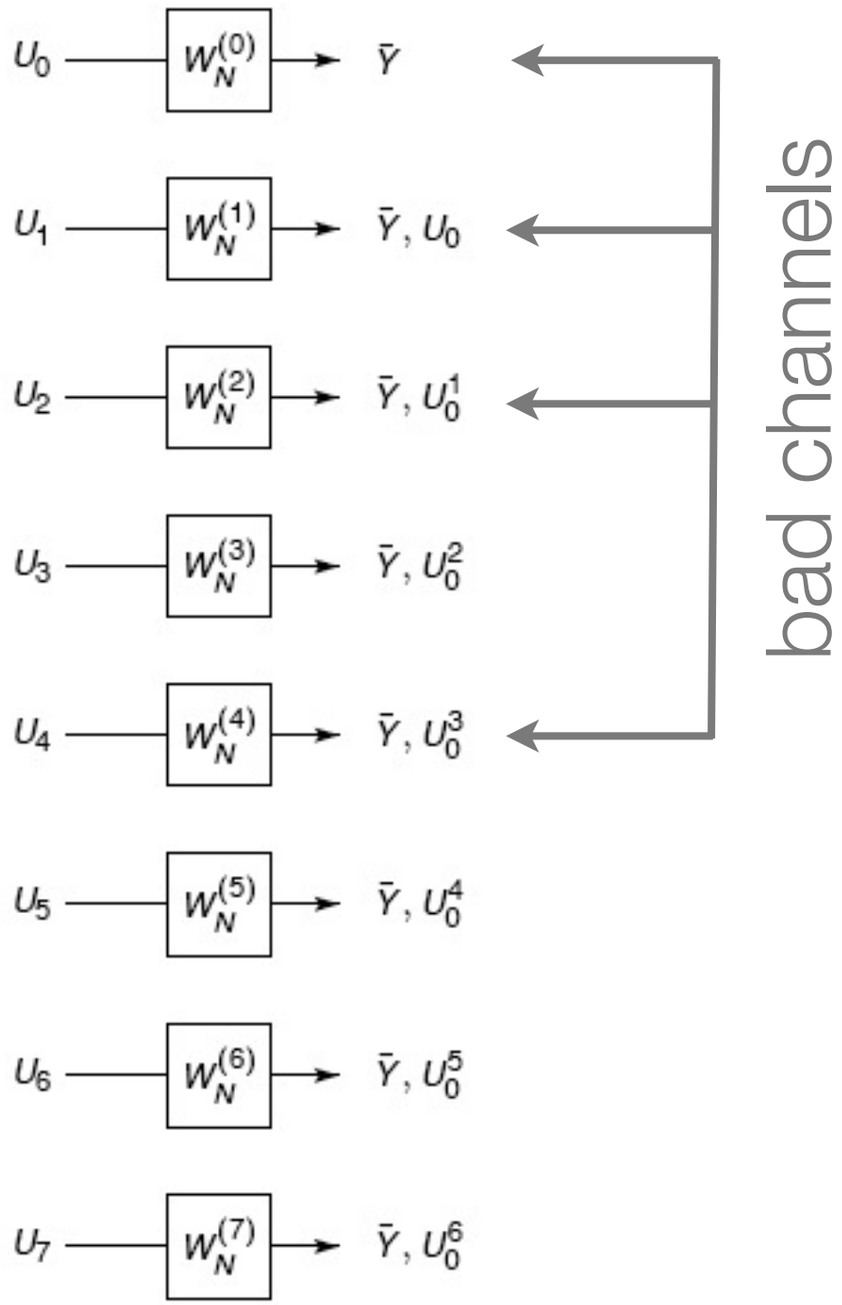


Channel Polarization

as $N \to \infty$, channels polarize, either completely noisy or noise-free

fraction of good channels approaches capacity $I(W)$

fix bad channels and transmit uncoded bits over the good ones

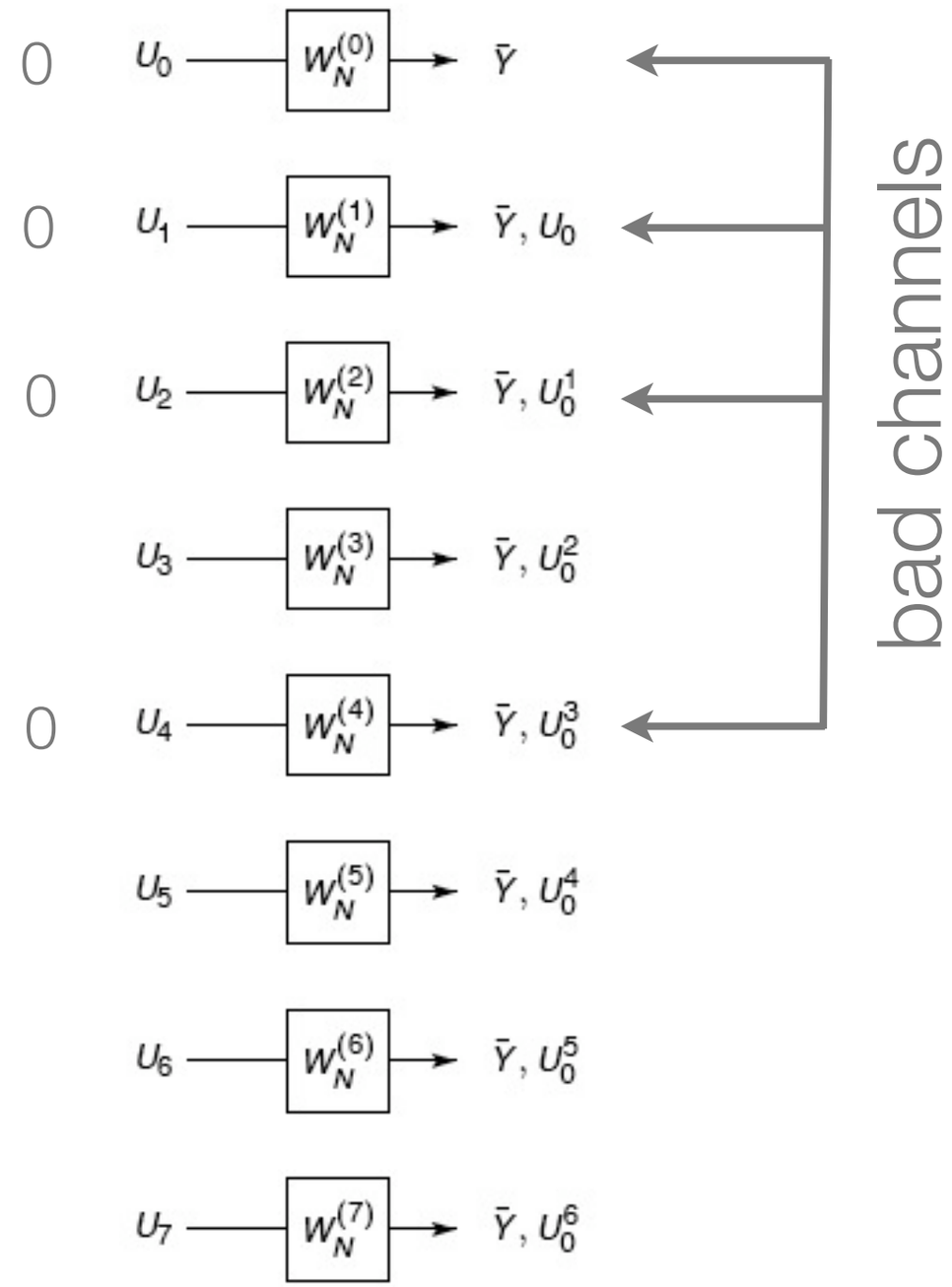


Channel Polarization

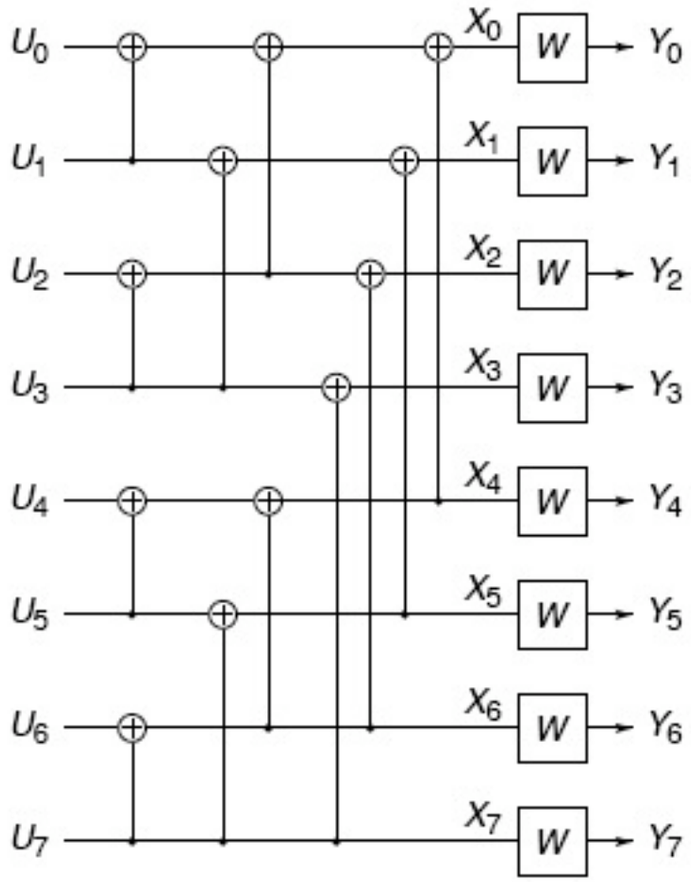
as $N \to \infty$, channels polarize, either completely noisy or noise-free

fraction of good channels approaches capacity $I(W)$

fix bad channels and transmit uncoded bits over the good ones

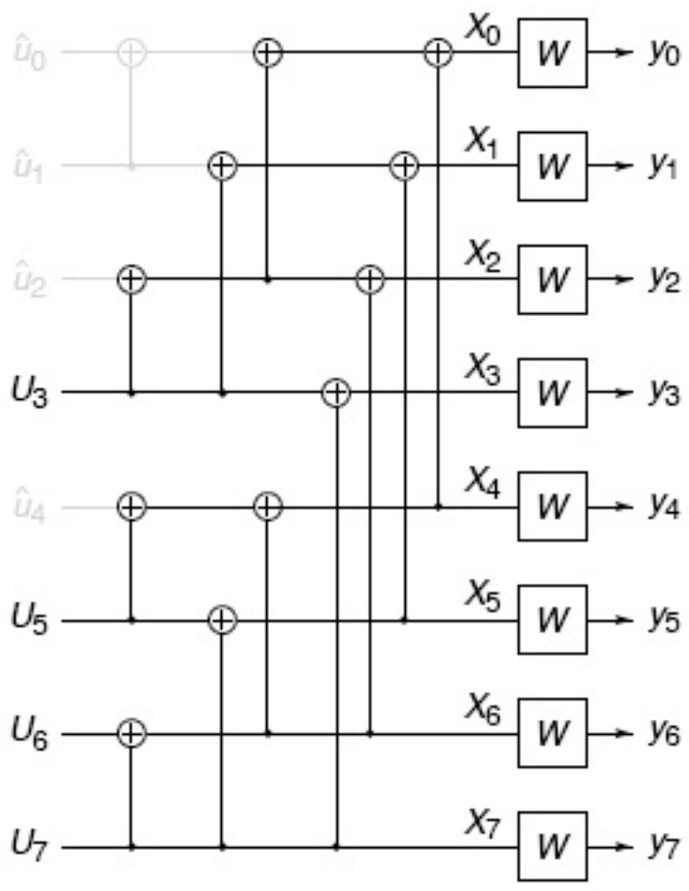


Successive Decoding



Successive Decoding

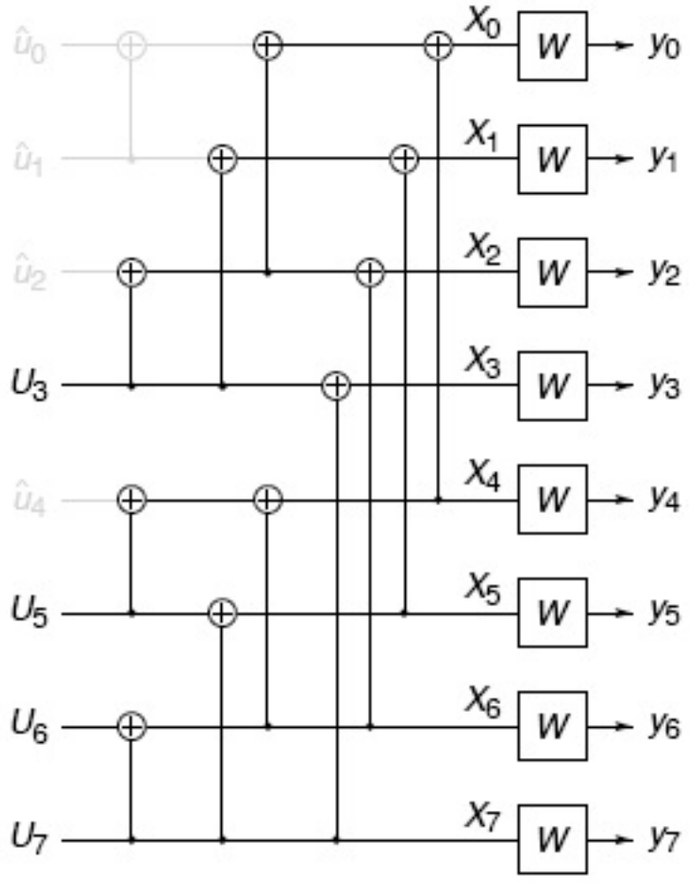
$$F = \{0, 1, 2, 4\}$$



Successive Decoding

$F = \{0, 1, 2, 4\}$

From 0 till $N - 1$



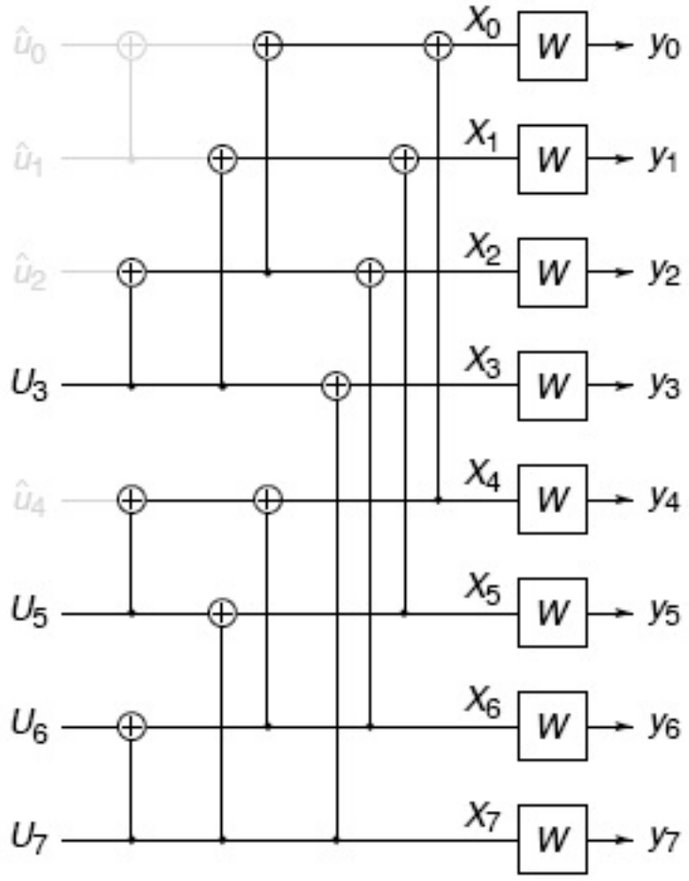
Successive Decoding

$F = \{0, 1, 2, 4\}$

From 0 till $N - 1$

if $i \in F$, $\hat{u}_i = 0$
if $i \in F^c$,

$$\hat{u}_i = \begin{cases} 0, & \text{if } \frac{P(0|\hat{u}_0^{i-1}, \bar{y})}{P(1|\hat{u}_0^{i-1}, \bar{y})} > 1 \\ 1, & \text{otherwise} \end{cases}$$



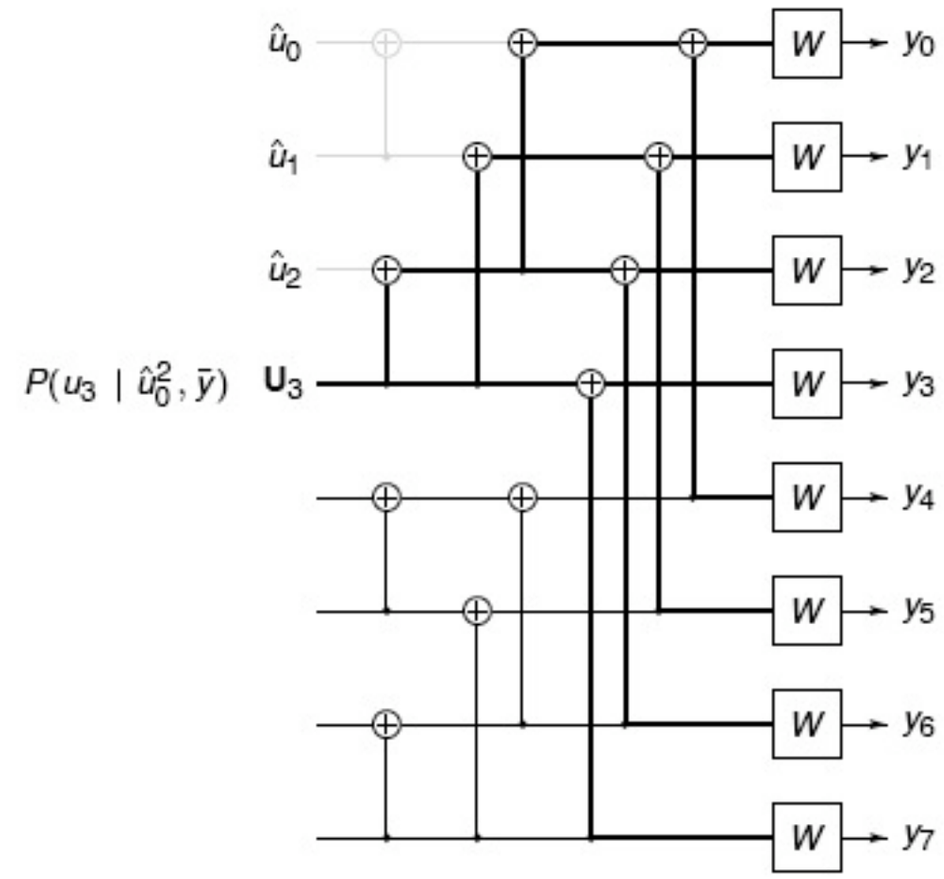
Successive Decoding

$F = \{0, 1, 2, 4\}$

From 0 till $N - 1$

if $i \in F$, $\hat{u}_i = 0$
if $i \in F^c$,

$$\hat{u}_i = \begin{cases} 0, & \text{if } \frac{P(0|\hat{u}_0^{i-1}, \bar{y})}{P(1|\hat{u}_0^{i-1}, \bar{y})} > 1 \\ 1, & \text{otherwise} \end{cases}$$



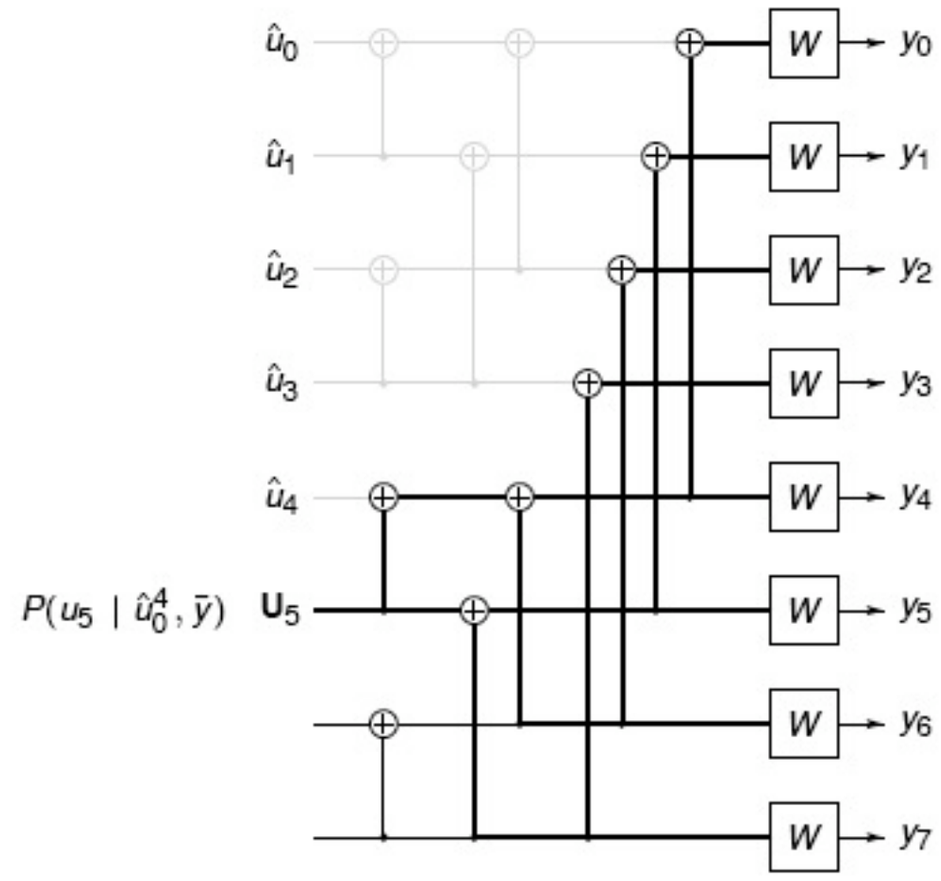
Successive Decoding

$F = \{0, 1, 2, 4\}$

From 0 till $N - 1$

if $i \in F$, $\hat{u}_i = 0$
if $i \in F^c$,

$$\hat{u}_i = \begin{cases} 0, & \text{if } \frac{P(0|\hat{u}_0^{i-1}, \bar{y})}{P(1|\hat{u}_0^{i-1}, \bar{y})} > 1 \\ 1, & \text{otherwise} \end{cases}$$



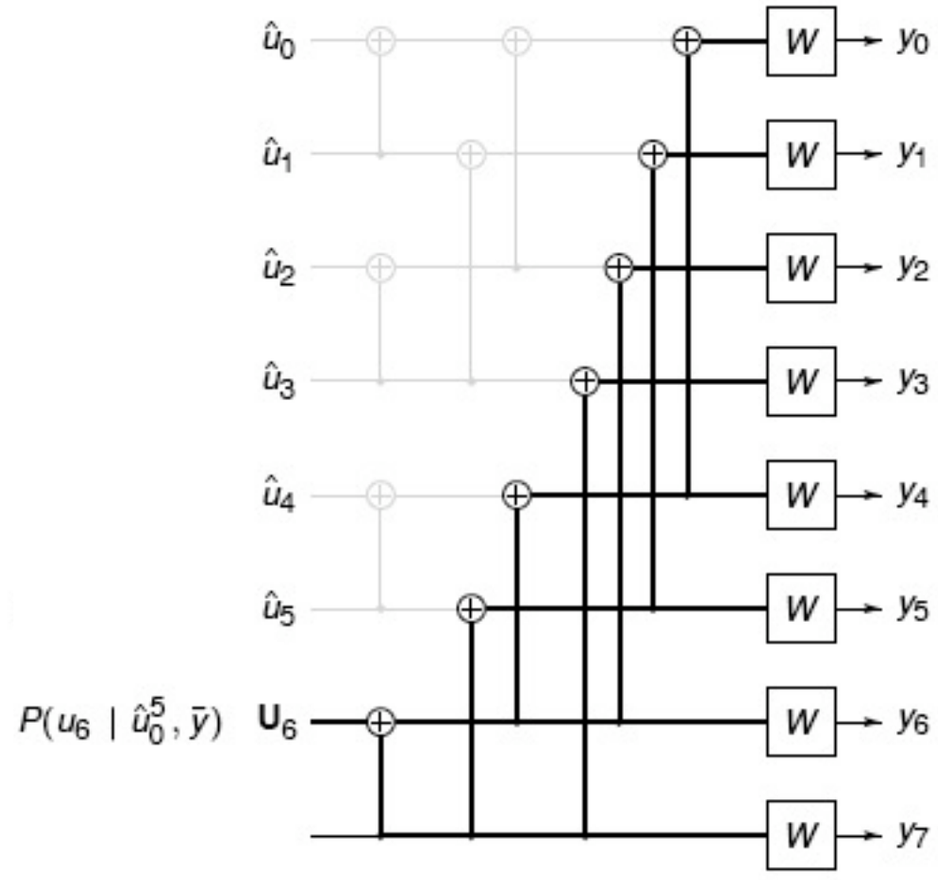
Successive Decoding

$F = \{0, 1, 2, 4\}$

From 0 till $N - 1$

if $i \in F$, $\hat{u}_i = 0$
if $i \in F^c$,

$$\hat{u}_i = \begin{cases} 0, & \text{if } \frac{P(0|\hat{u}_0^{i-1}, \bar{y})}{P(1|\hat{u}_0^{i-1}, \bar{y})} > 1 \\ 1, & \text{otherwise} \end{cases}$$



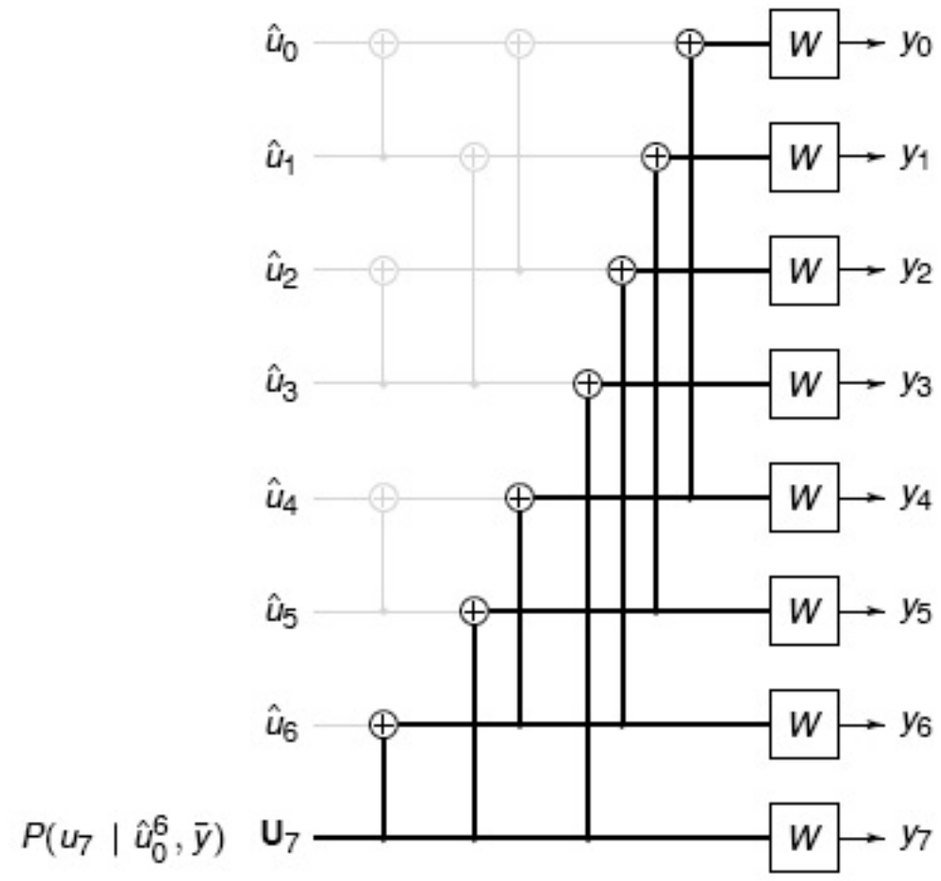
Successive Decoding

$F = \{0, 1, 2, 4\}$

From 0 till $N - 1$

if $i \in F$, $\hat{u}_i = 0$
if $i \in F^c$,

$$\hat{u}_i = \begin{cases} 0, & \text{if } \frac{P(0|\hat{u}_0^{i-1}, \bar{y})}{P(1|\hat{u}_0^{i-1}, \bar{y})} > 1 \\ 1, & \text{otherwise} \end{cases}$$



Successive Decoding

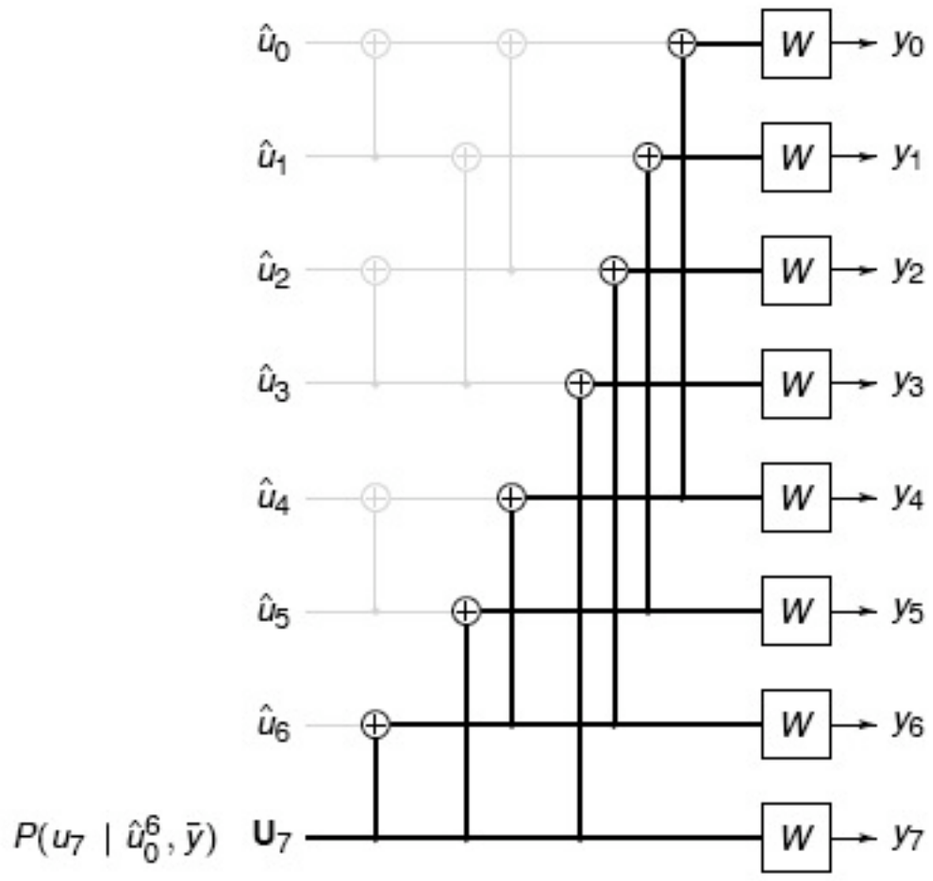
$F = \{0, 1, 2, 4\}$

From 0 till $N - 1$

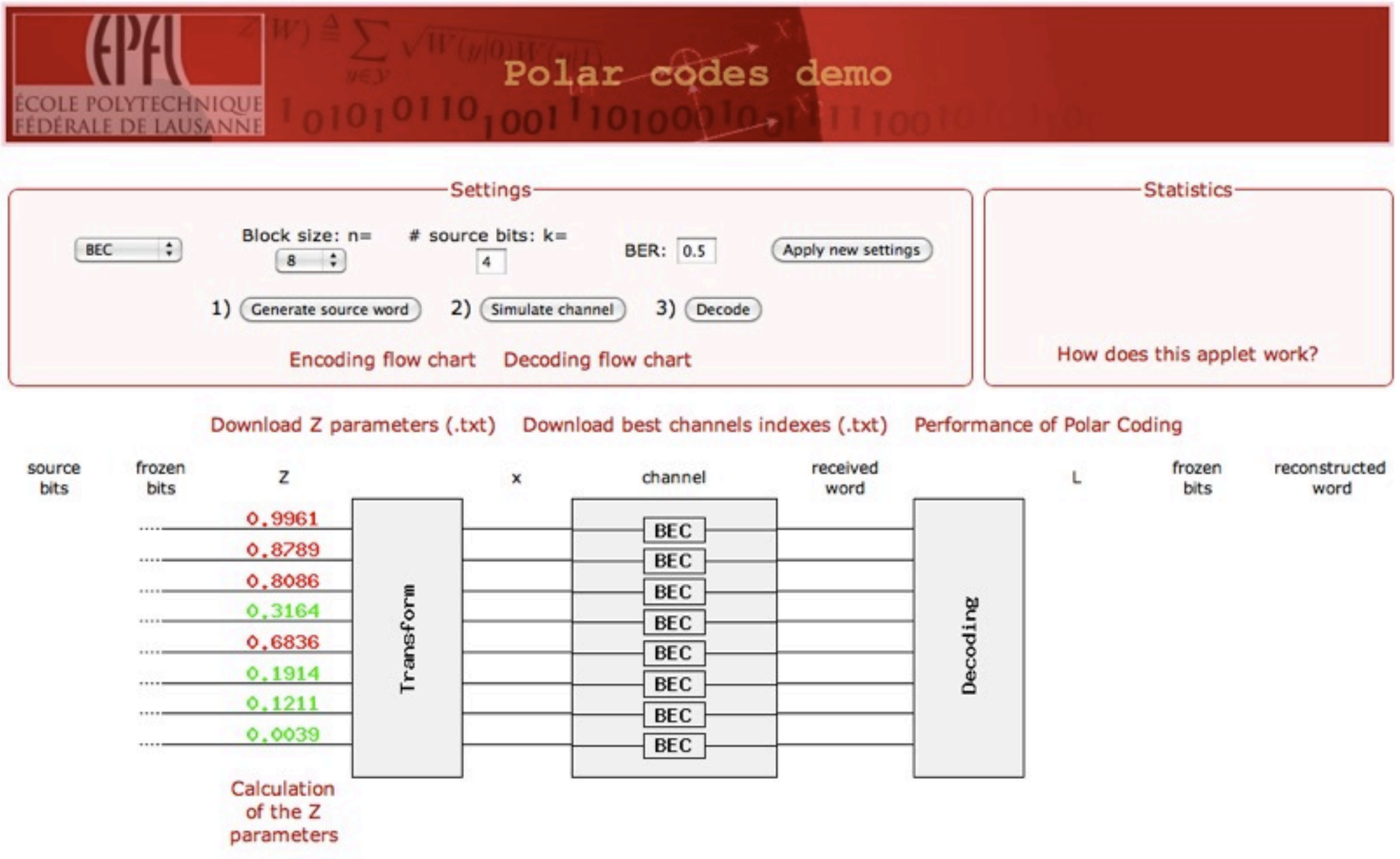
if $i \in F$, $\hat{u}_i = 0$
if $i \in F^c$,

$$\hat{u}_i = \begin{cases} 0, & \text{if } \frac{P(0|\hat{u}_0^{i-1}, \bar{y})}{P(1|\hat{u}_0^{i-1}, \bar{y})} > 1 \\ 1, & \text{otherwise} \end{cases}$$

Complexity $O(N \log N)$



Polar Code Demo

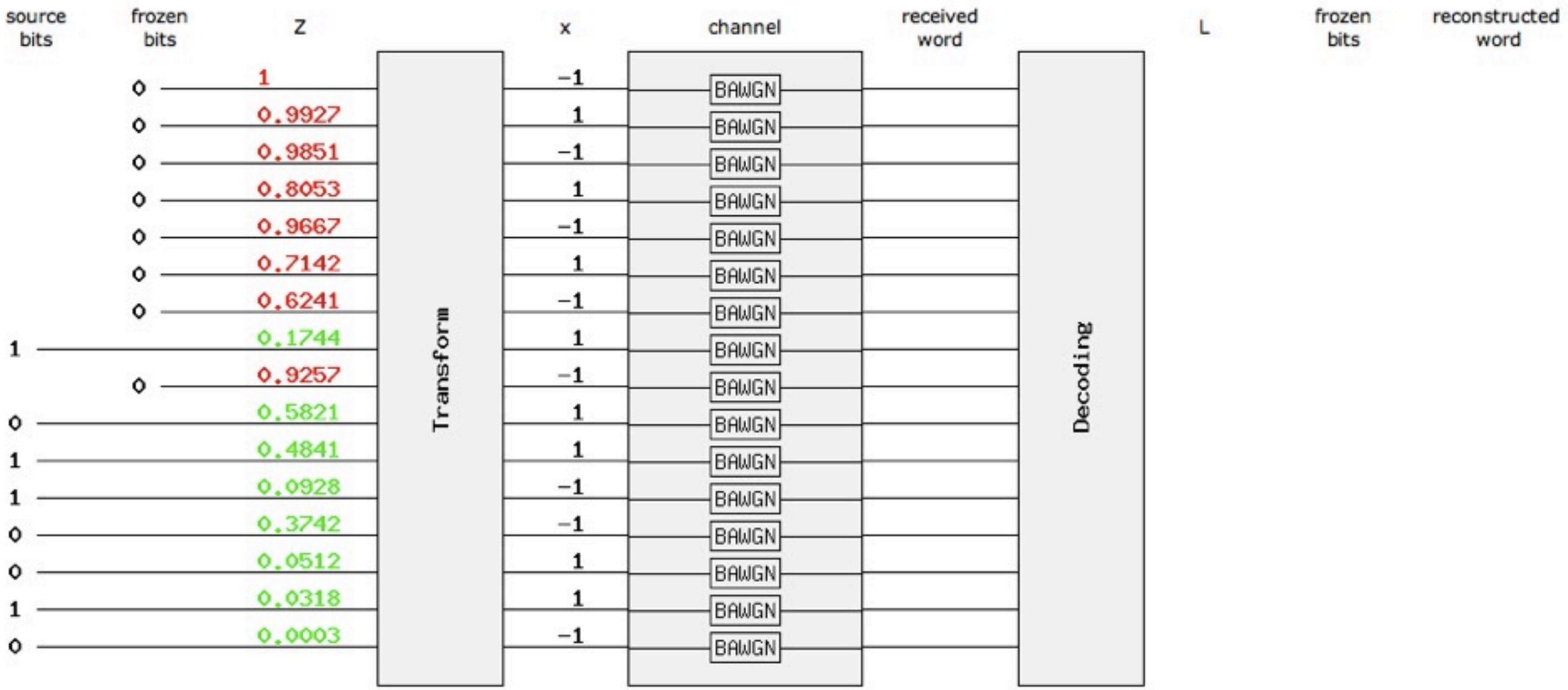


see http://ipgdemos.epfl.ch/polarcodes/
(Stefan Meier)

Successive Decoding

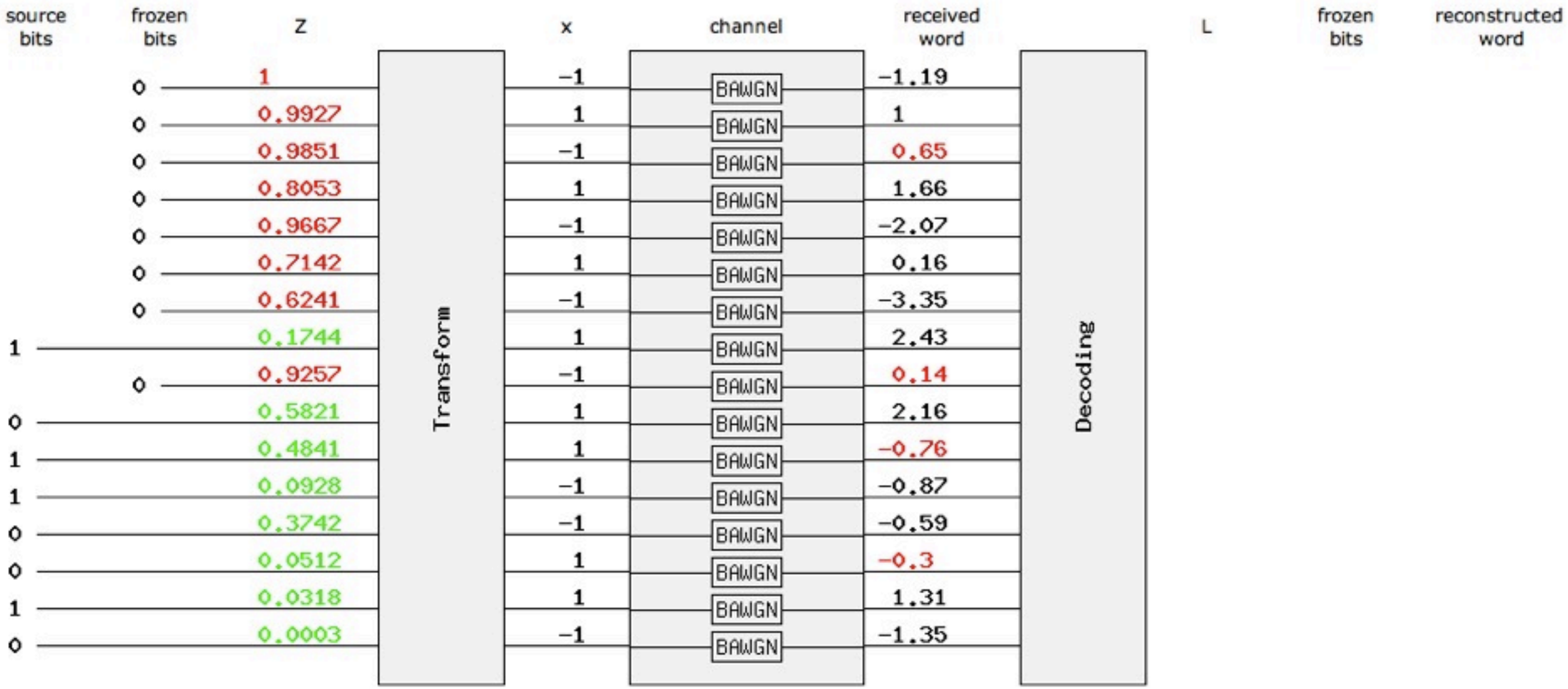
see http://ipgdemos.epfl.ch/polarcodes/
(Stefan Meier)

Successive Decoding



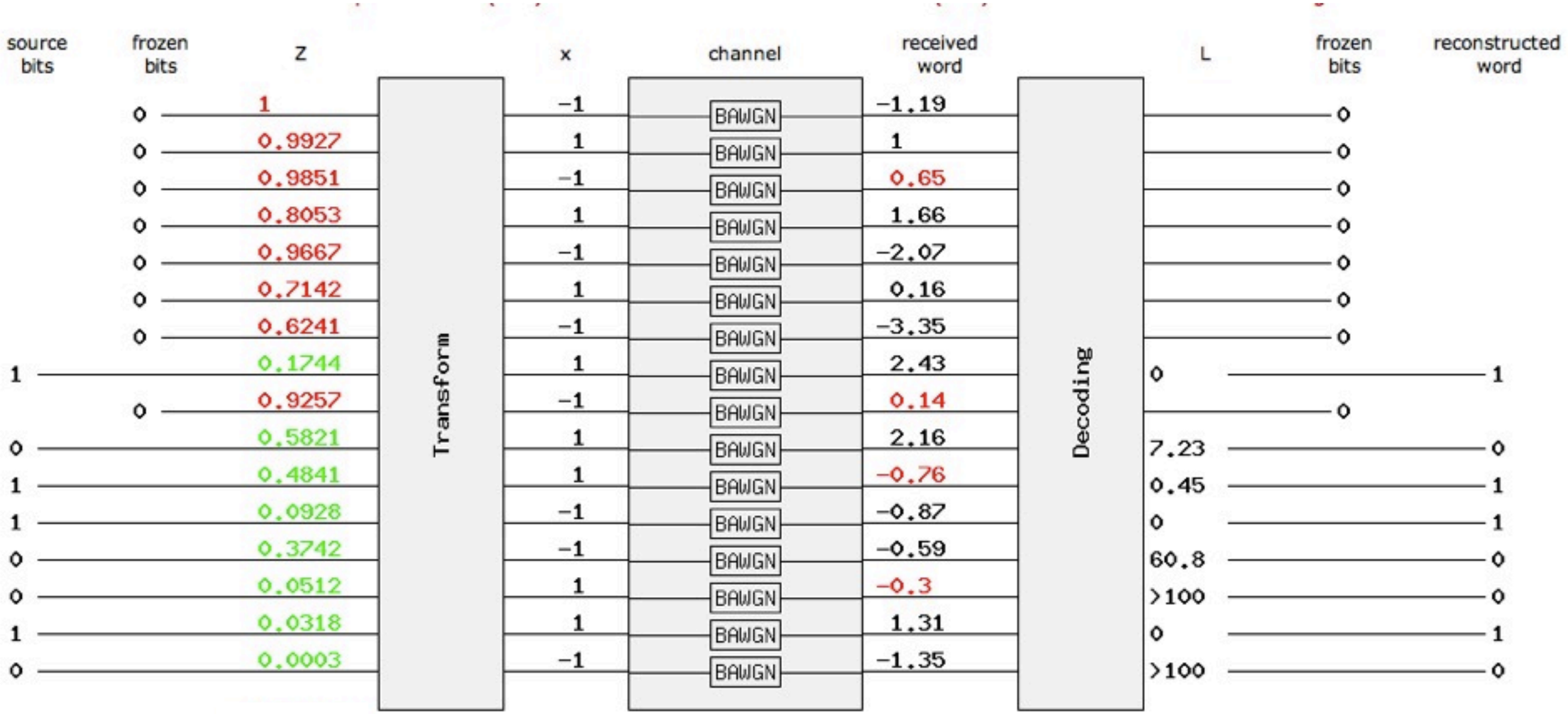
see http://ipgdemos.epfl.ch/polarcodes/
(Stefan Meier)

Successive Decoding



see http://ipgdemos.epfl.ch/polarcodes/
(Stefan Meier)

Successive Decoding



see http://ipgdemos.epfl.ch/polarcodes/
(Stefan Meier)

Historical comments
(slide courtesy Erdal Arikan)

Historical comments
(slide courtesy Erdal Arikan)

discovered by Muller and Reed in separate works both in 1954

Historical comments
(slide courtesy Erdal Arikan)

discovered by Muller and Reed in separate works both in 1954

recursive construction due to Plotkin; (u, u+v) construction

Historical comments
(slide courtesy Erdal Arikan)

discovered by Muller and Reed in separate works both in 1954

recursive construction due to Plotkin; (u, u+v) construction

- Majority-logic decoding
  - Originates with Reed's algorithm (1954)
  - Complexity $O(nk)$ where n is code length, k is dimension
- ML decoding
  - Feasible only for low-order RM codes and their duals
  - $O(n \log n)$ complexity for 1st order code ("Green machine")
  - May be capacity-achieving with RM codes
- Recursive decoding
  - Exploits the recursive Plotkin construction
  - Complexity $O(n \log n)$ for all RM codes of length n
  - Applicable to polar codes as well
    - Achieves channel capacity with polar codes
    - Fails to achieve channel capacity with RM codes

Historical comments
(slide courtesy Erdal Arikan)

- There are two fundamental aspects of the recursive decoder:
  - The $|u|u+v|$ structure of the code – the basis of the recursion
    - This is due to Plotkin (1960)
    - Naive recursion gives decoder complexity $O(n^2)$
  - Design of a "fast" decoder of complexity $O(n \log n)$
    - JPL's Green first to design an $O(n \log n)$ decoder (late 1960s)
    - "Green machine" an ML decoder for 1st order codes
    - Recursive decoders for arbitrary RM codes took very long to appear
    - Lack of interest in RM codes a likely reason for the delay

Historical comments
(slide courtesy Erdal Arikan)

- There are two fundamental aspects of the recursive decoder:
  - The $|u|u+v|$ structure of the code – the basis of the recursion
    - This is due to Plotkin (1960)
    - Naive recursion gives decoder complexity $O(n^2)$
  - Design of a "fast" decoder of complexity $O(n \log n)$
    - JPL's Green first to design an $O(n \log n)$ decoder (late 1960s)
    - "Green machine" an ML decoder for 1st order codes
    - Recursive decoders for arbitrary RM codes took very long to appear
    - Lack of interest in RM codes a likely reason for the delay

Historical comments (slide courtesy Erdal Arikan)

- Litsyn and Shekhovtsov (1983): $O(n)$ bounded distance decoder RM$(1, m)$
- Litsyn (1988): Extension of $O(n)$ BDD to RM codes of fixed order
- Kabatiansky (1990): $O(n \log n)$ recursive decoder for arbitrary RM codes – similar to the one here
- Kabatianky/Bossert (1990s): $O(n \log n)$ decoder for "generalized concatenated codes"
- Schnabl and Bossert (1995): $O(n \log n)$ decoder presented in this paper
- There are many more papers on this subject

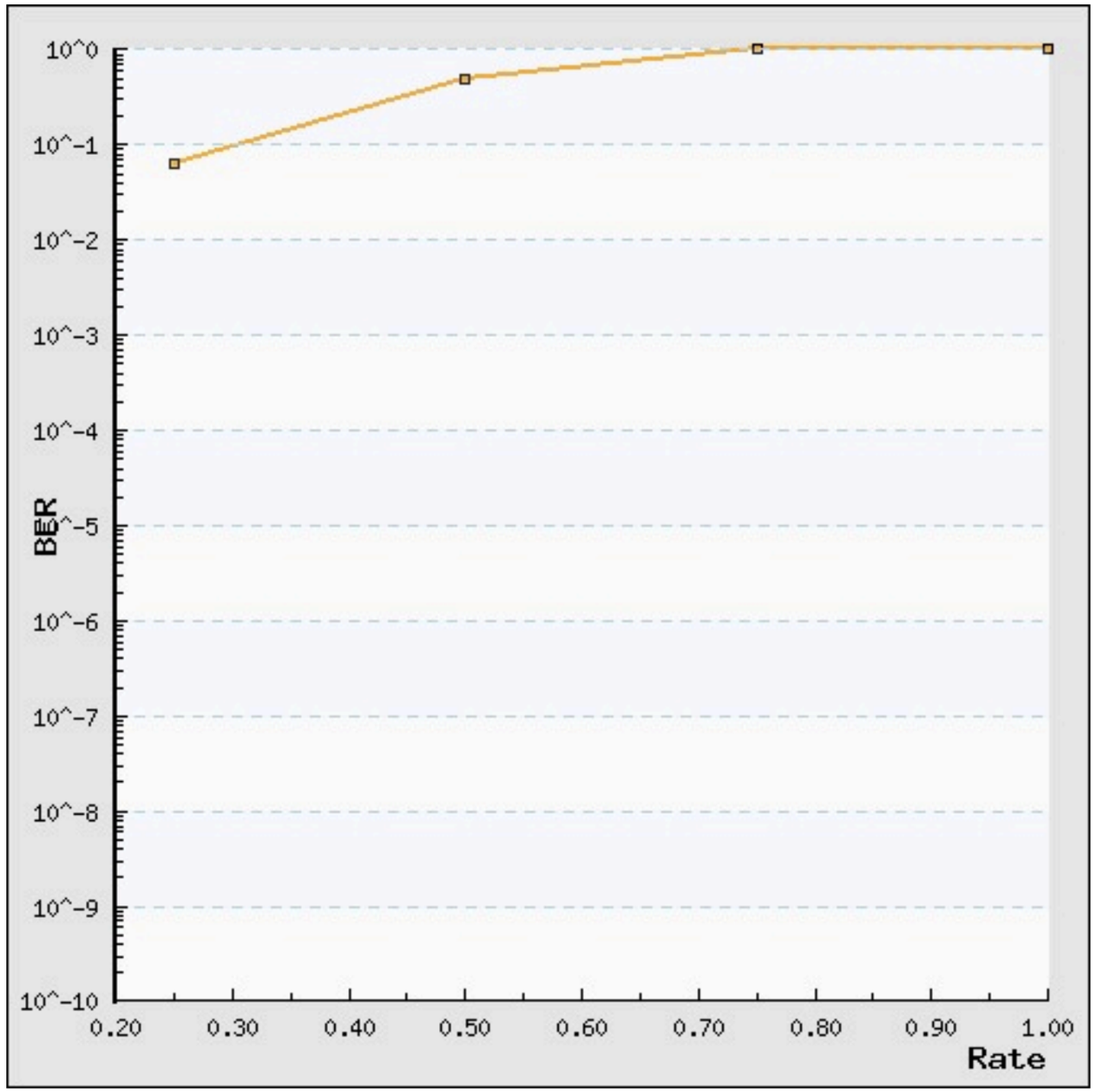
Historical comments
(slide courtesy Erdal Arikan)

- Dumer and Shabunov(ISIT'2000) recognized that some coordinates of RM codes are very weakly protected under recursive decoding.
- Dumer and Shabunov (ISIT'2002) proposed the use of "permutation decoding" as a remedy to this problem.
- In recent work, Burnashev and Dumer (2006, 2008, 2009) carried out an analysis for identifying the weak spots under recursive decoding.
- The idea of avoiding weak spots under recursive decoding—if it had been pursued in full—would have led to polar coding.

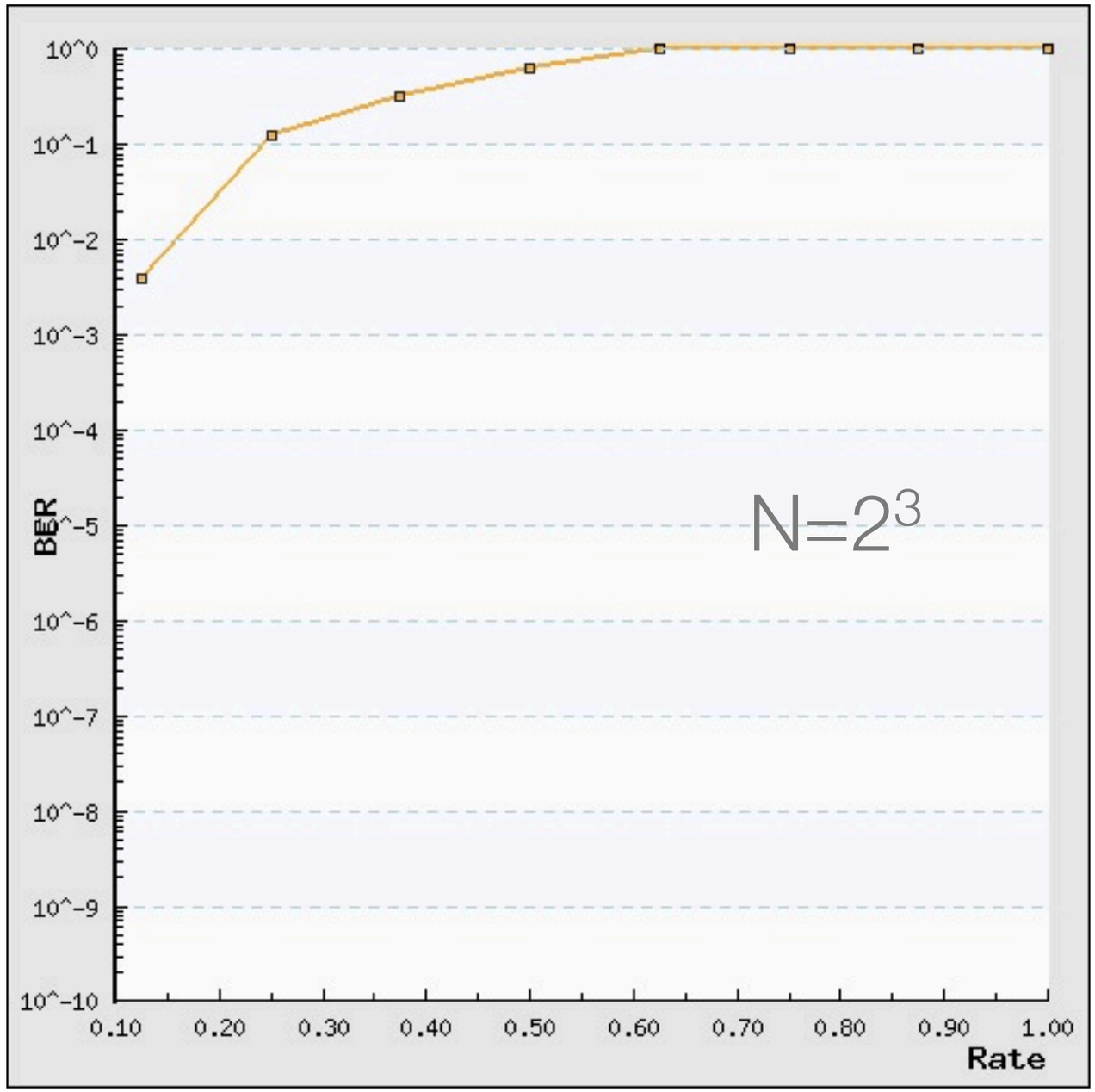
P.S.: The work by Erdal Arikan was actually not motivated by any of the connections above; these he all found a posteriori; his starting point was the view point of sequential decoding and the observation that the cut-off rate improves under the (u|u+v) construction.

Channel Polarization

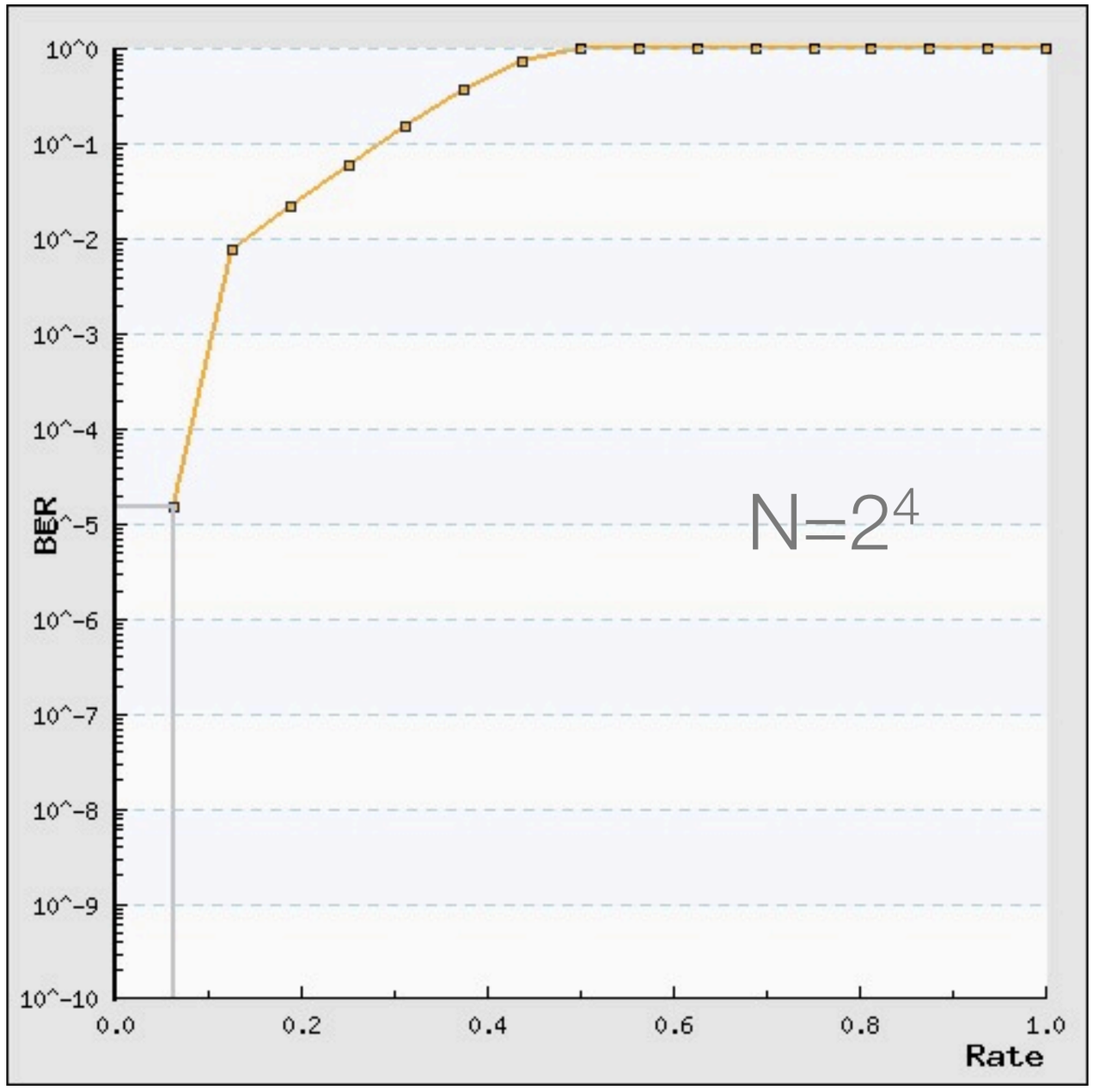
Channel Polarization



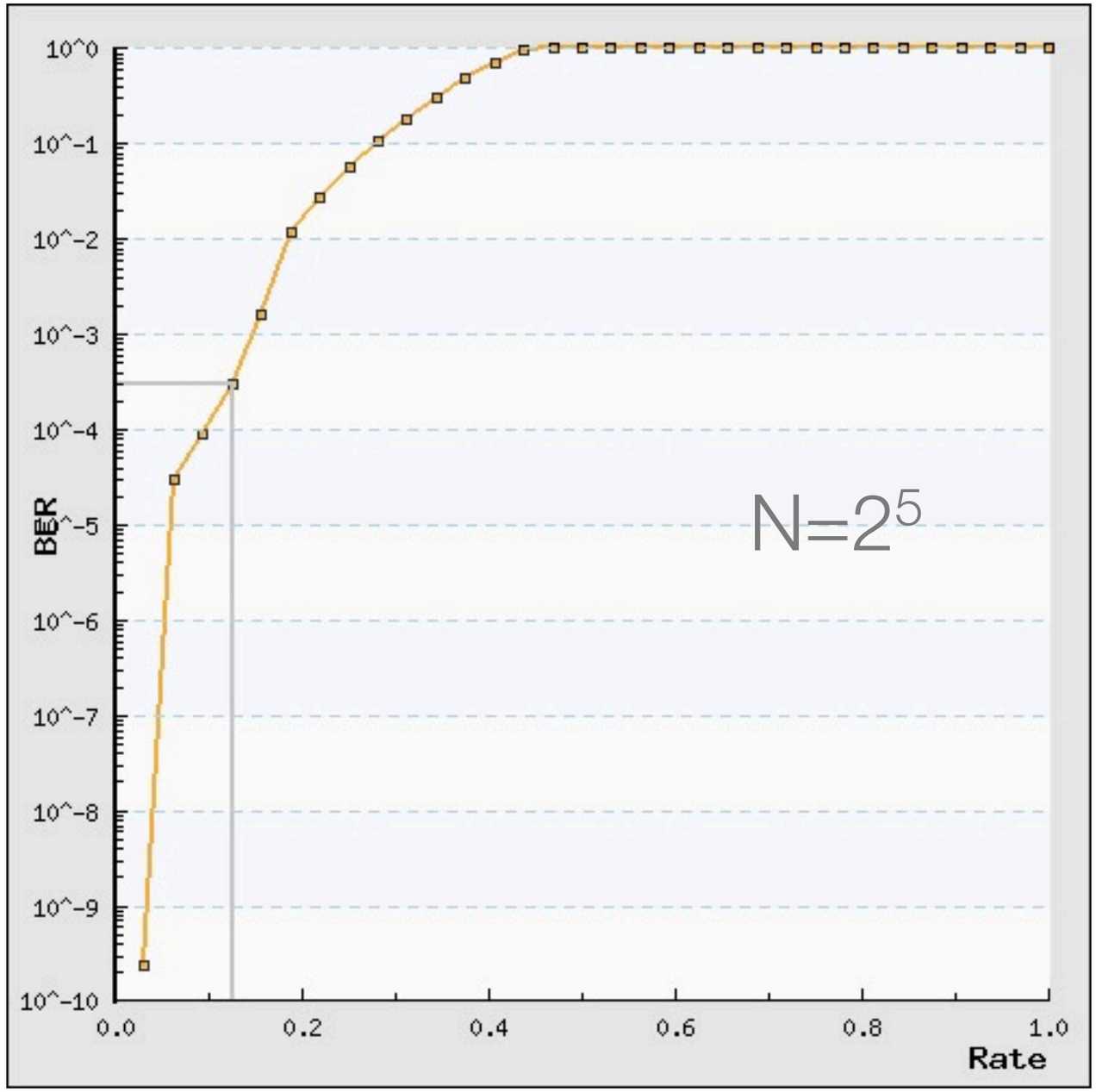
Channel Polarization



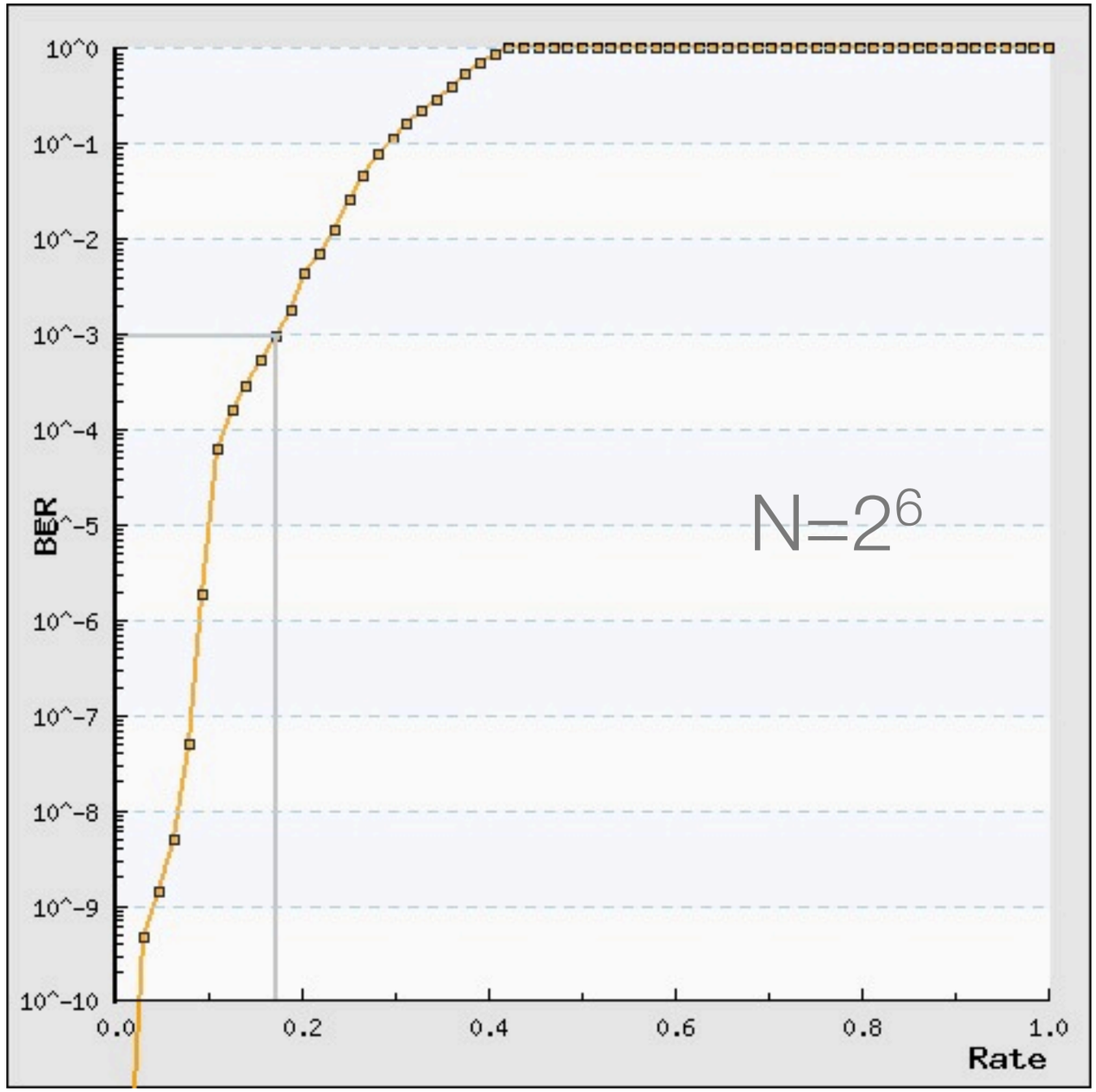
Channel Polarization



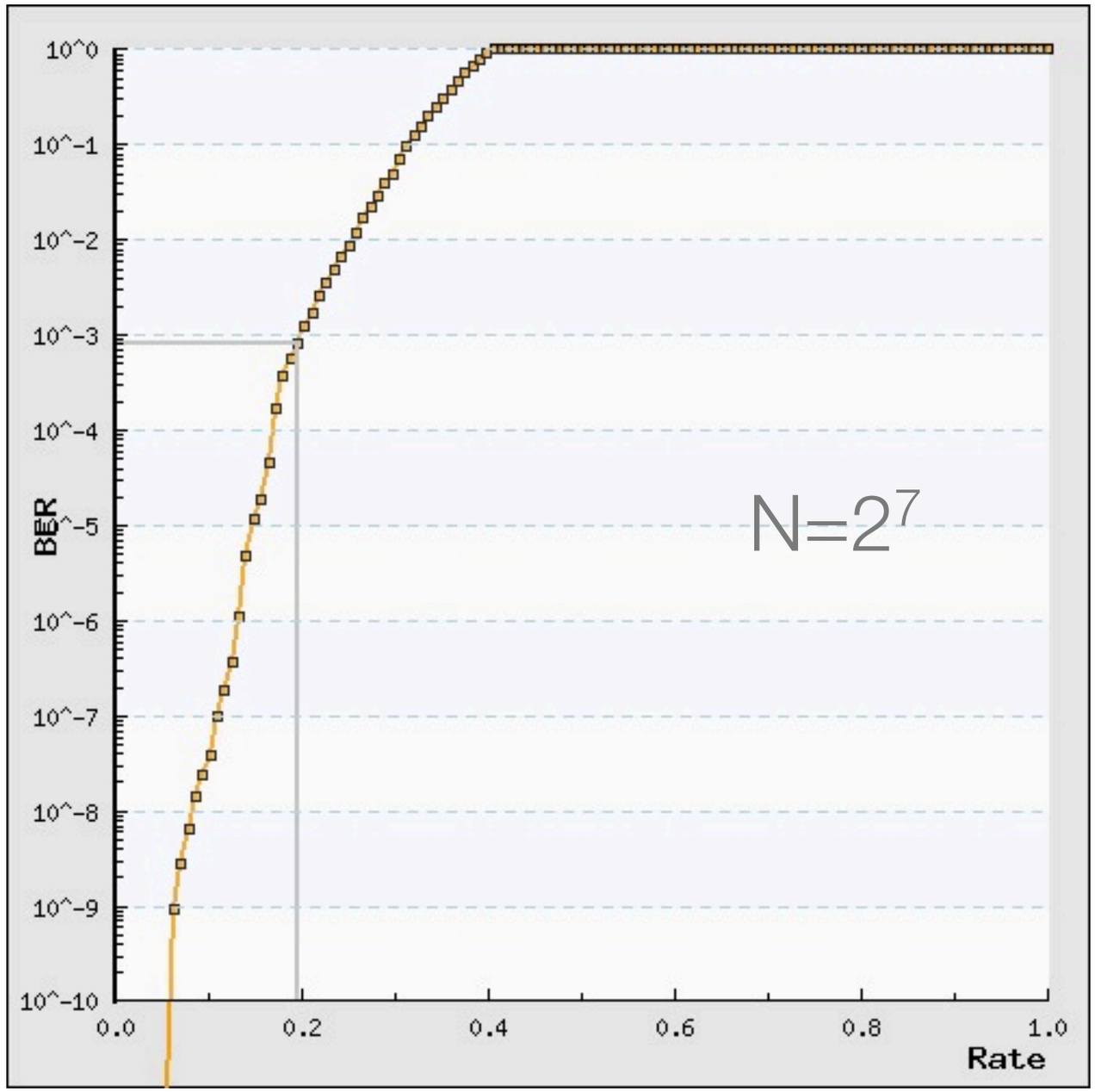
Channel Polarization



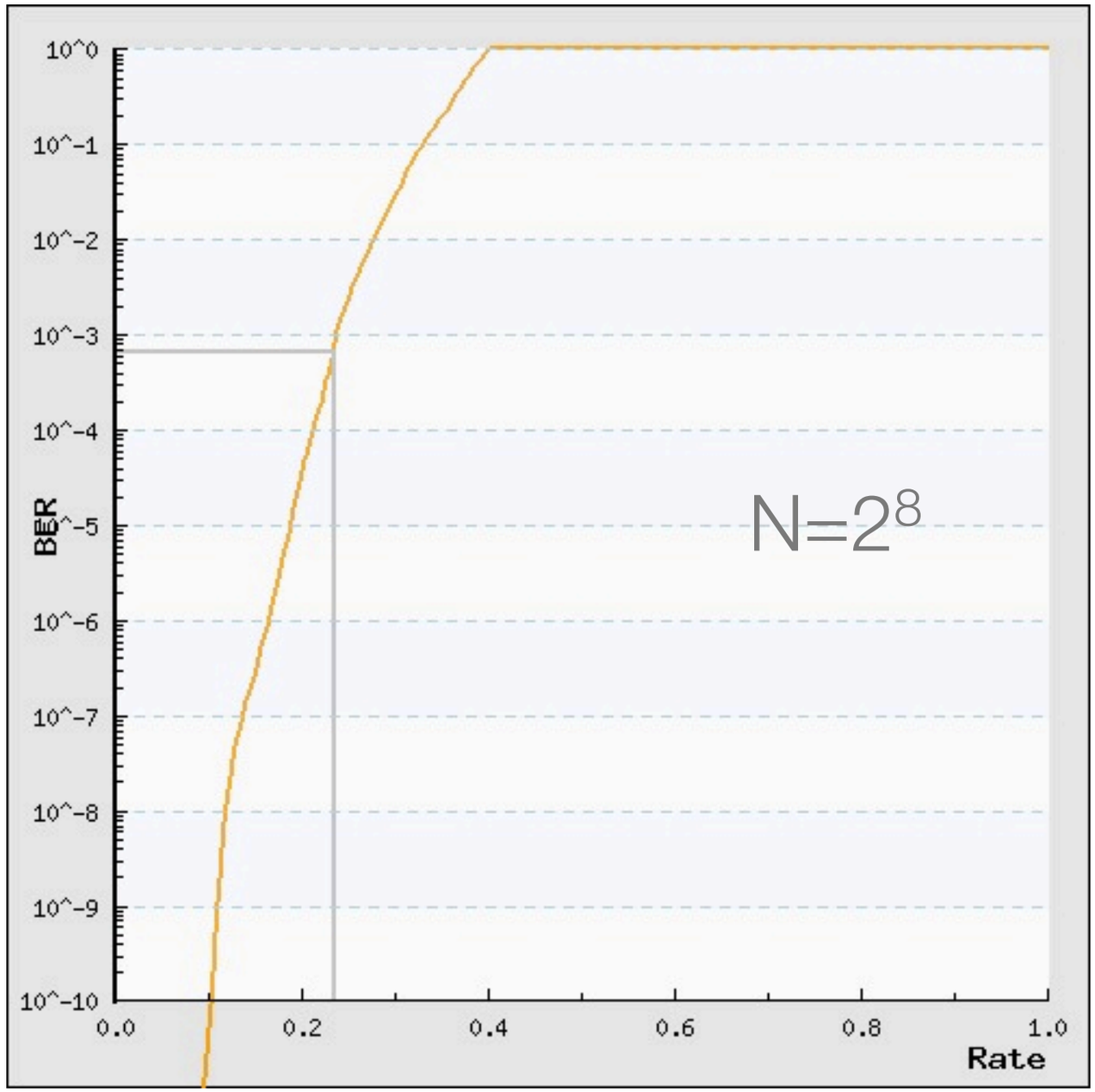
Channel Polarization



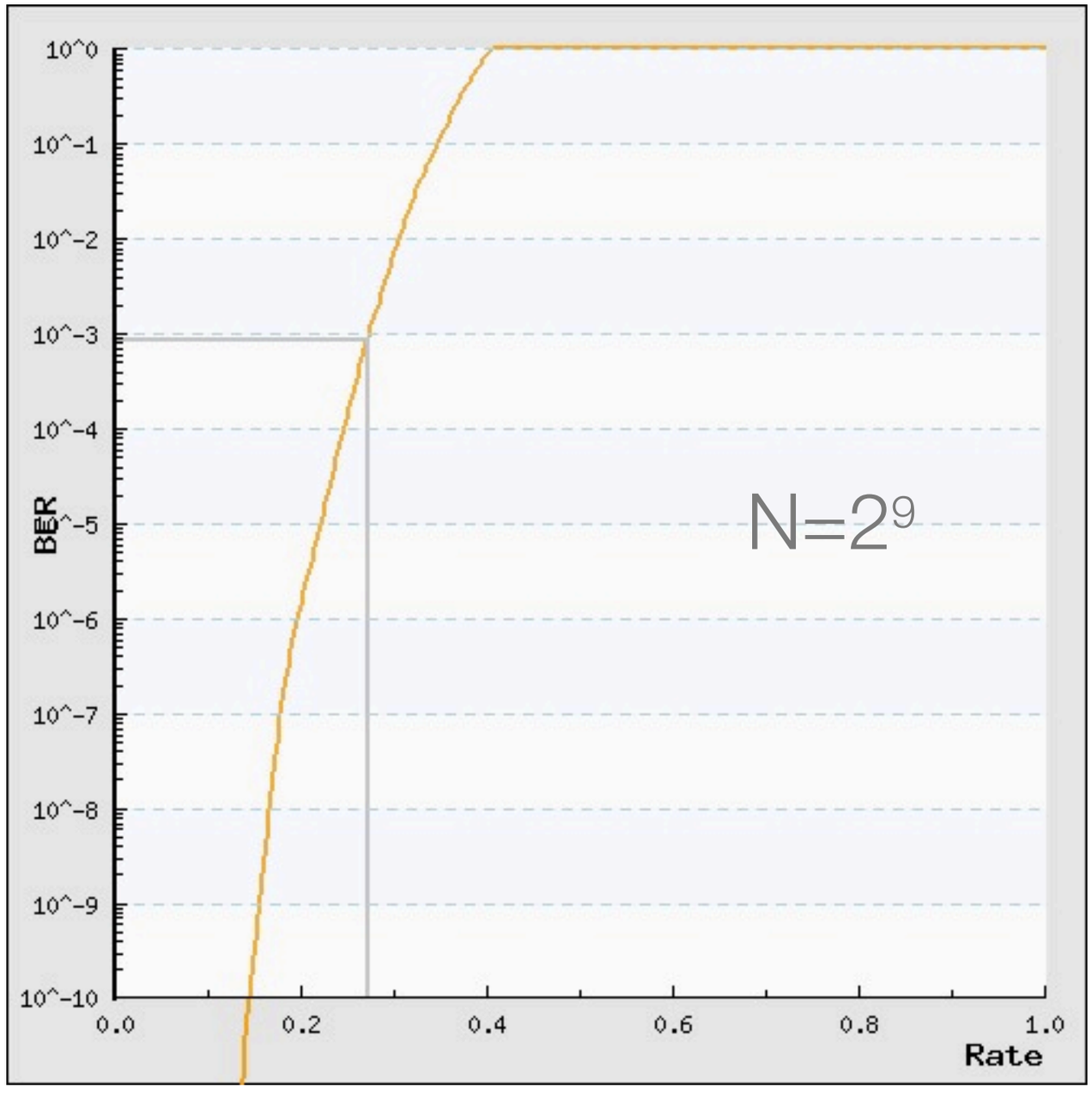
Channel Polarization



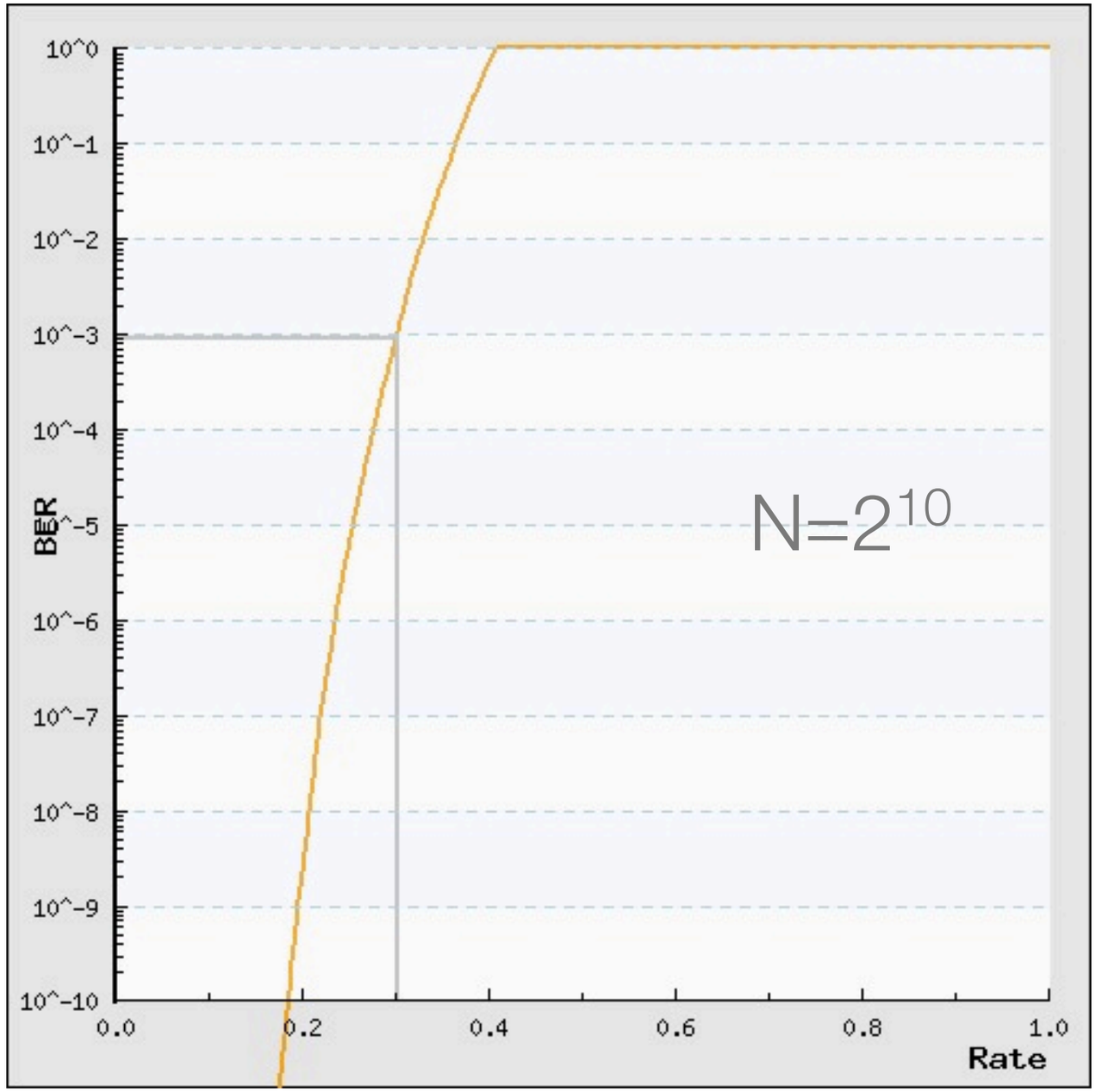
Channel Polarization



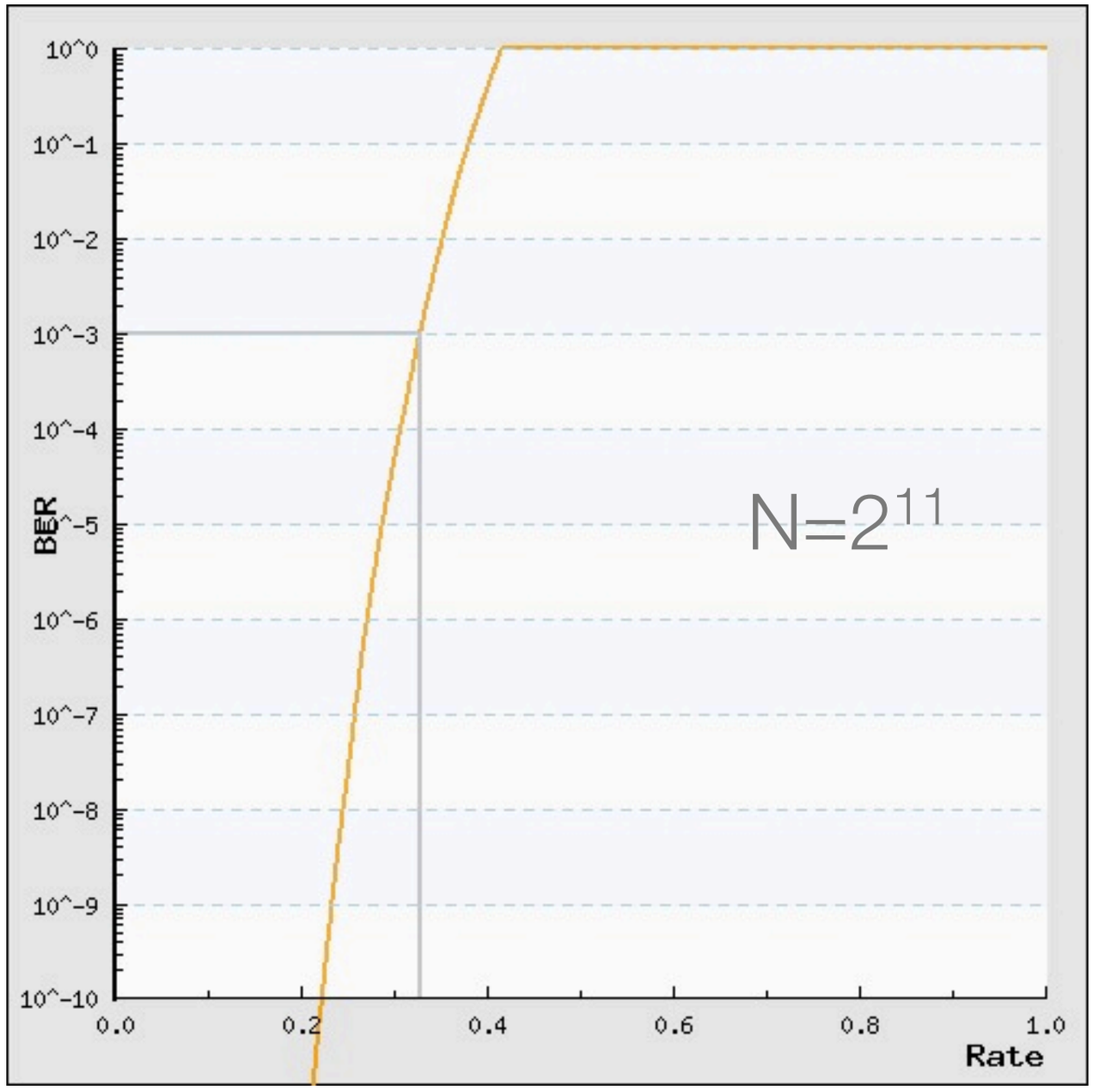
Channel Polarization



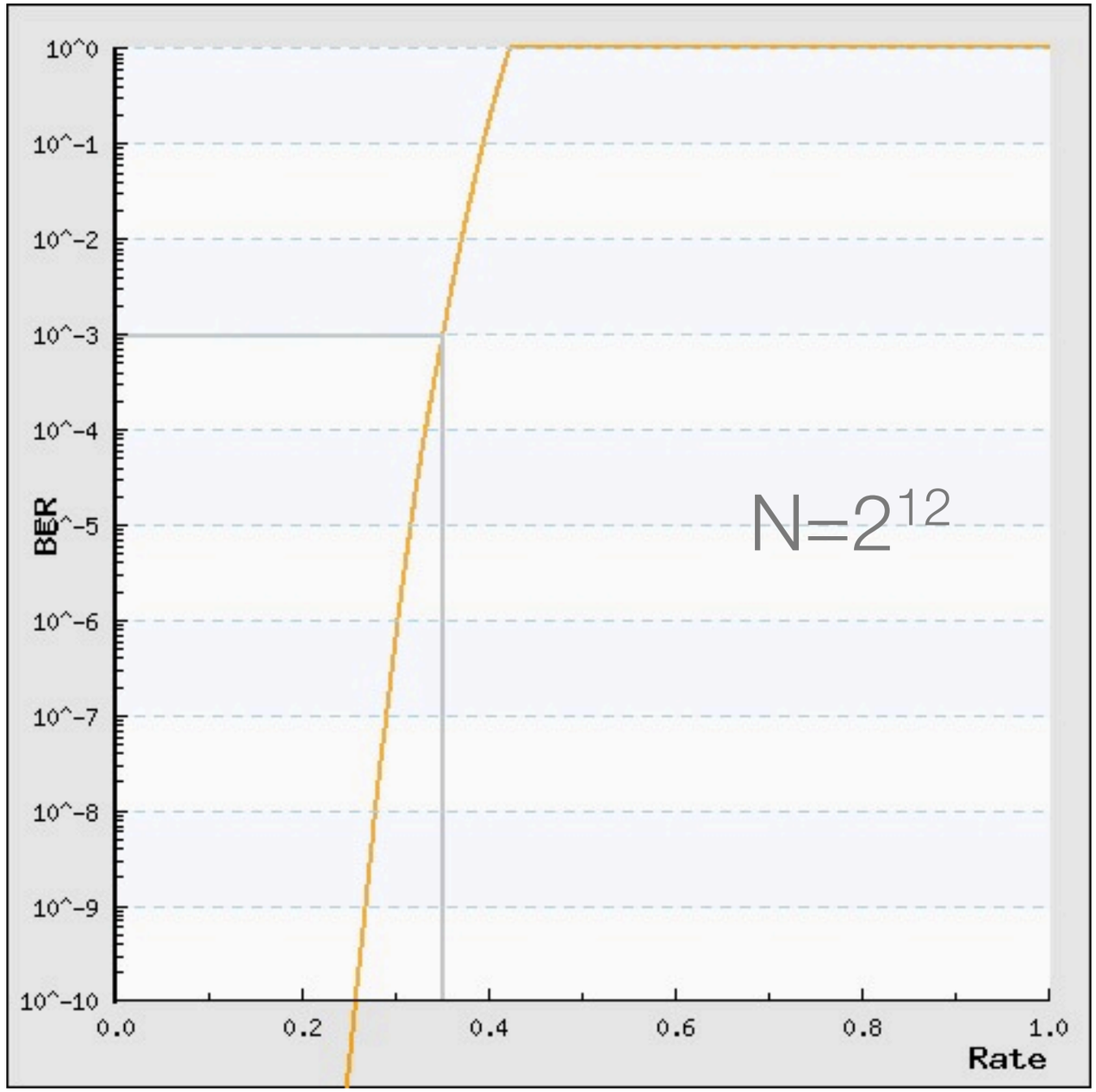
Channel Polarization



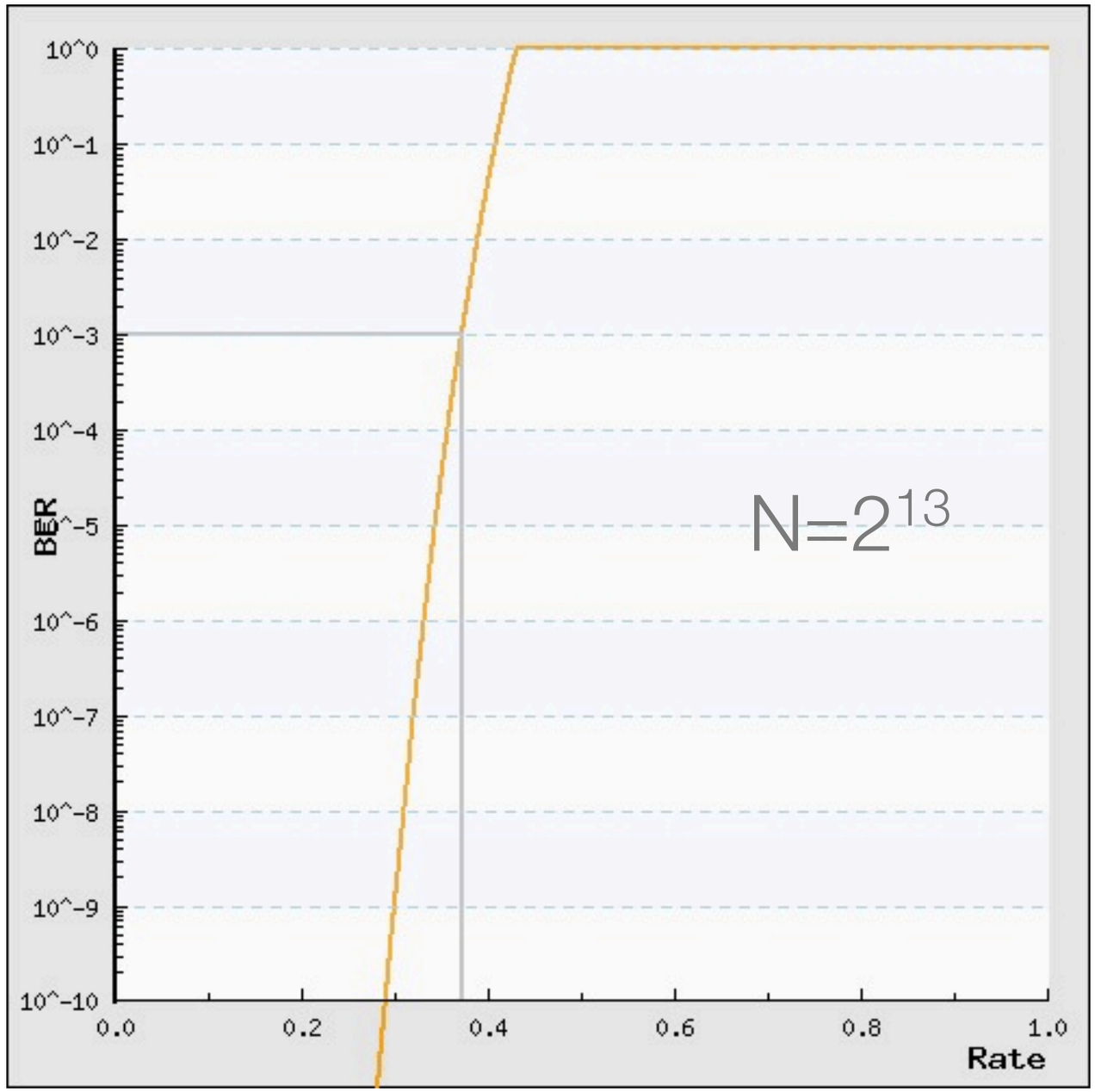
Channel Polarization



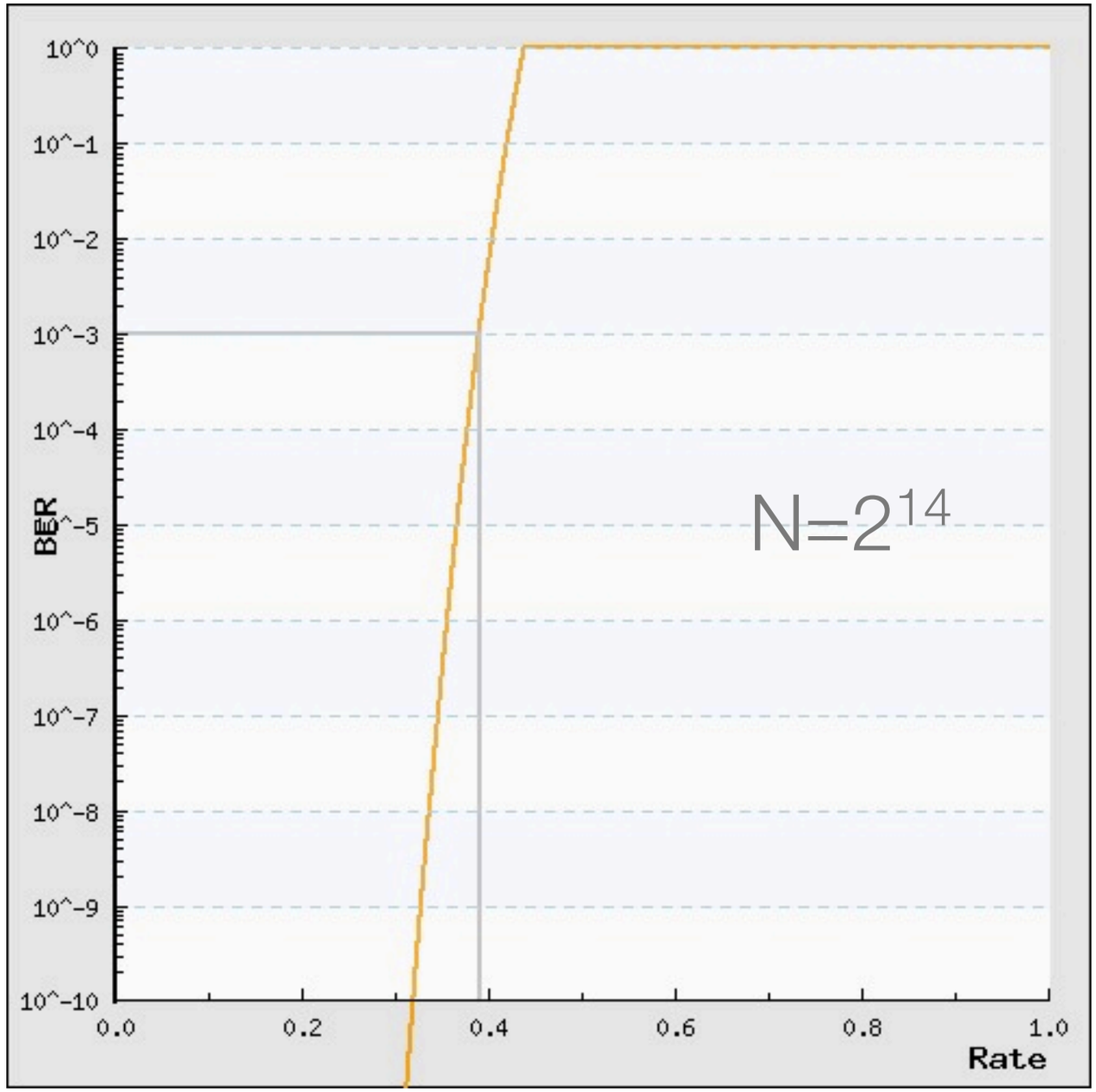
Channel Polarization



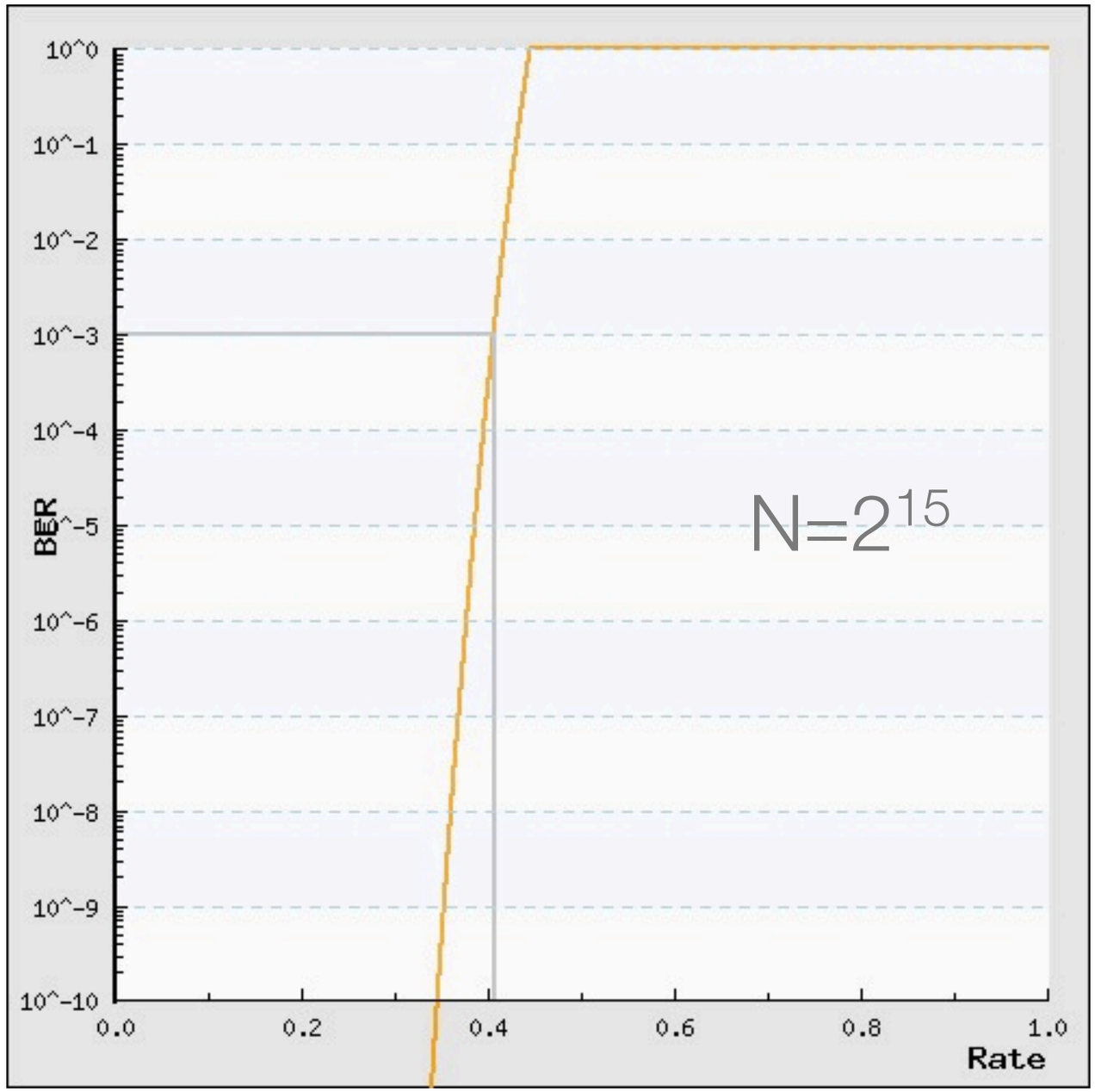
Channel Polarization



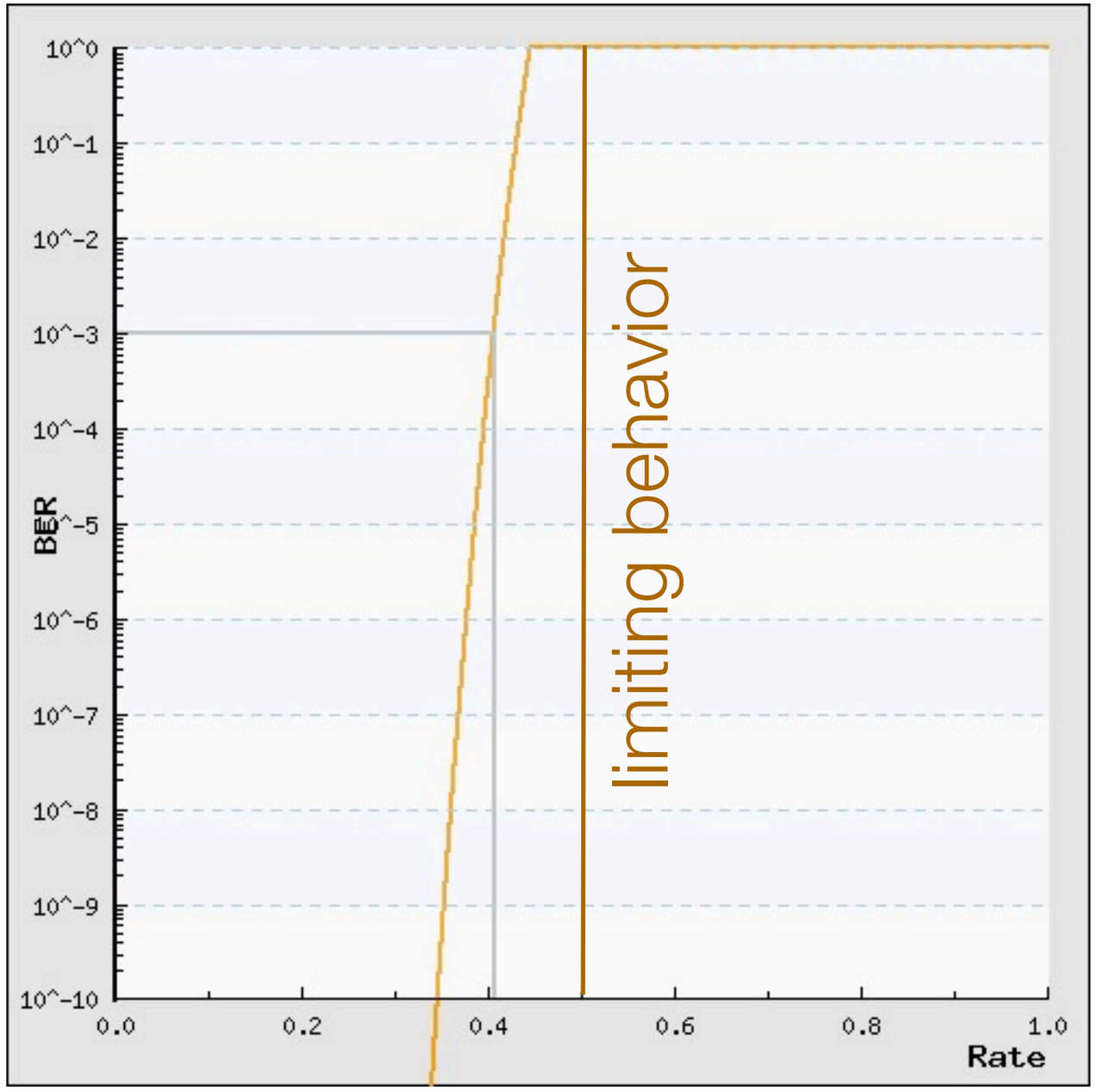
Channel Polarization



Channel Polarization

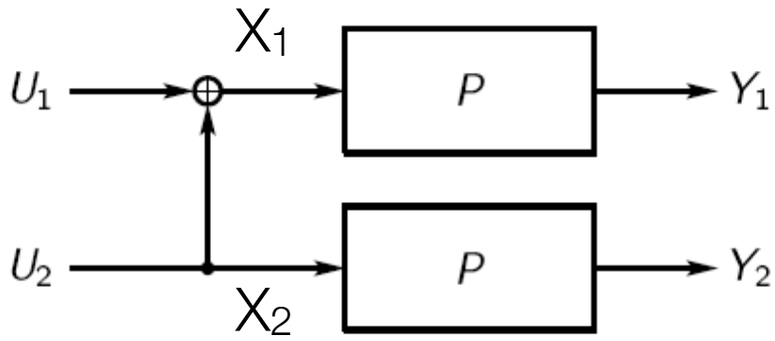


Channel Polarization

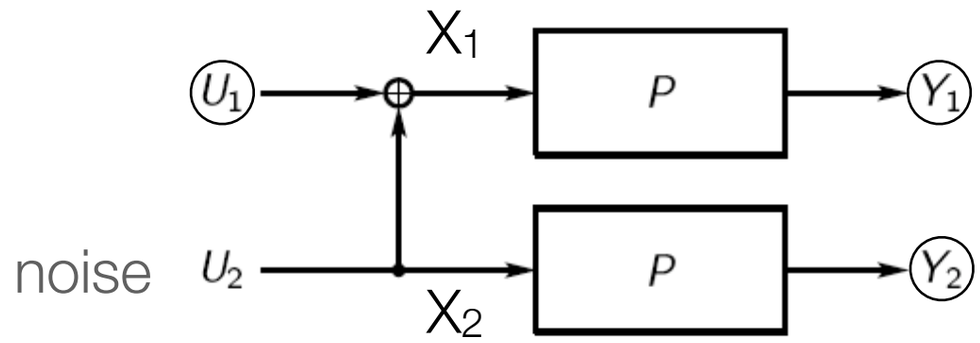


How do channels polarize?

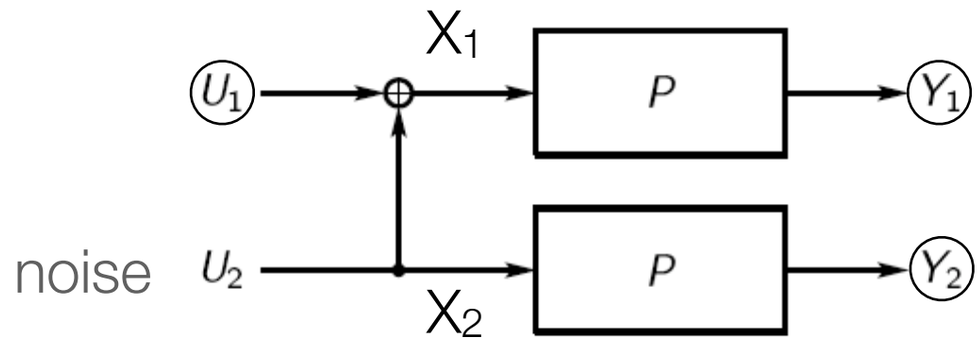
How do channels polarize?



How do channels polarize?

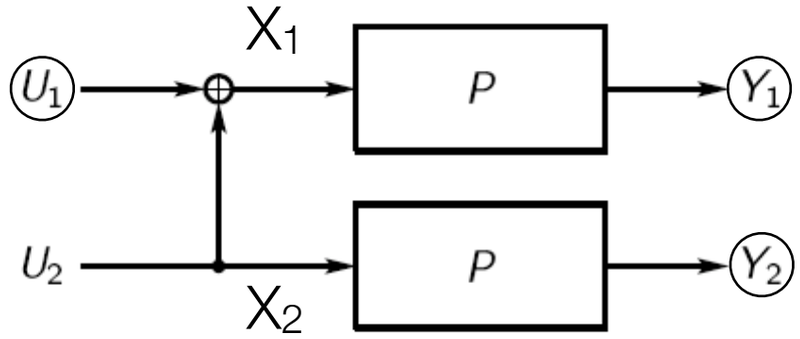


How do channels polarize?

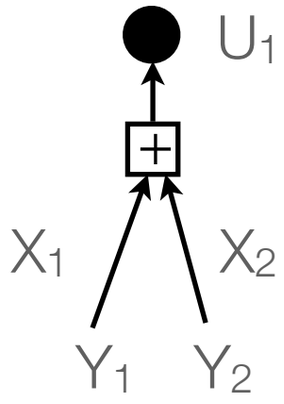


$U_1 = X_1 + X_2$; observe Y_1 and Y_2

How do channels polarize?

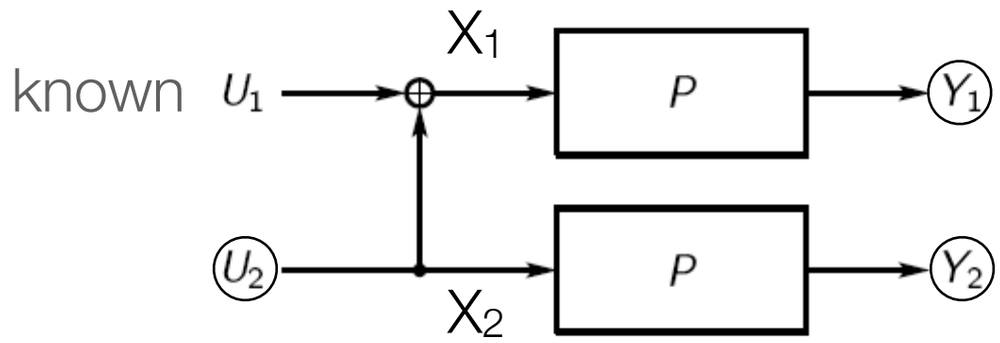


$U_1 = X_1 + X_2$; observe Y_1 and Y_2

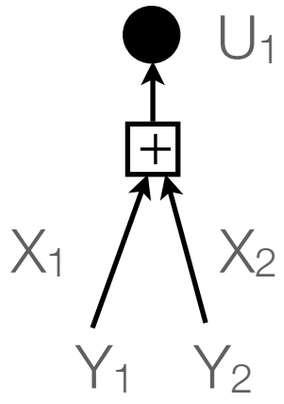


parity-check node

How do channels polarize?

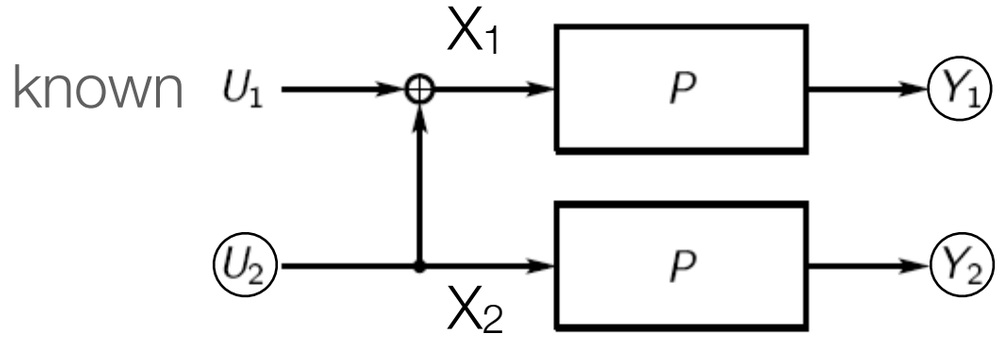


$U_1 = X_1 + X_2$; observe Y_1 and Y_2

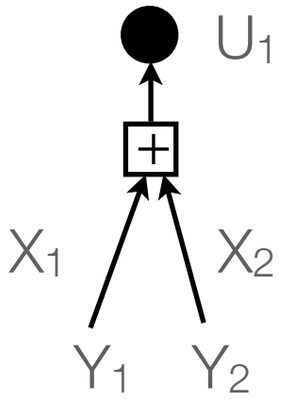


parity-check node

How do channels polarize?

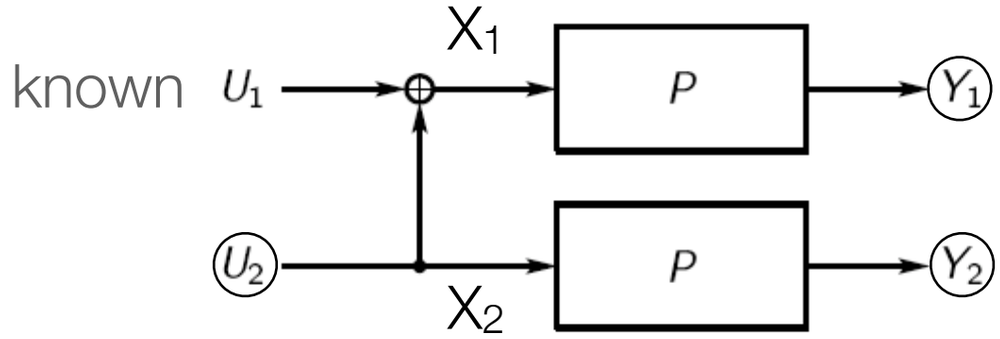


$U_1 = X_1 + X_2$; observe Y_1 and Y_2 $U_2 = X_2$; $U_2 = X_1 + U_1$; observe Y_1 and Y_2

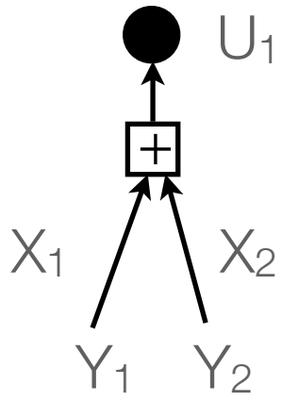


parity-check node

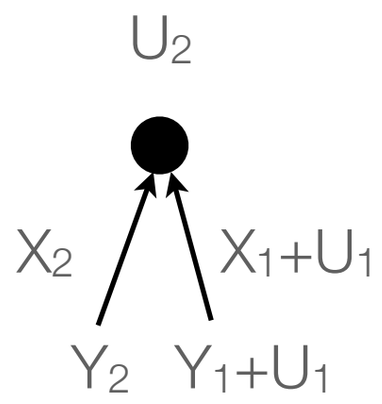
How do channels polarize?



$U_1 = X_1 + X_2$; observe Y_1 and Y_2 $U_2 = X_2$; $U_2 = X_1 + U_1$; observe Y_1 and Y_2

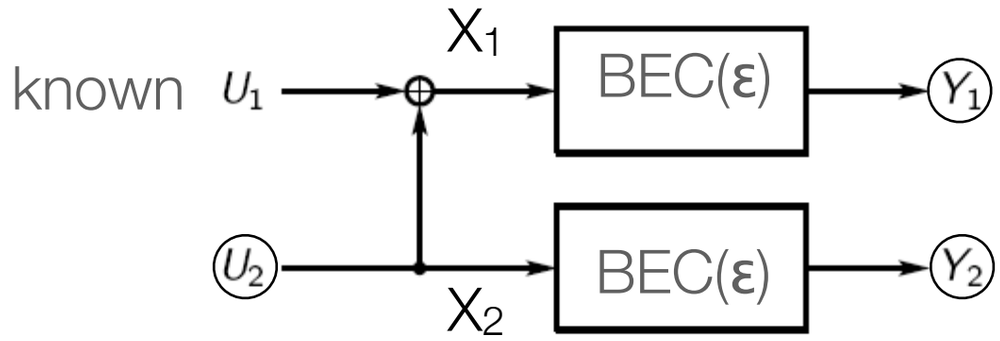


parity-check node

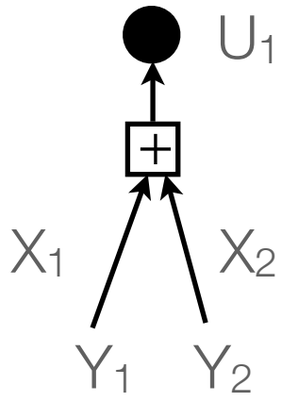


repetition code

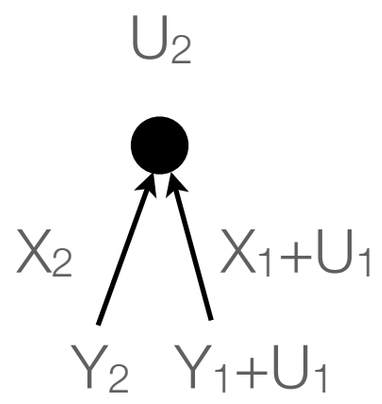
How do channels polarize?



$U_1 = X_1 + X_2$; observe Y_1 and Y_2 $U_2 = X_2$; $U_2 = X_1 + U_1$; observe Y_1 and Y_2

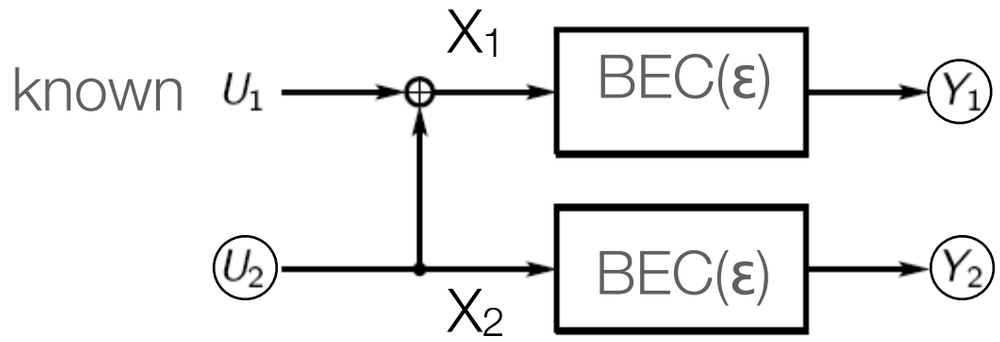


parity-check node

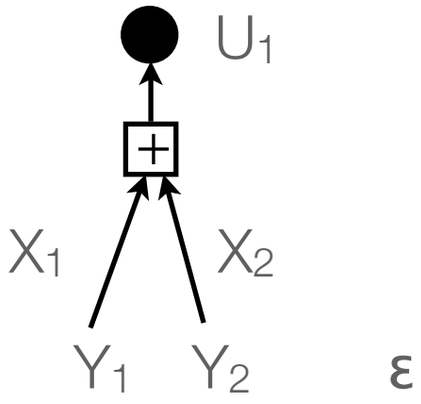


repetition code

How do channels polarize?

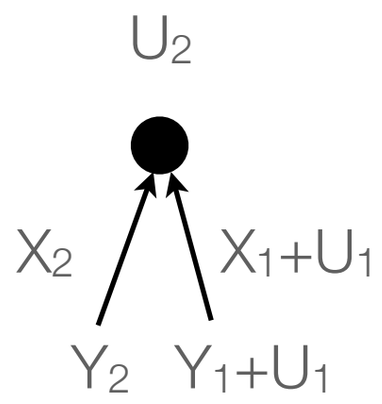


$U_1 = X_1 + X_2$; observe Y_1 and Y_2 $U_2 = X_2$; $U_2 = X_1 + U_1$; observe Y_1 and Y_2



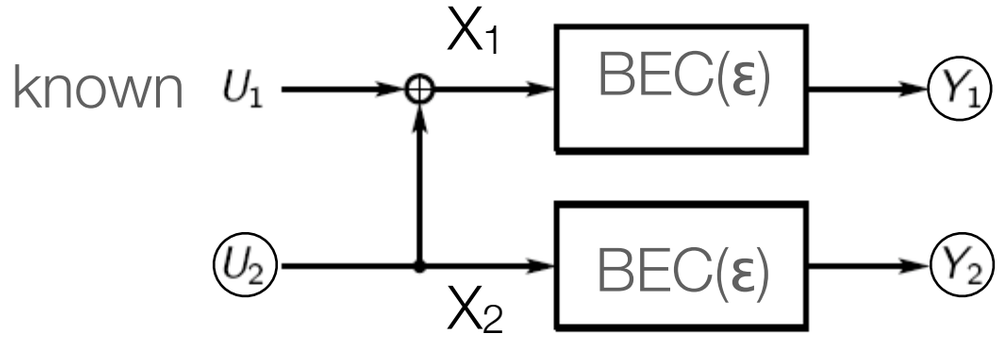
ε

parity-check node

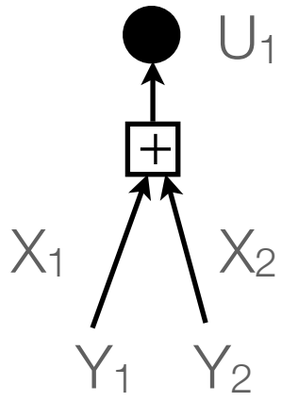


repetition code

How do channels polarize?



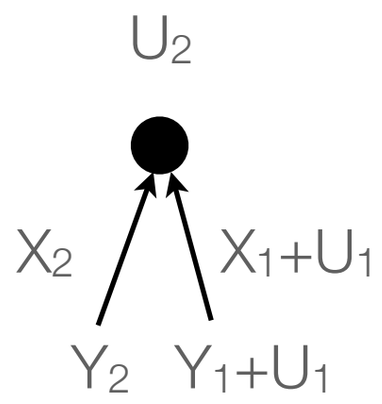
$U_1 = X_1 + X_2$; observe Y_1 and Y_2 $U_2 = X_2$; $U_2 = X_1 + U_1$; observe Y_1 and Y_2



$1-(1-\varepsilon)^2$
much worse

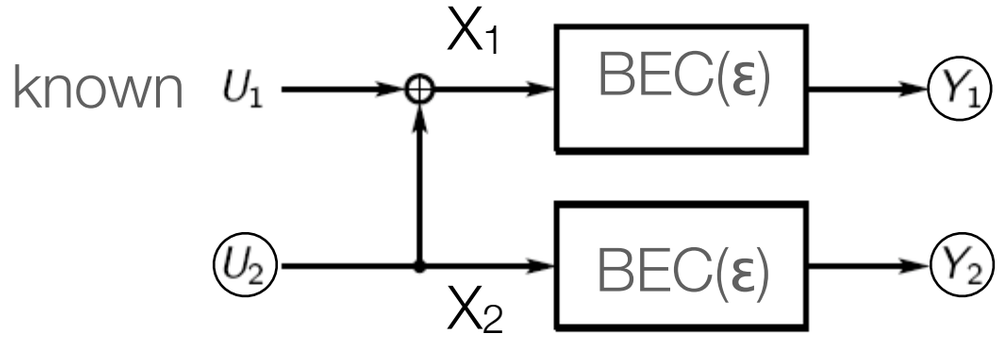
ε

parity-check node

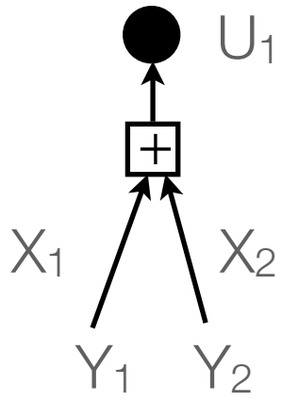


repetition code

How do channels polarize?



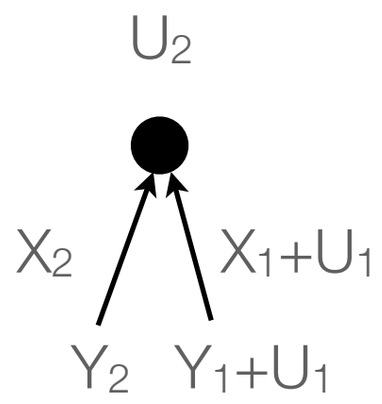
$U_1 = X_1 + X_2$; observe Y_1 and Y_2 $U_2 = X_2$; $U_2 = X_1 + U_1$; observe Y_1 and Y_2



$1-(1-\varepsilon)^2$
much worse

ε

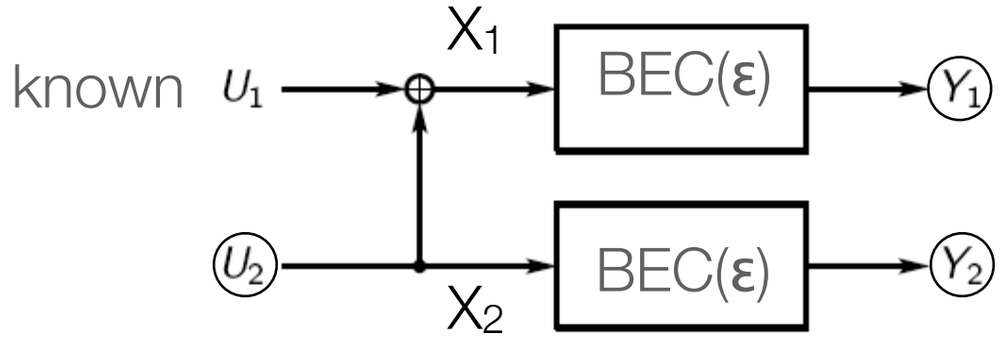
parity-check node



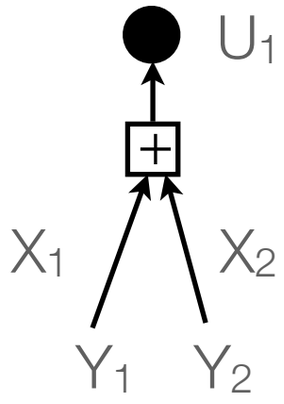
ε

repetition code

How do channels polarize?



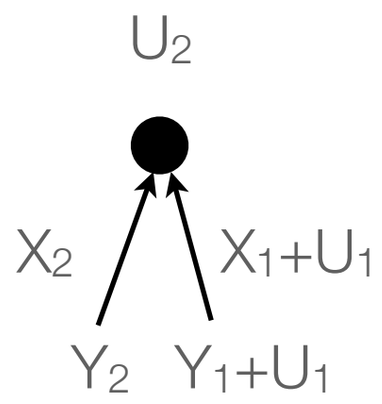
$U_1 = X_1 + X_2$; observe Y_1 and Y_2 $U_2 = X_2$; $U_2 = X_1 + U_1$; observe Y_1 and Y_2



$1-(1-\varepsilon)^2$
much worse

ε

parity-check node

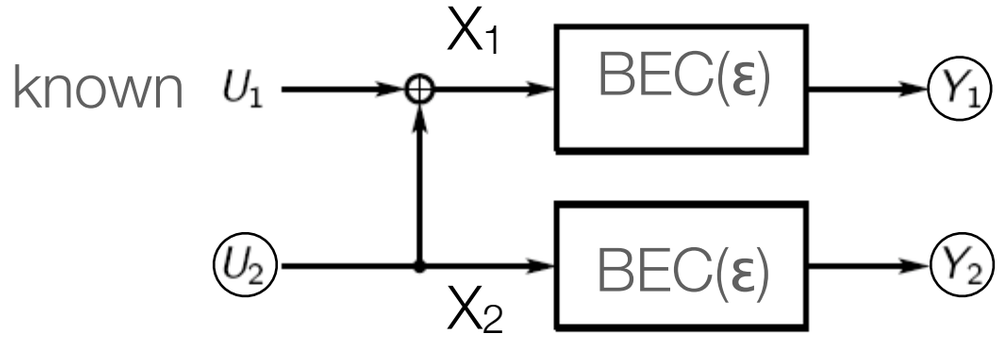


ε^2 much better

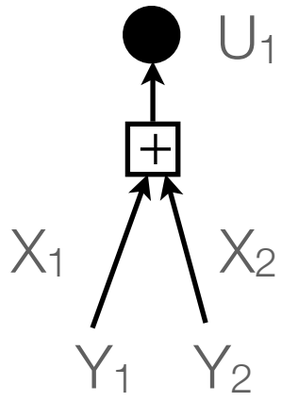
ε

repetition code

How do channels polarize?



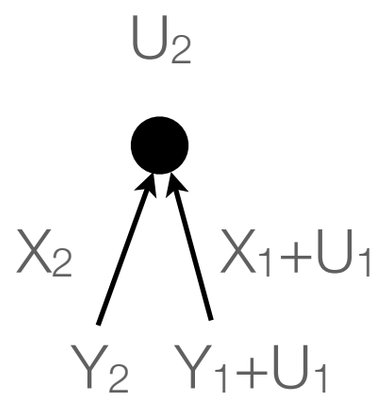
$U_1 = X_1 + X_2$; observe Y_1 and Y_2 $U_2 = X_2$; $U_2 = X_1 + U_1$; observe Y_1 and Y_2



$1-(1-\varepsilon)^2$
much worse

ε

parity-check node



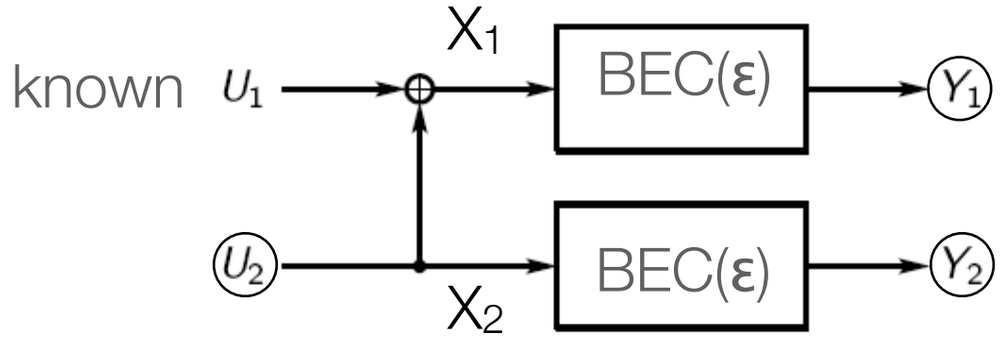
ε^2 much better

ε

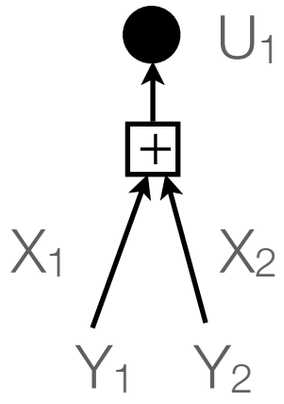
repetition code

total capacity = $(1-\varepsilon)^2+1-\varepsilon^2=2(1-\varepsilon)$

How do channels polarize?



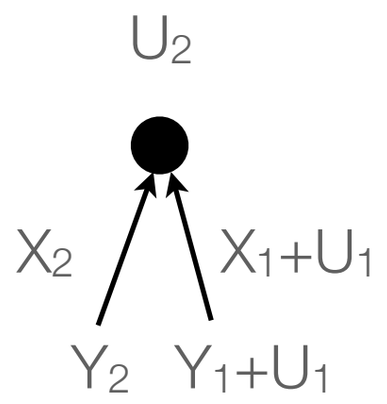
$U_1 = X_1 + X_2$; observe Y_1 and Y_2 $U_2 = X_2$; $U_2 = X_1 + U_1$; observe Y_1 and Y_2



$1-(1-\varepsilon)^2$
much worse

ε

parity-check node



ε^2 much better

ε

repetition code

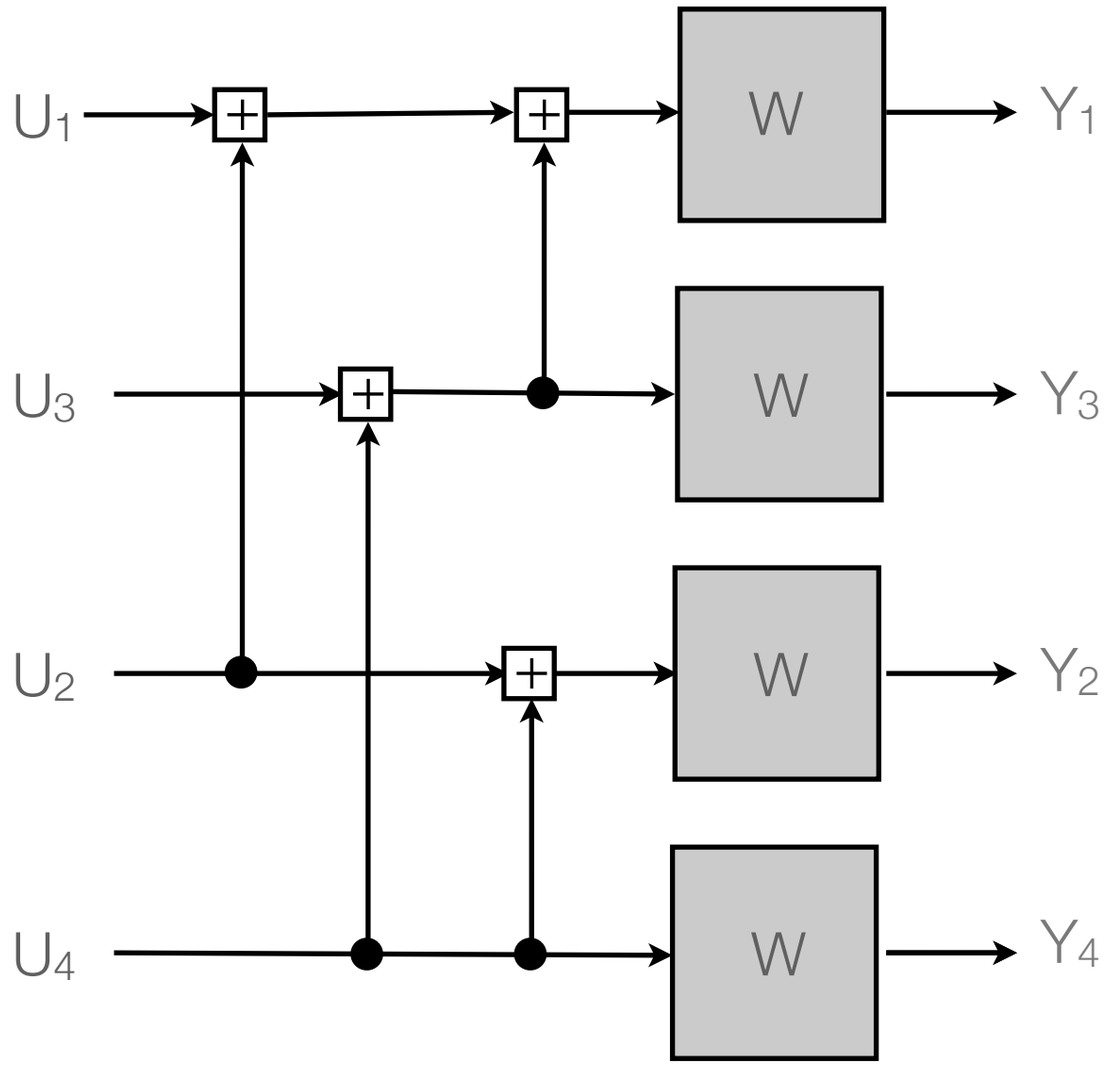
total capacity = $(1-\varepsilon)^2+1-\varepsilon^2=2(1-\varepsilon)$

LEMMA 4.41 (DUALITY RULE FOR ENTROPY). Let a and b denote two symmetric L-densities. Then

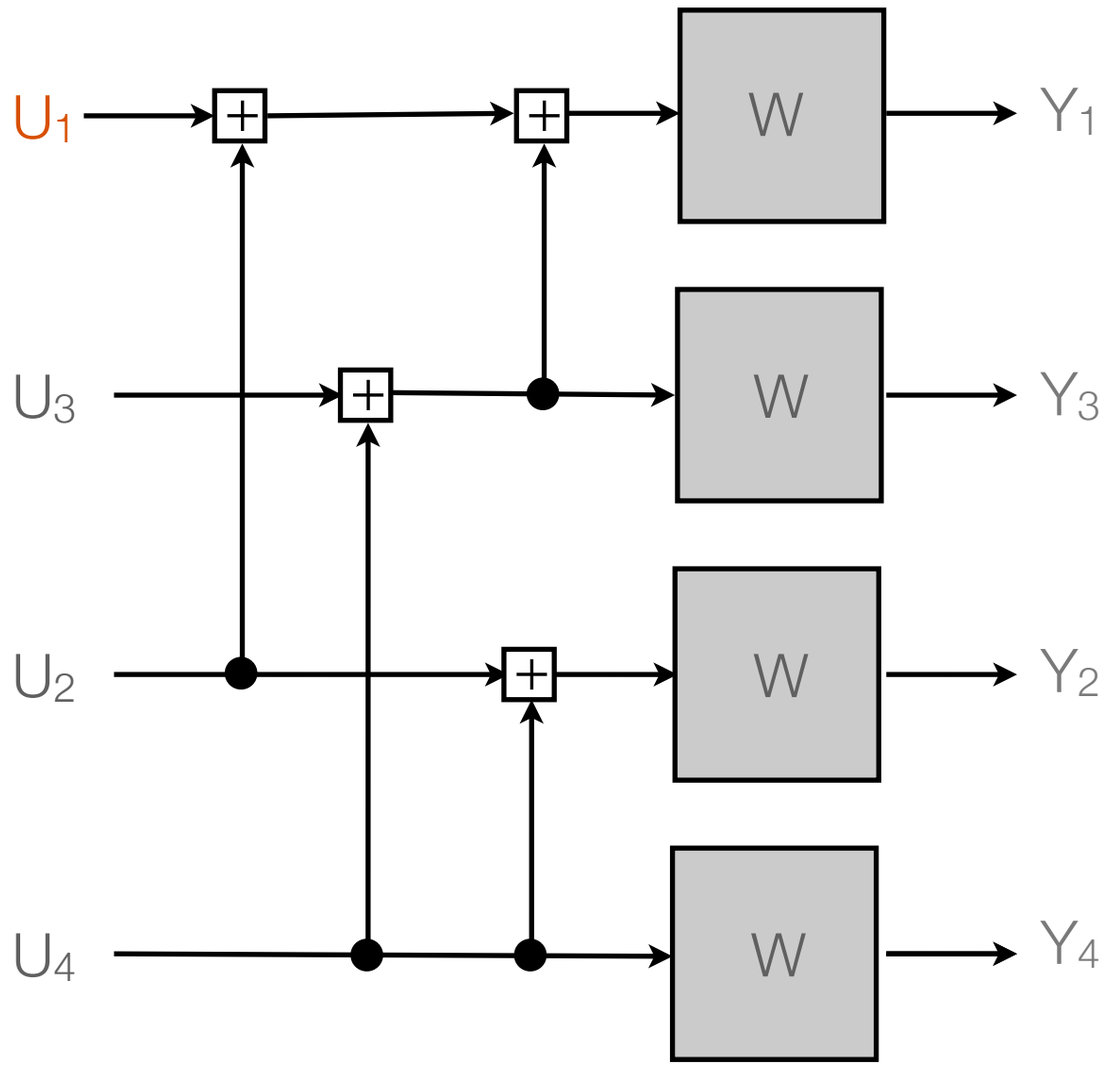
$$H(a \circledast b) + H(a \boxast b) = H(a) + H(b).$$

How do channels polarize?

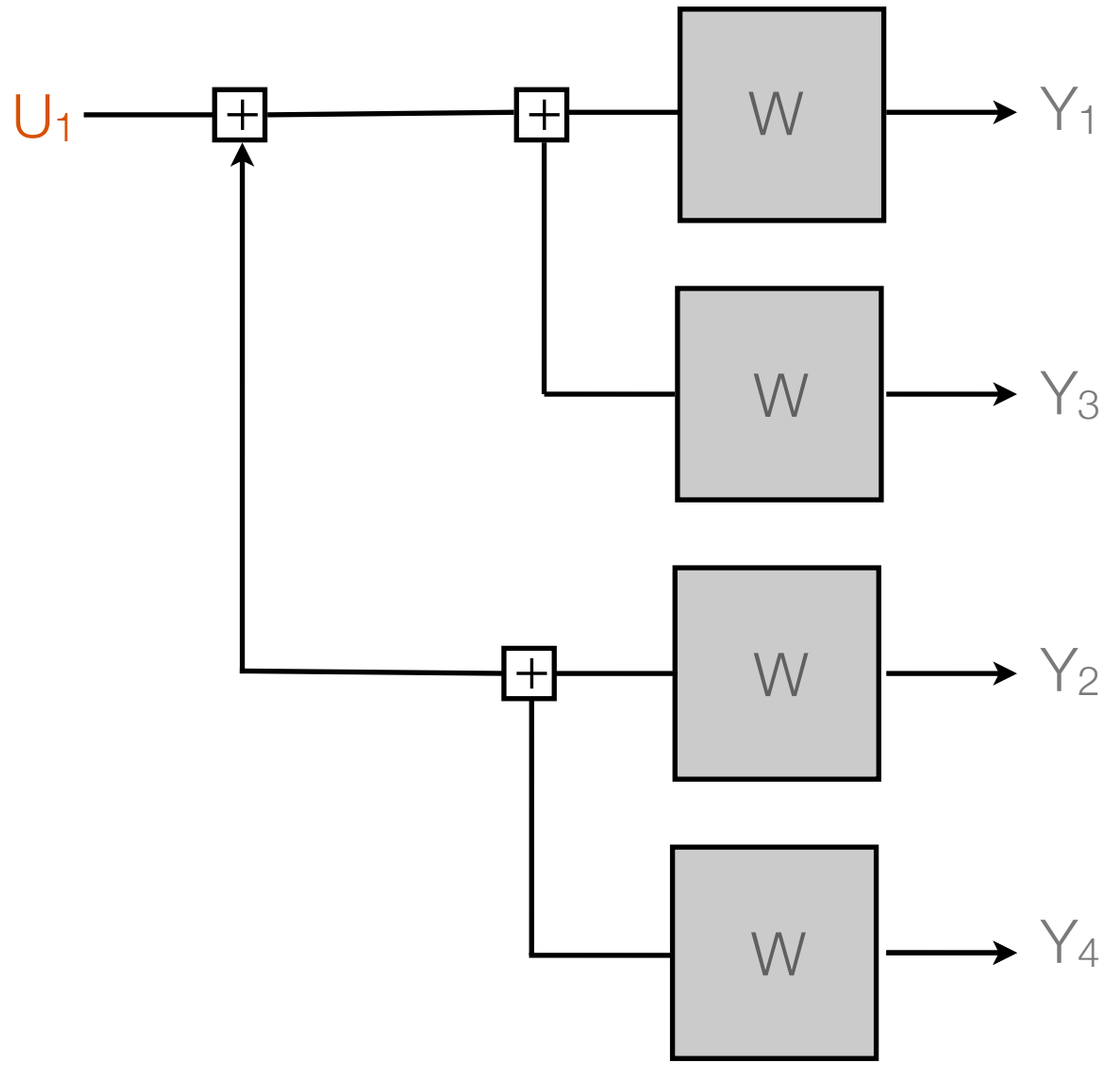
How do channels polarize?



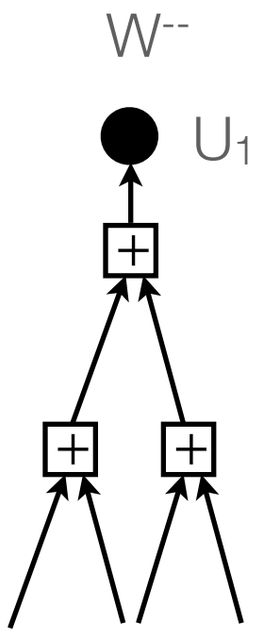
How do channels polarize?

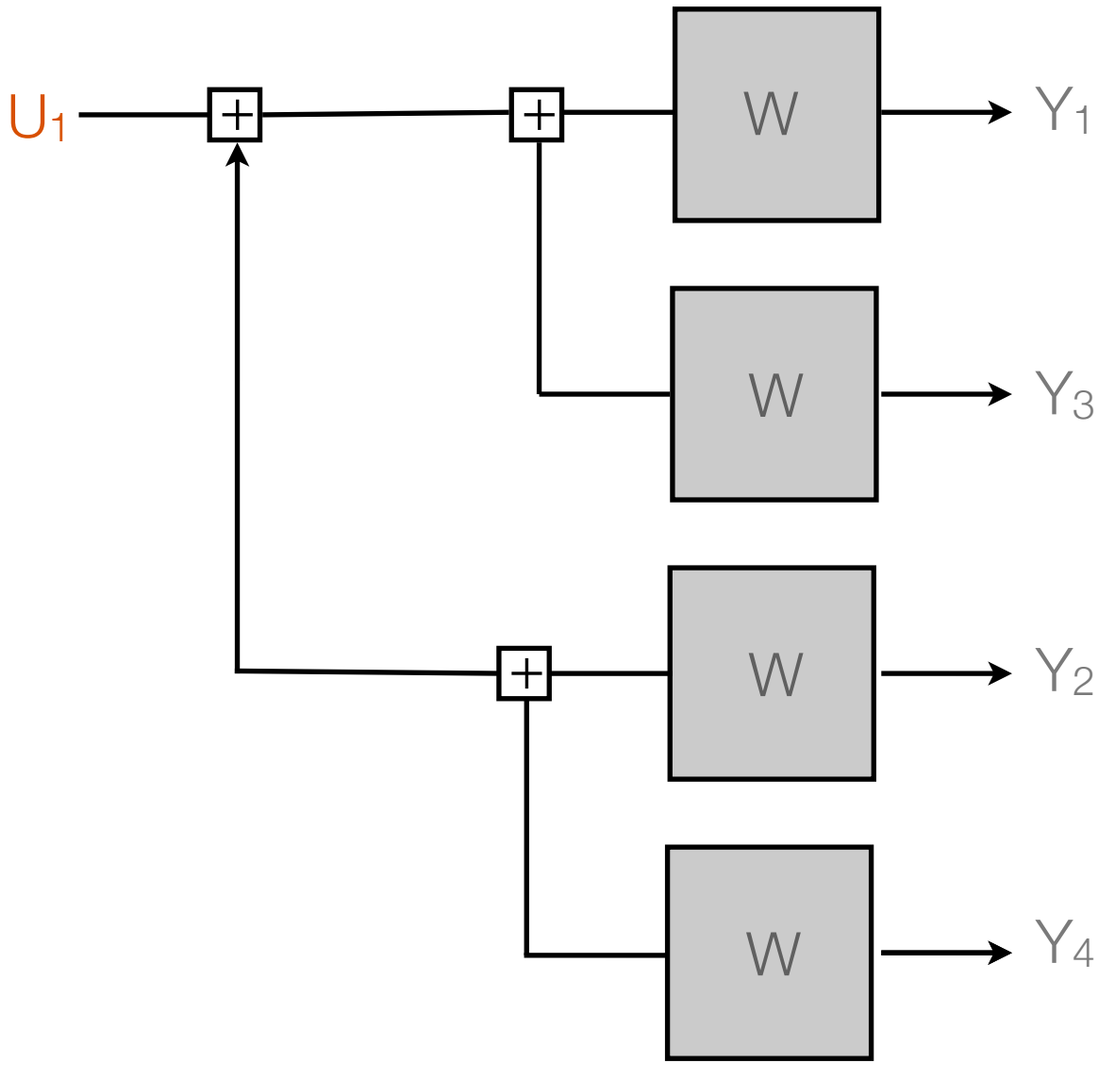


How do channels polarize?

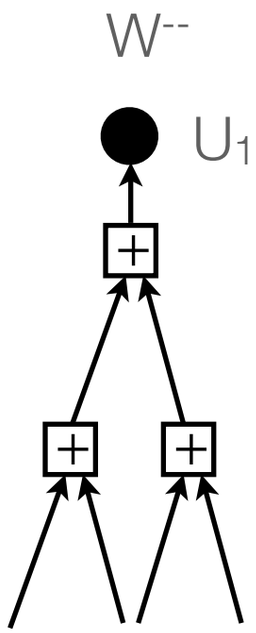


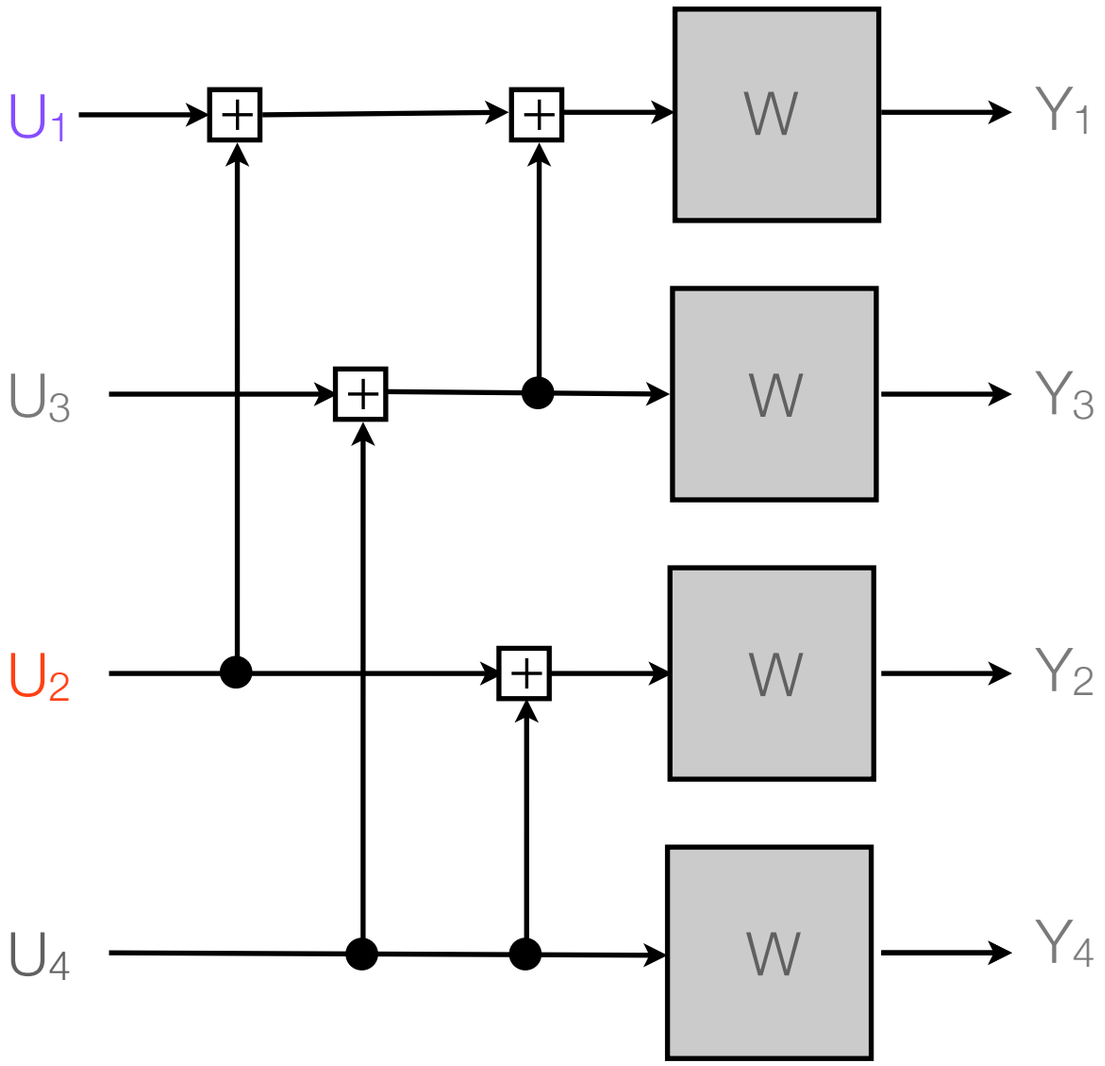
How do channels polarize?



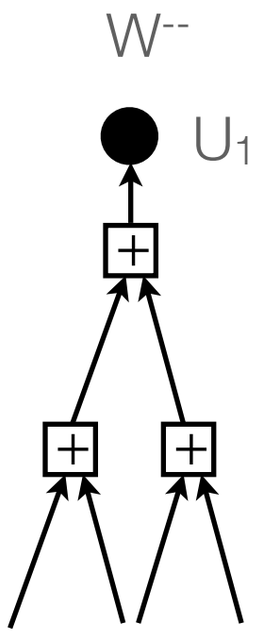


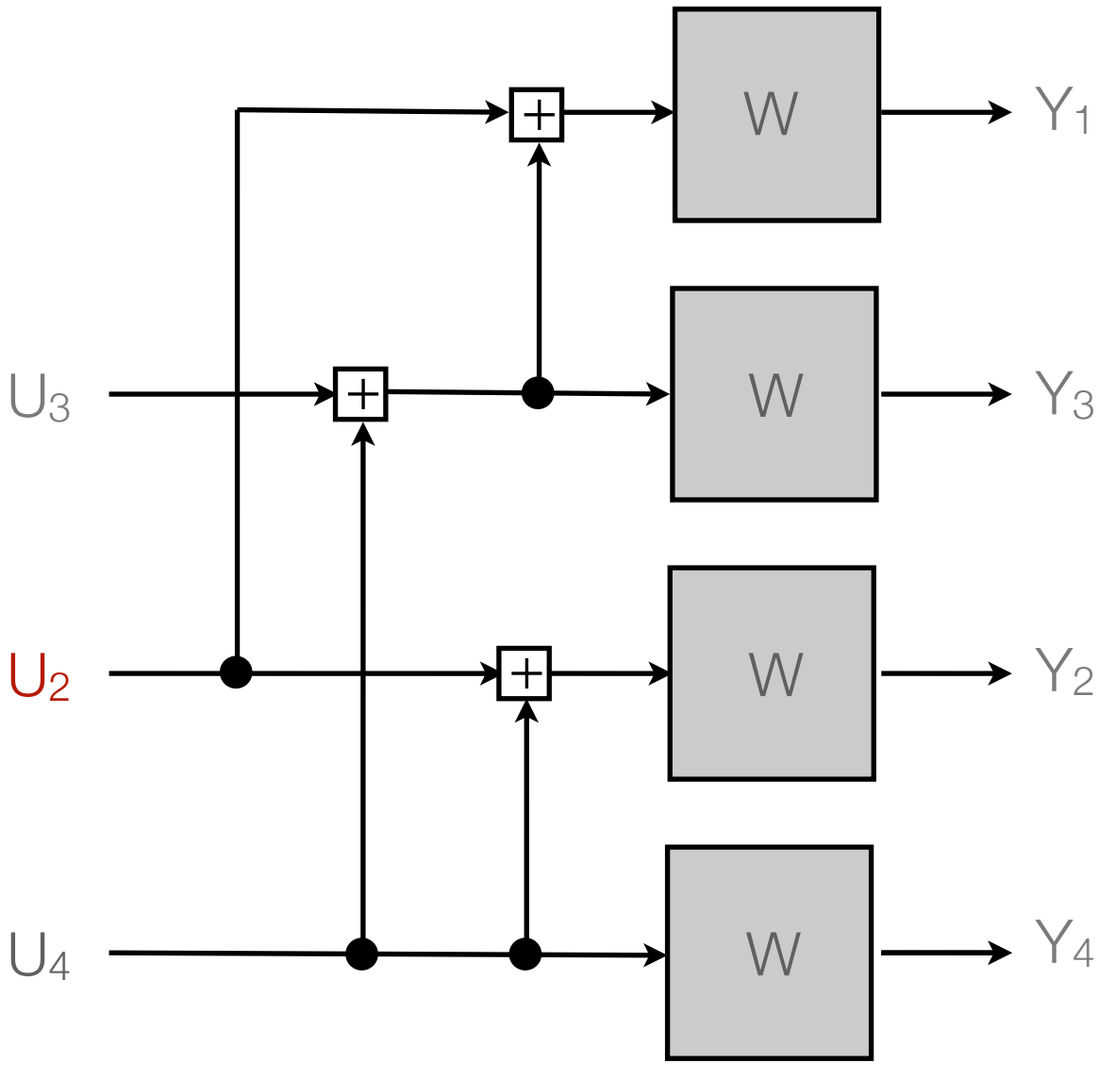
How do channels polarize?



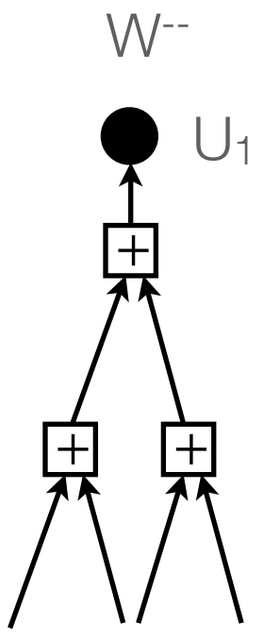


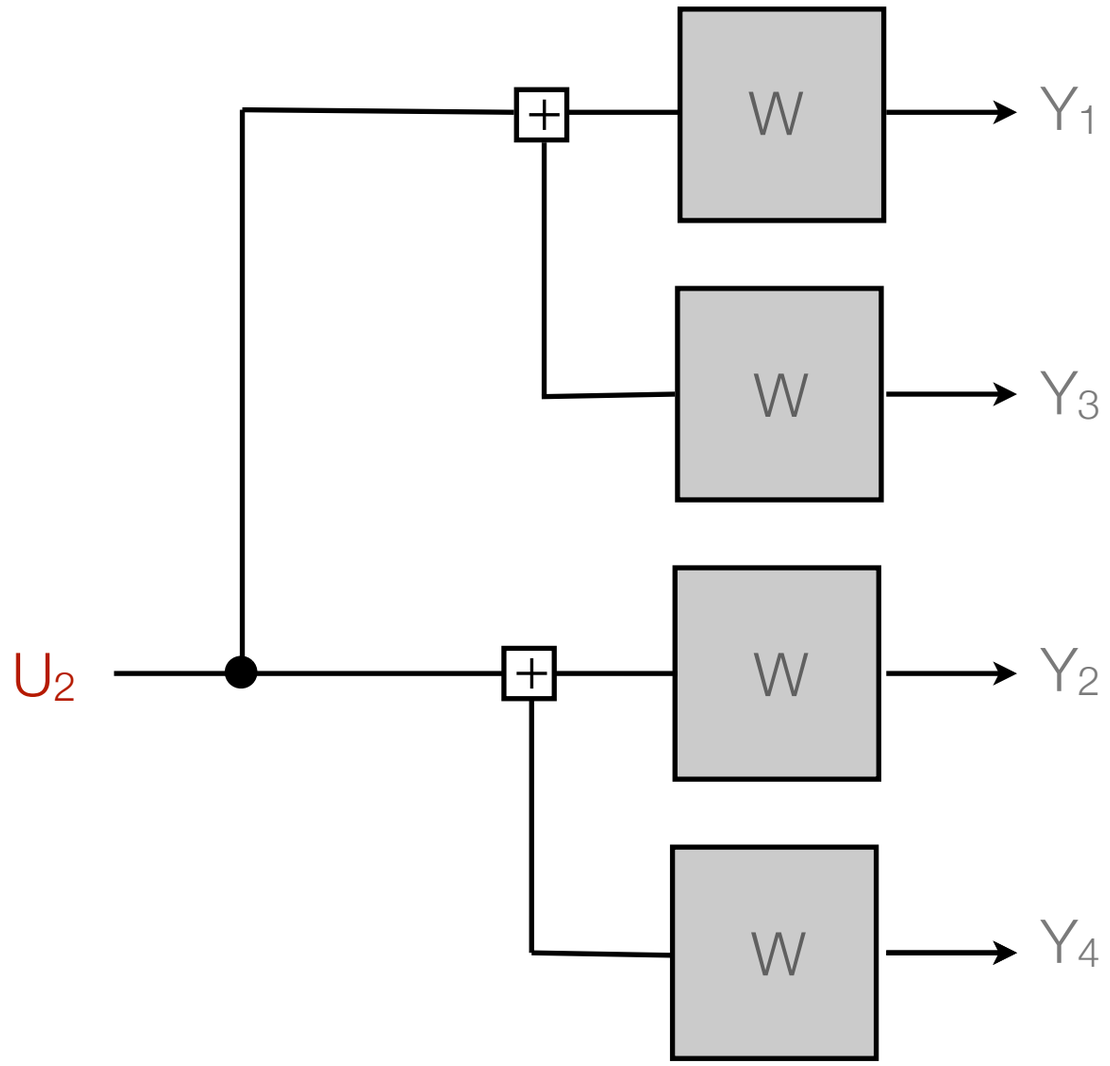
How do channels polarize?



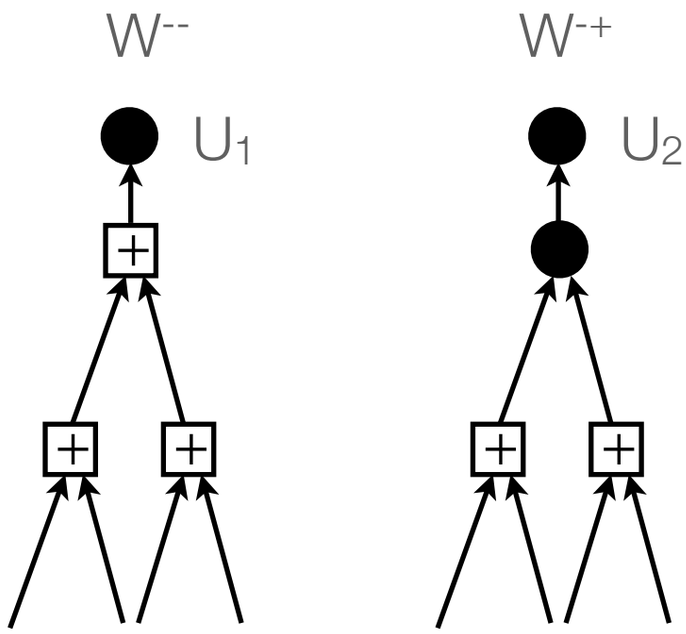


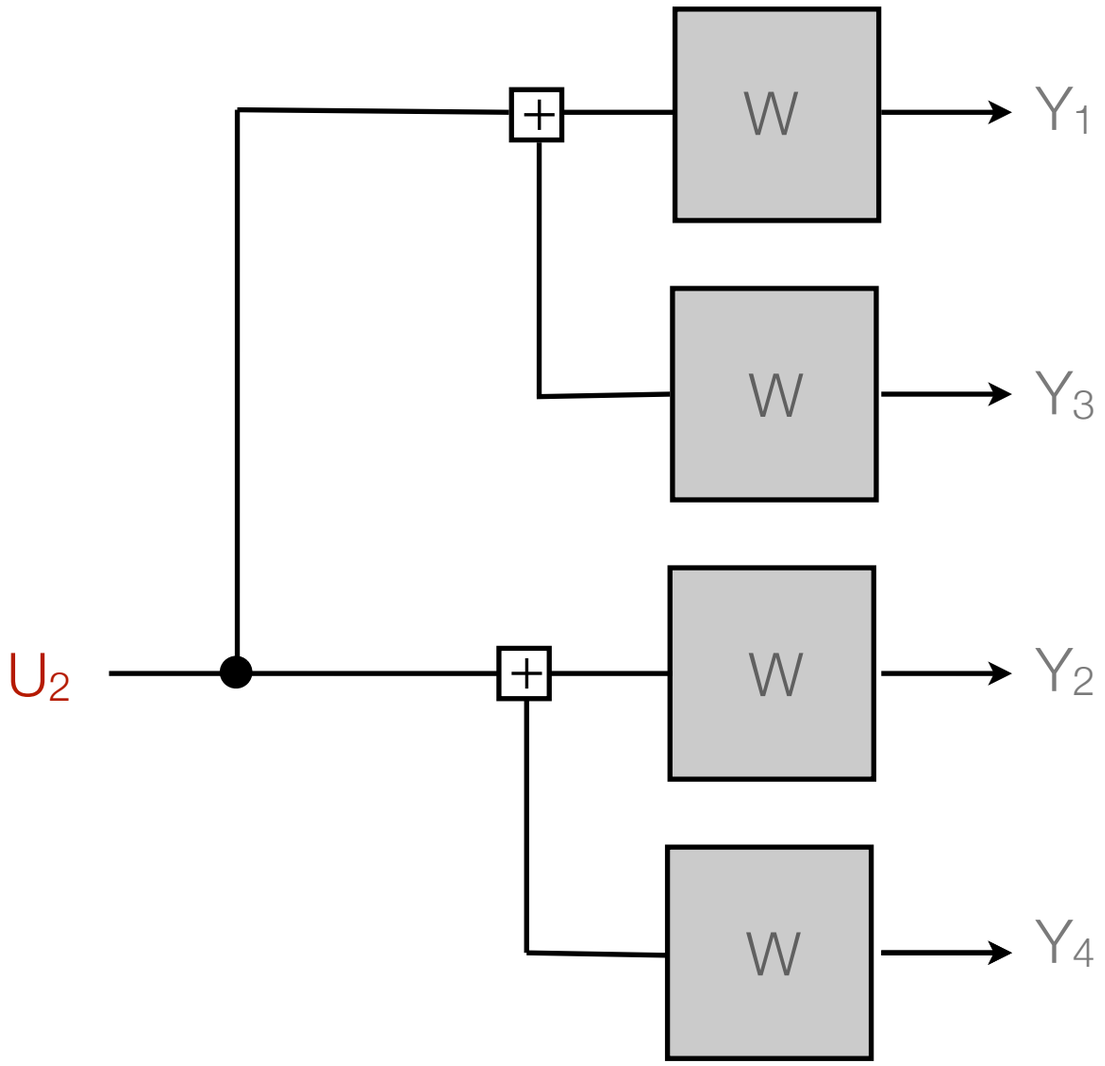
How do channels polarize?



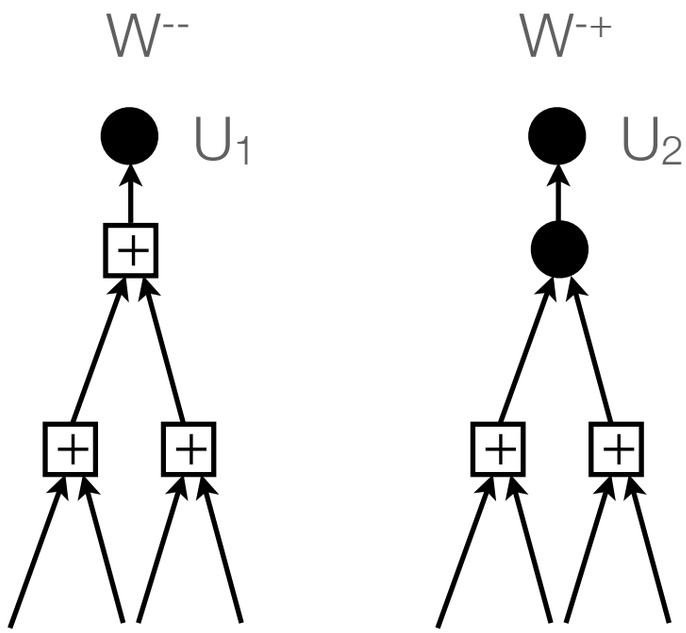


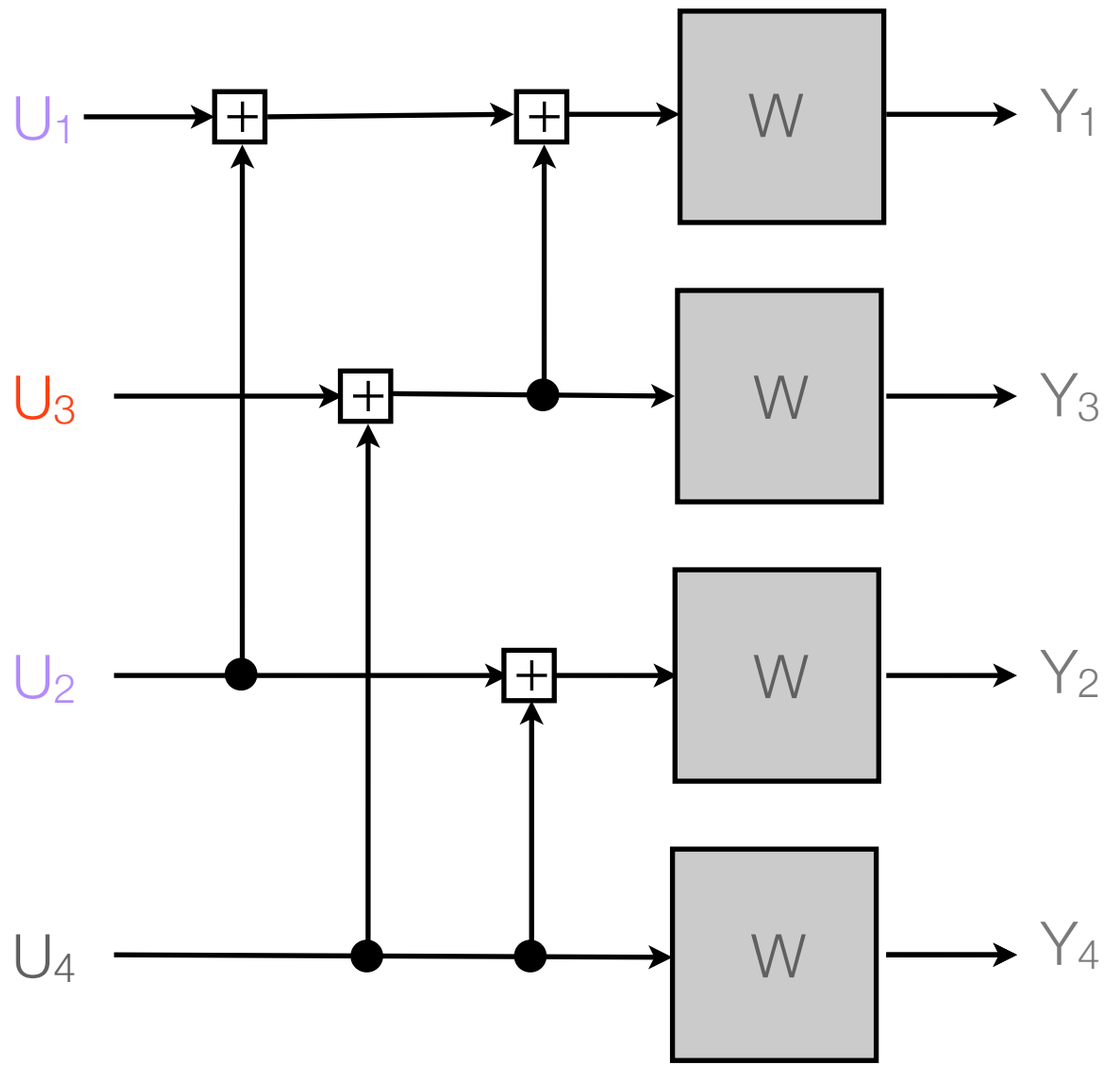
How do channels polarize?



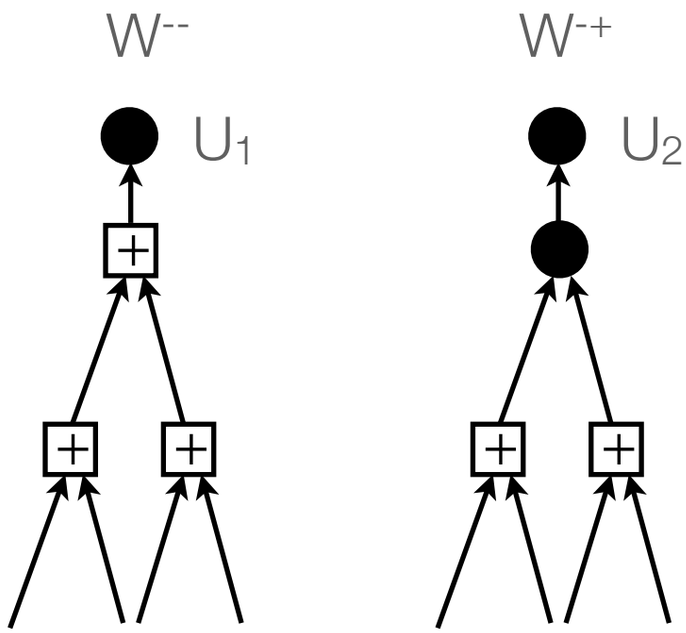


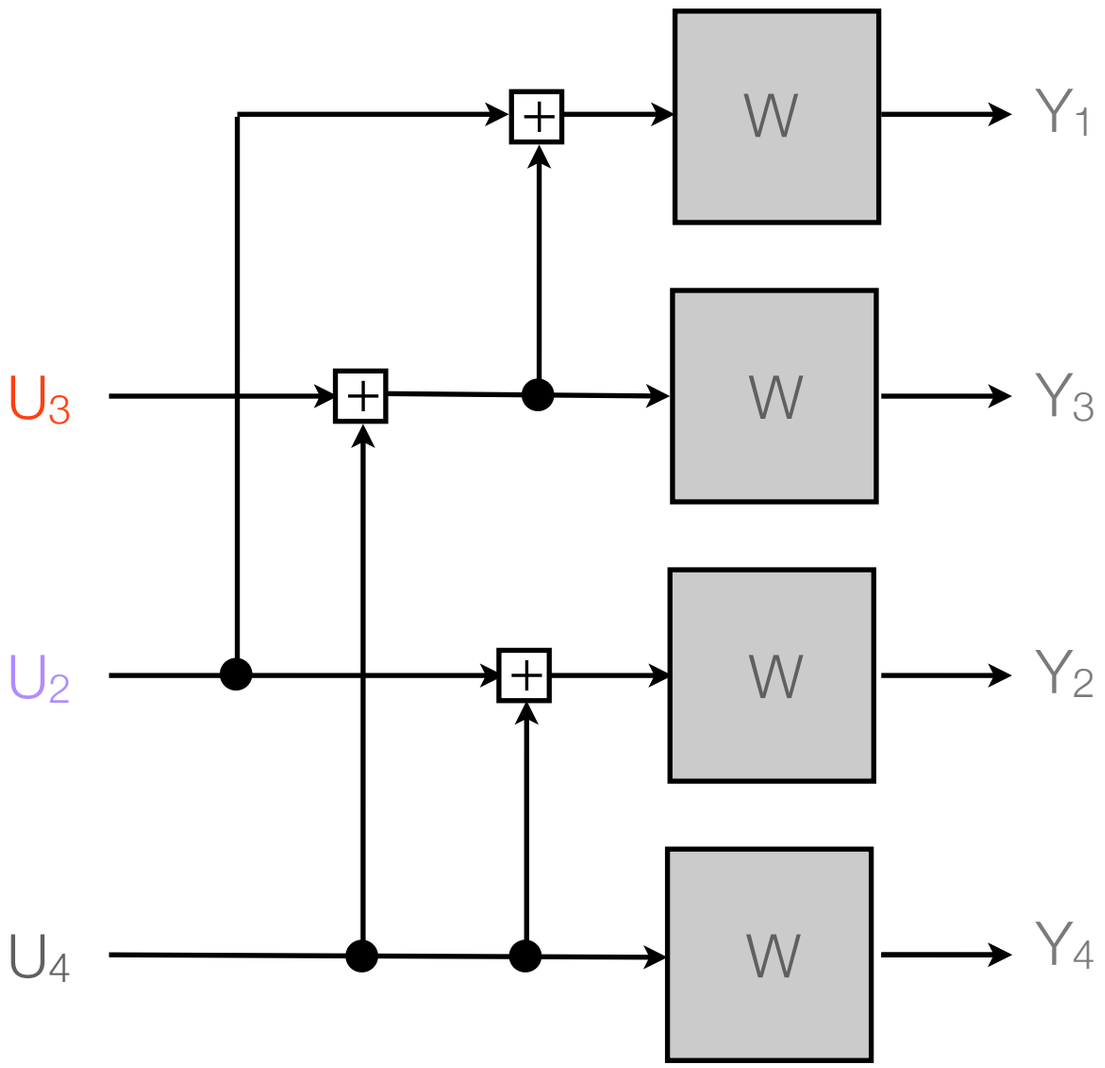
How do channels polarize?



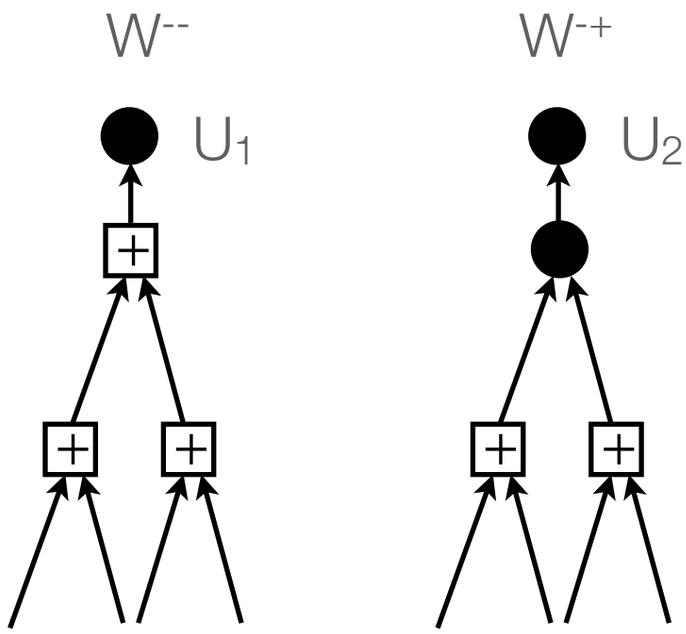


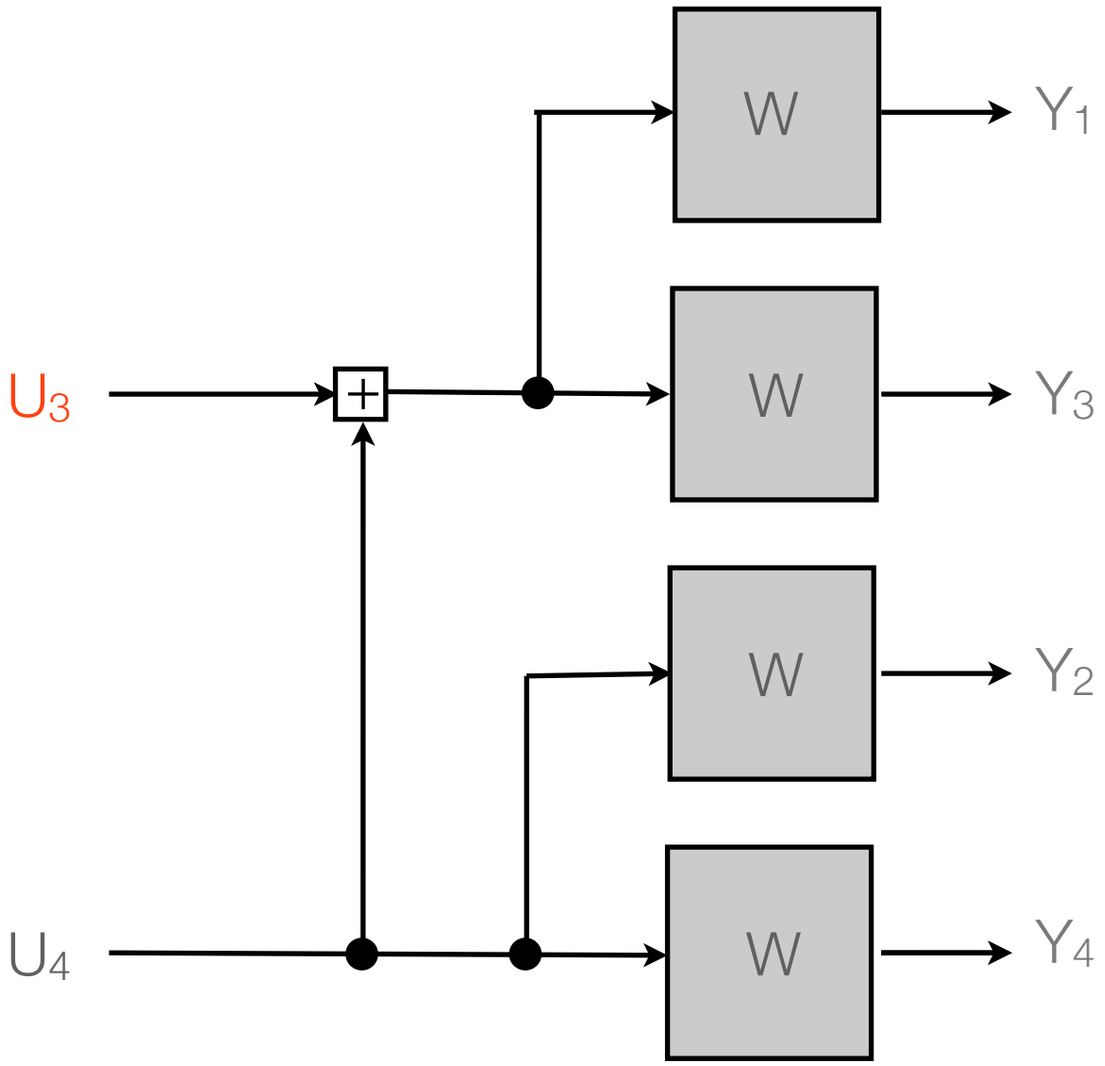
How do channels polarize?



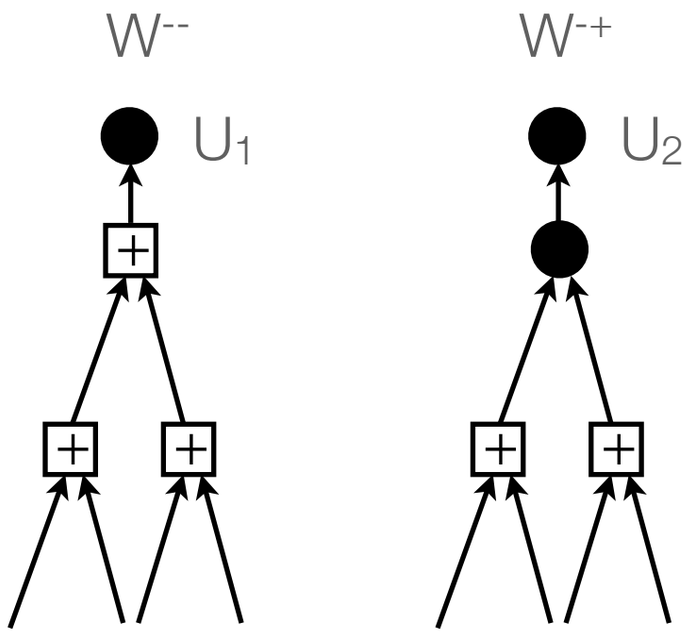


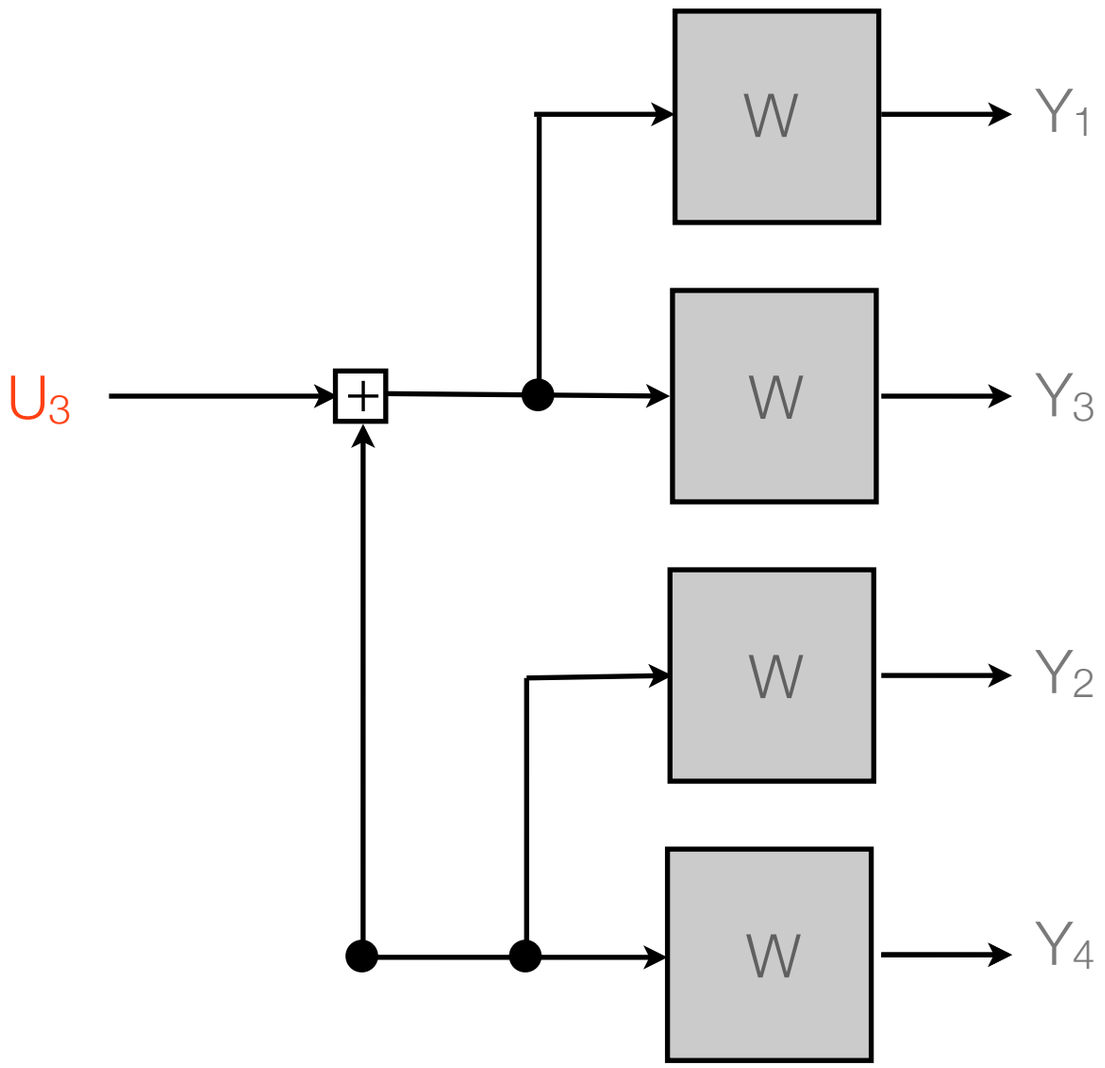
How do channels polarize?



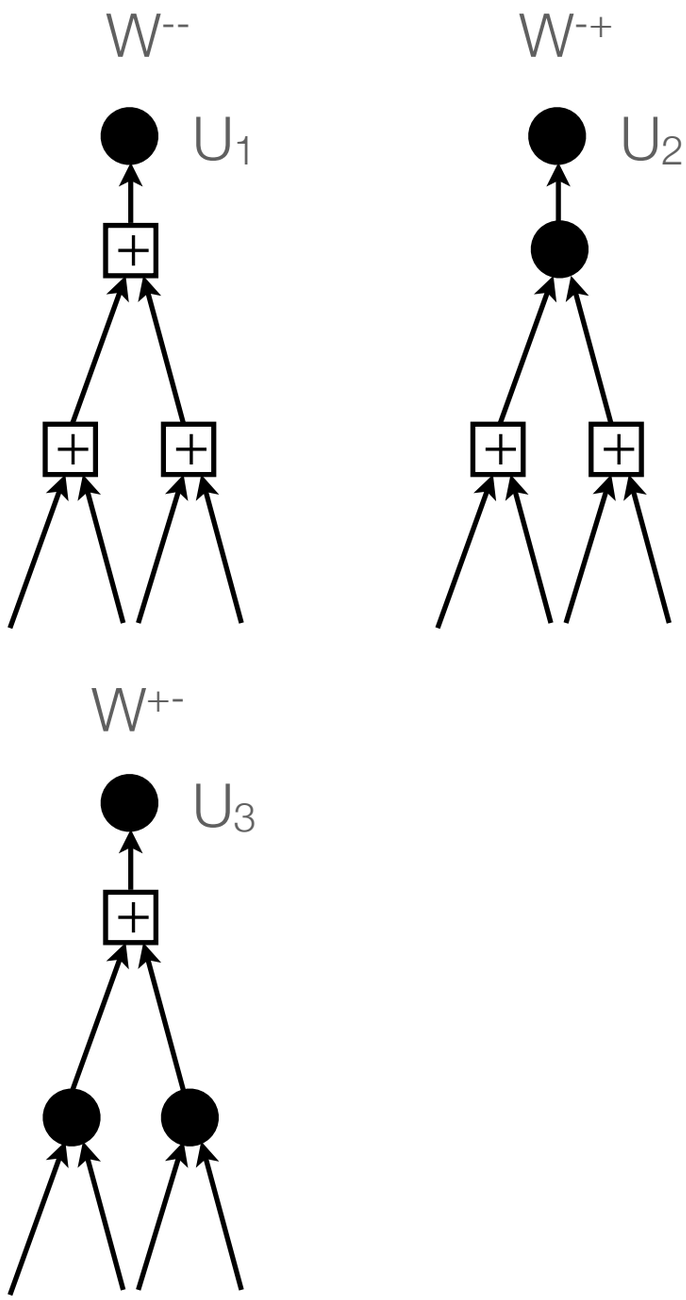


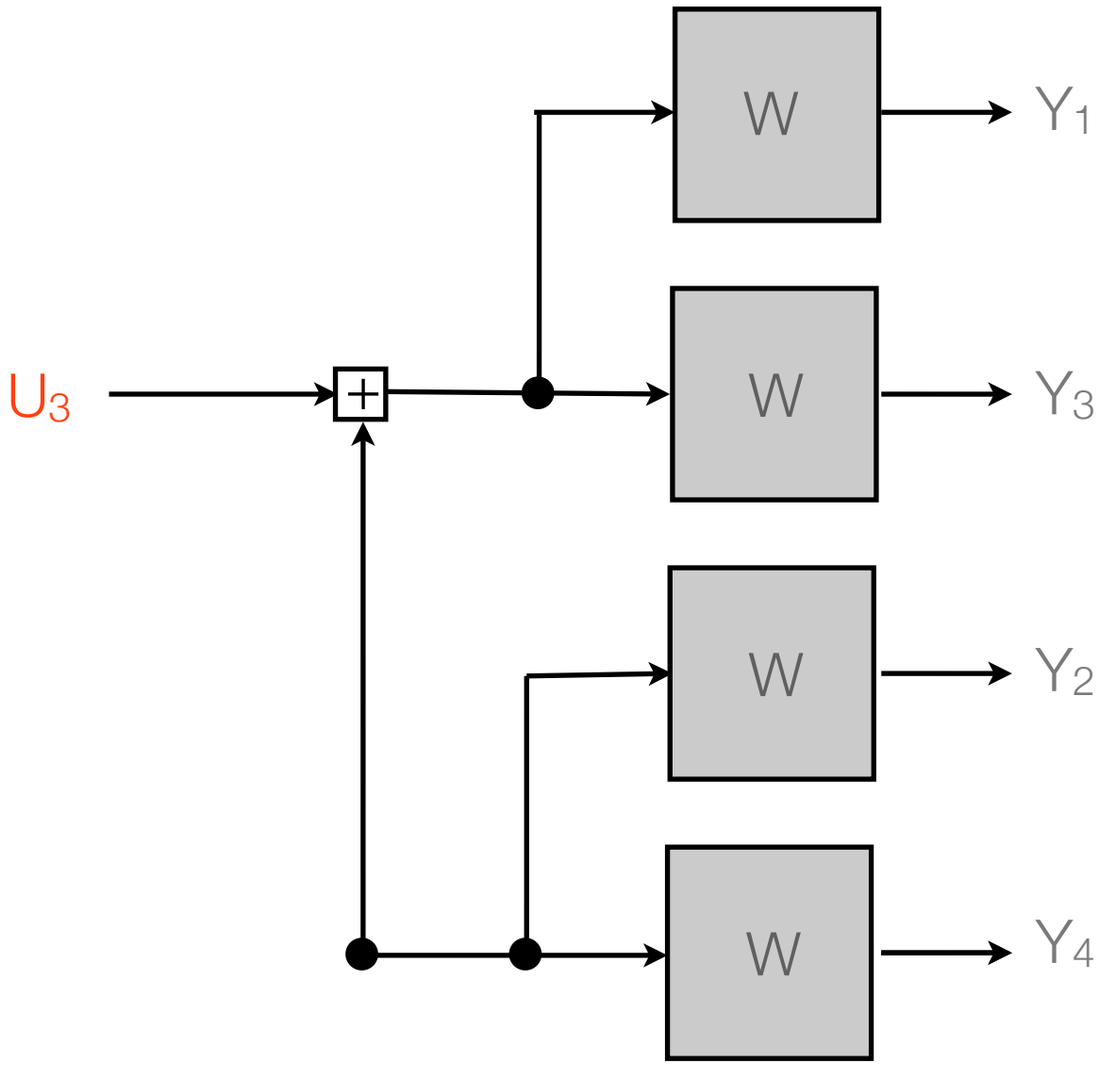
How do channels polarize?



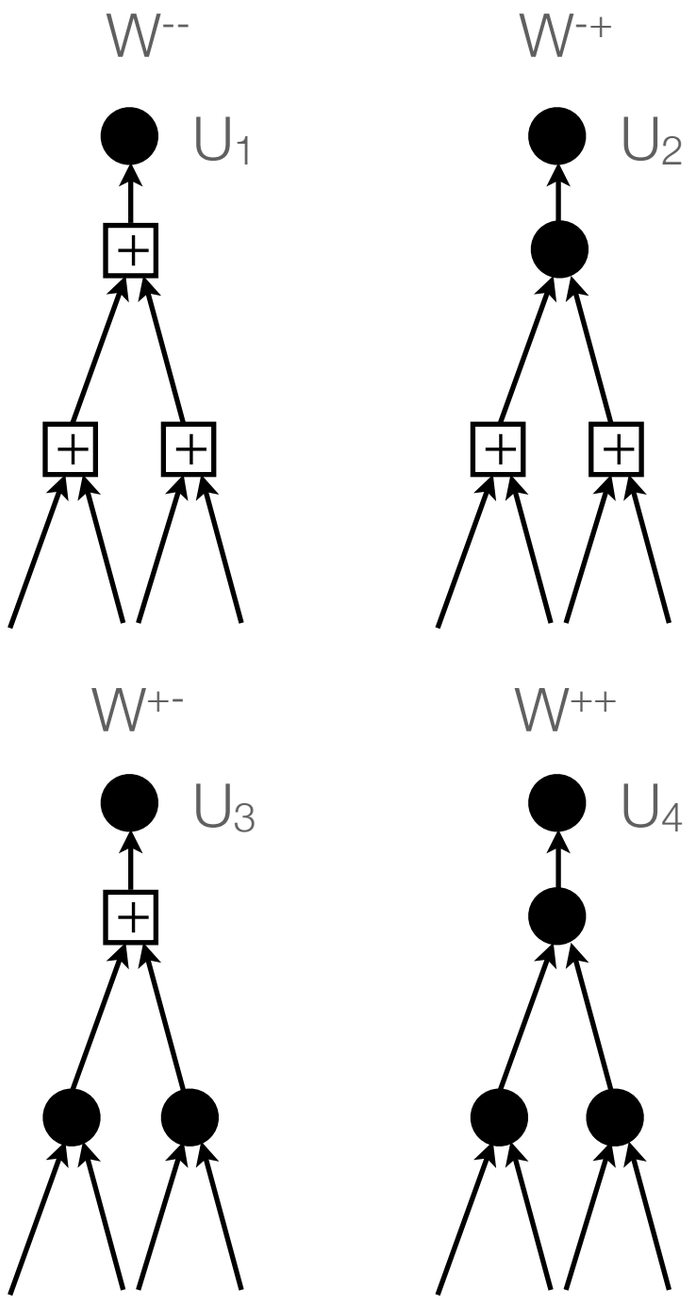


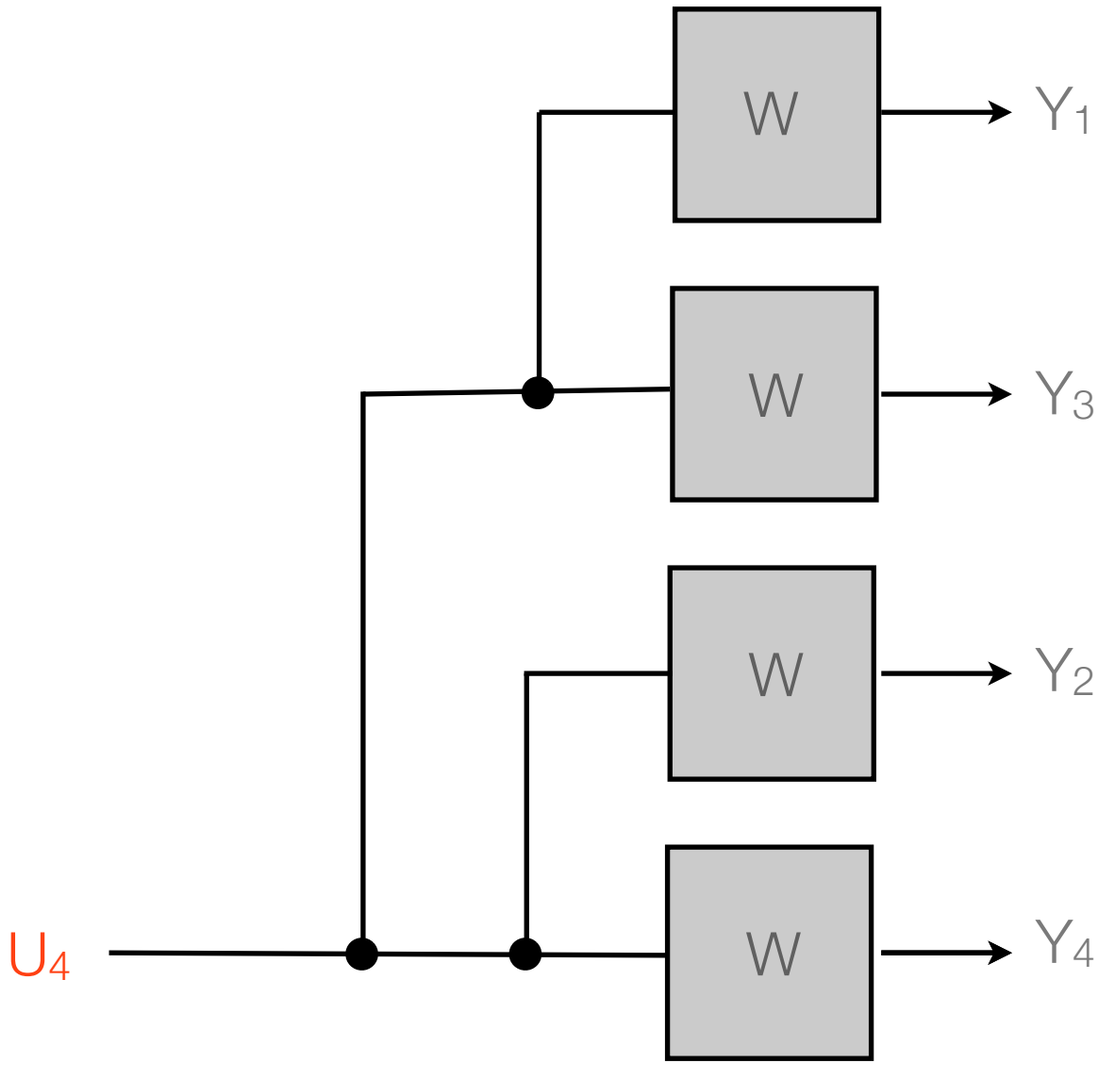
How do channels polarize?





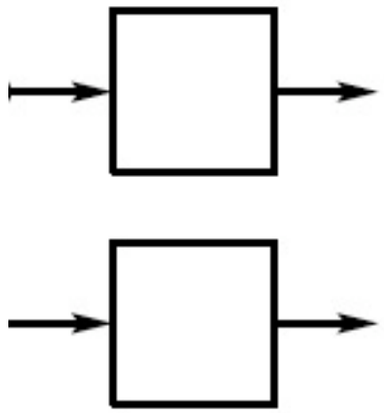
How do channels polarize?



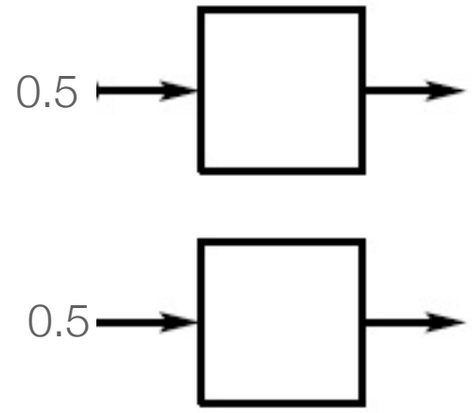


How do channels polarize?

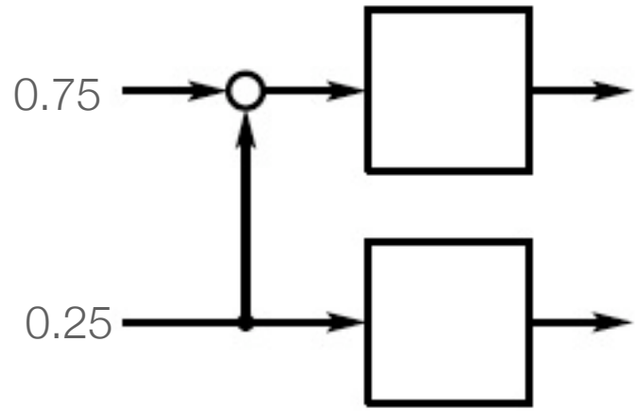
How do channels polarize?



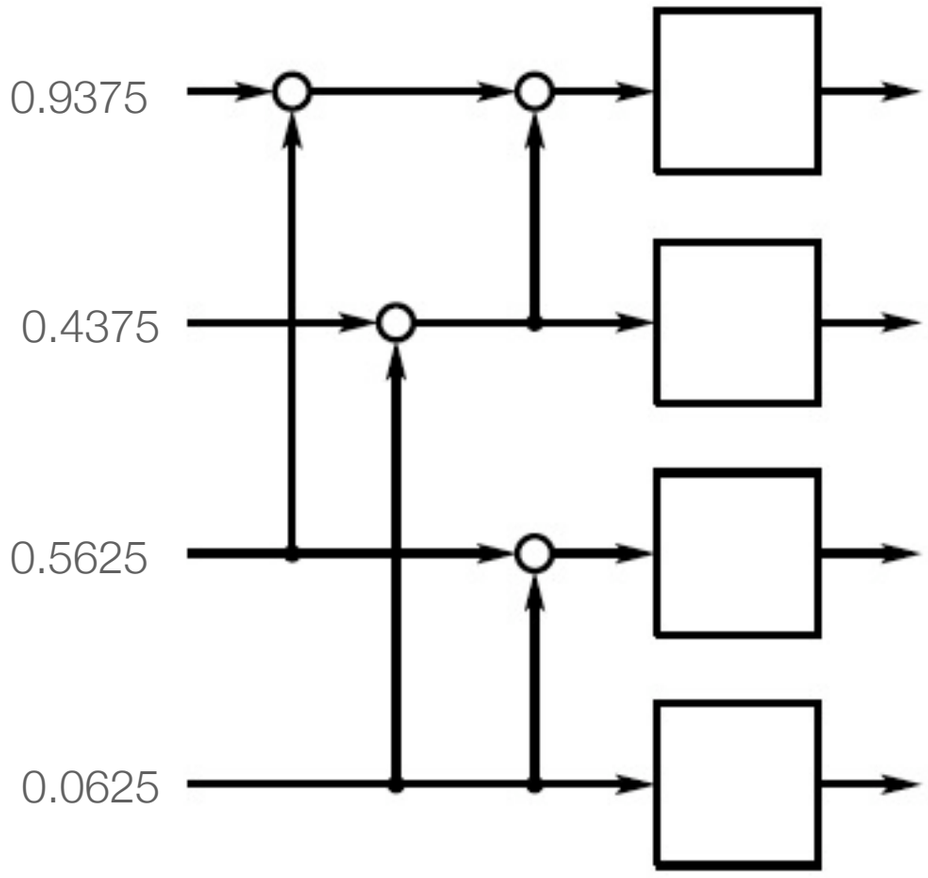
How do channels polarize?



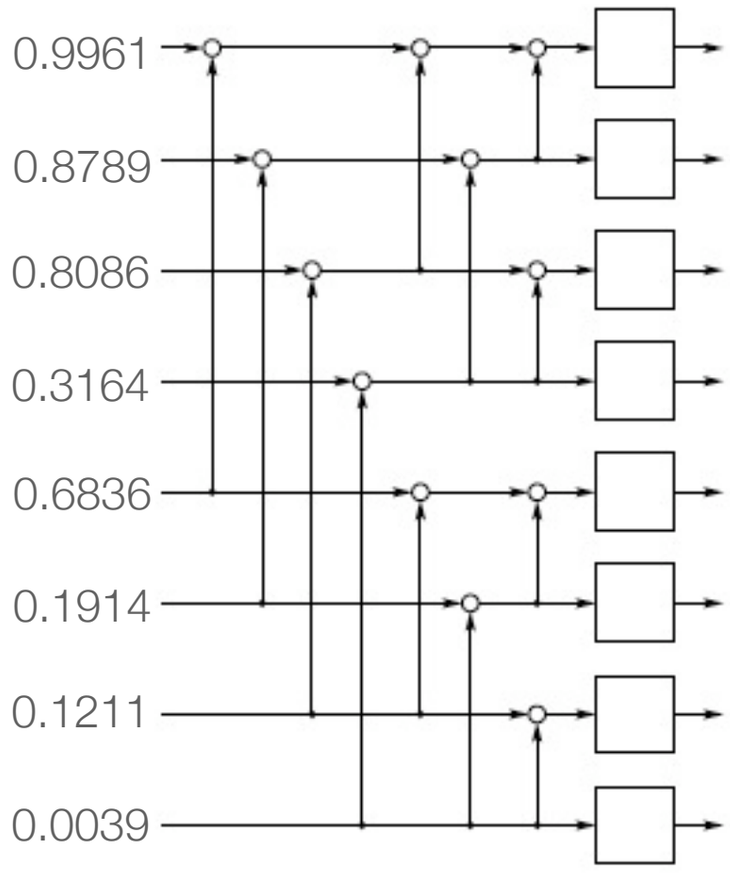
How do channels polarize?



How do channels polarize?

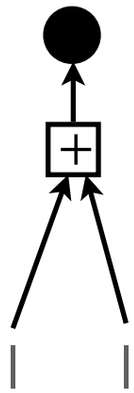


How do channels polarize?



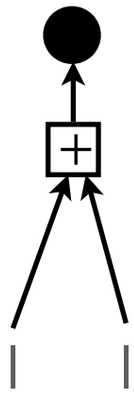
Extremes of Information Combining

Extremes of Information Combining



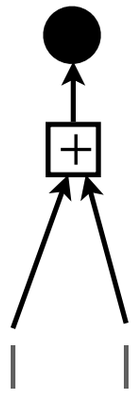
Extremes of Information Combining

$I^2 \leq I(P^-)$



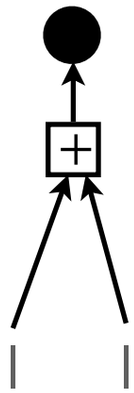
Extremes of Information Combining

$I^2 \leq I(P^-)$



Extremes of Information Combining

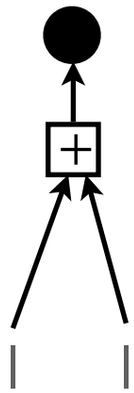
$I^2 \leq I(P^-)$



$I(P^+) \leq 1-(1-I)^2$

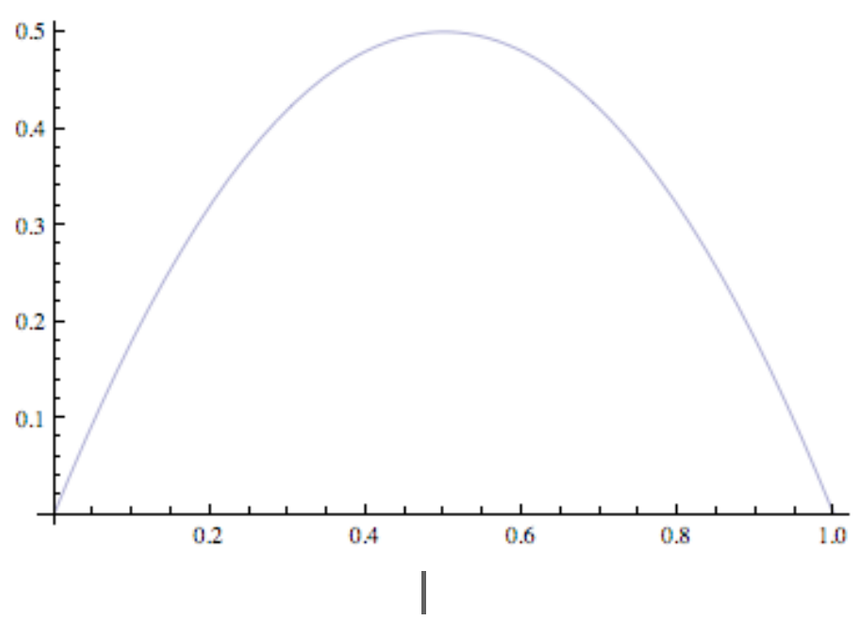
Extremes of Information Combining

$I^2 \leq I(P^-)$



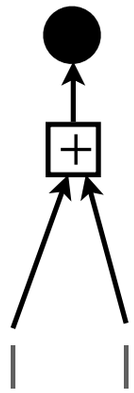
$I(P^+) \leq 1-(1-I)^2$

$I(P^+) - I(P^-) \leq 1-(1-I)^2-I^2=2\,I\,(1-I)$



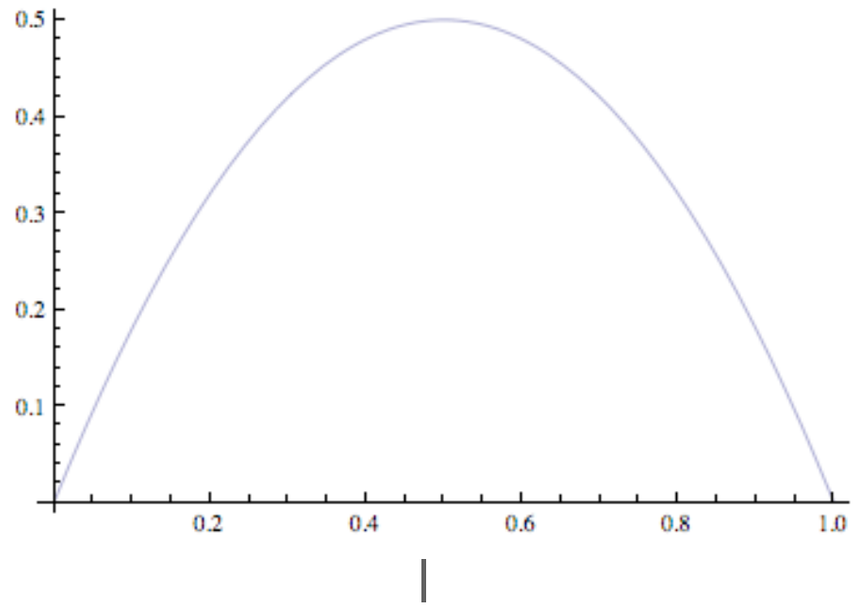
Extremes of Information Combining

$I^2 \leq I(P^-)$



$I = 1 - h(\varepsilon)$

$I(P^+) - I(P^-) \leq 1-(1-I)^2-I^2 = 2I(1-I)$

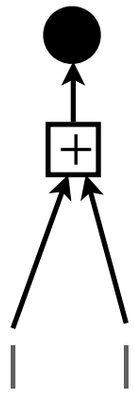


$I(P^+) \leq 1-(1-I)^2$

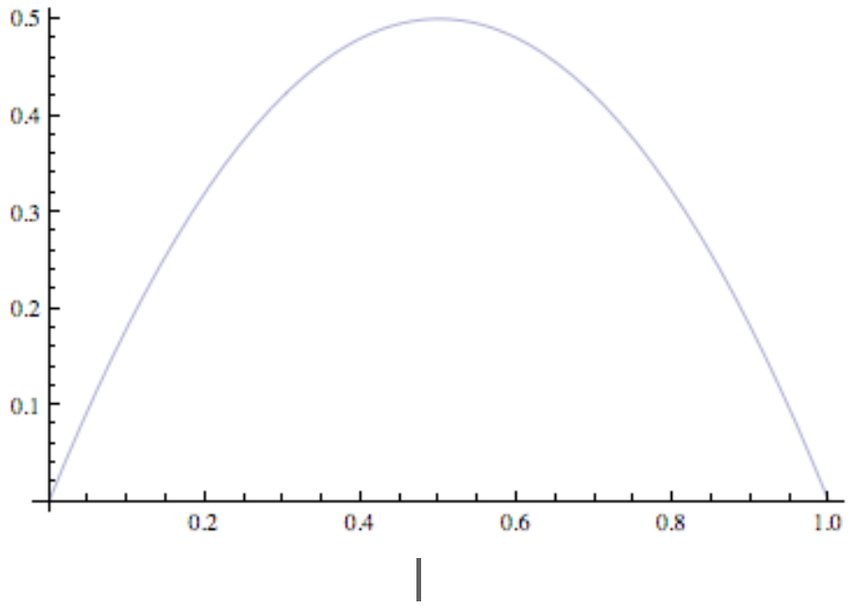
Extremes of Information Combining

$I^2 \leq I(P^-) \leq 1-h(2\,\varepsilon\,(1-\varepsilon))$

$I=1-h(\varepsilon)$



$I(P^+)- I(P^-) \leq 1-(1-I)^2-I^2=2\,I\,(1-I)$

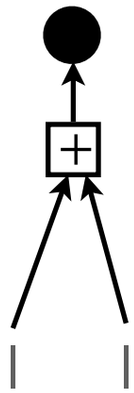


$I(P^+) \leq 1-(1-I)^2$

Extremes of Information Combining

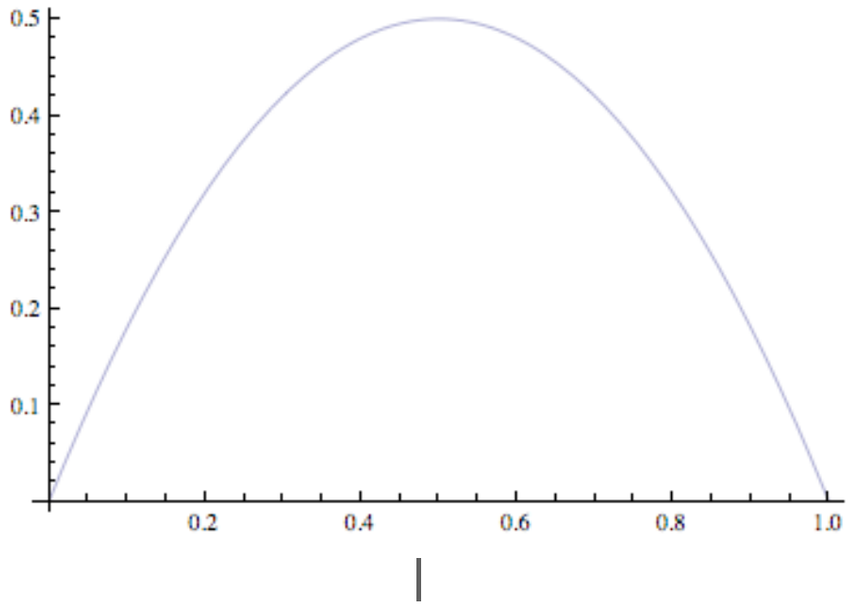
$I^2 \le I(P^-) \le 1-h(2\,\varepsilon\,(1-\varepsilon))$

$1-2\varepsilon(1-\varepsilon)-\varepsilon^2\log_2(1+(1-\varepsilon)^2/\varepsilon^2)-(1-\varepsilon)^2\log_2(1+\varepsilon^2/(1-\varepsilon)^2) \le I(P^+) \le 1-(1-I)^2$



$I=1-h(\varepsilon)$

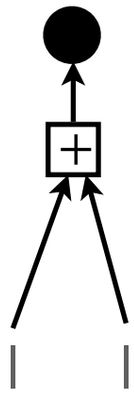
$I(P^+)- I(P^-) \le 1-(1-I)^2-I^2=2\,I\,(1-I)$



Extremes of Information Combining

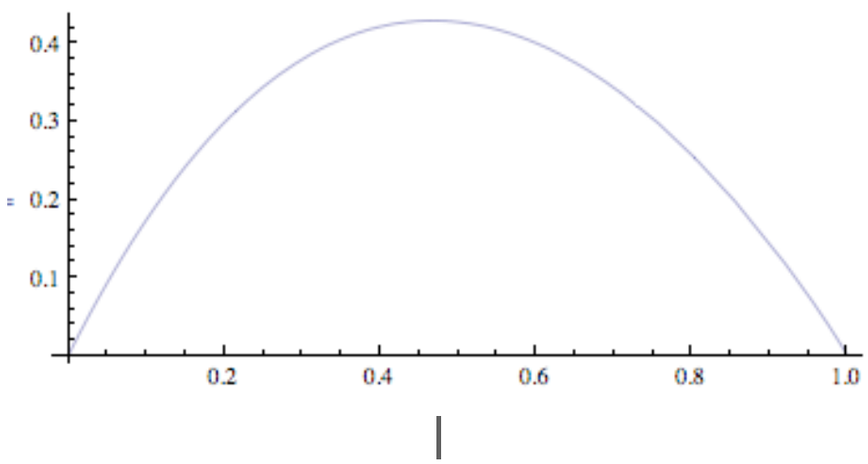
$I^2 \leq I(P^-) \leq 1-h(2\,\varepsilon\,(1-\varepsilon))$

$1-2\varepsilon(1-\varepsilon)-\varepsilon^2\log_2(1+(1-\varepsilon)^2/\varepsilon^2)-(1-\varepsilon)^2\log_2(1+\varepsilon^2/(1-\varepsilon)^2) \leq I(P^+) \leq 1-(1-I)^2$



$I=1-h(\varepsilon)$

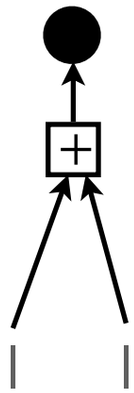
$I(P^+)- I(P^-)$



Extremes of Information Combining

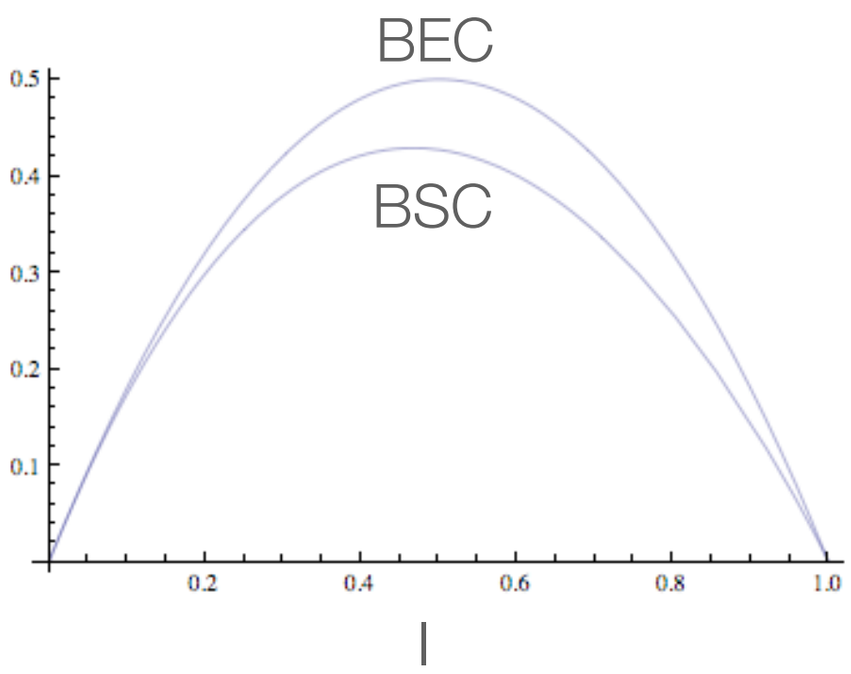
$I^2 \le I(P^-) \le 1-h(2\,\varepsilon\,(1-\varepsilon))$

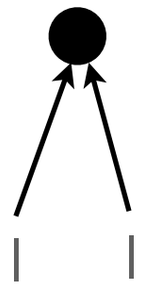
$1-2\varepsilon(1-\varepsilon)-\varepsilon^2\log_2(1+(1-\varepsilon)^2/\varepsilon^2)-(1-\varepsilon)^2\log_2(1+\varepsilon^2/(1-\varepsilon)^2) \le I(P^+) \le 1-(1-I)^2$



$I=1-h(\varepsilon)$

$I(P^+)- I(P^-)$





Equivalent “Random” Channel

Equivalent “Random” Channel

Set B1, B2, ... to be i.i.d. {+, -} valued,
uniformly distributed random variables

Equivalent “Random” Channel

Set B1, B2, ... to be i.i.d. {+, -} valued,
uniformly distributed random variables

Define $I_n = I(W^{B_1, B_2, ..., B_n})$

Equivalent “Random” Channel

Set B1, B2, ... to be i.i.d. {+, -} valued,
uniformly distributed random variables

Define $I_n = I(W^{B_1, B_2, ..., B_n})$

Study the distribution of I_n

Properties of I_n

Properties of I_n

$I_0 = I(W)$ is a constant

Properties of I_n

$I_0 = I(W)$ is a constant

$I_n \in [0, 1]$; so I_n is bounded

Properties of I_n

$I_0 = I(W)$ is a constant

$I_n \in [0, 1]$; so I_n is bounded

Conditional on $B_1, B_2, \ldots, B_n$, and with $P = W^{B_1, B_2, \ldots, B_n}$, I_{n+1} can only take on the two values $I(P^+)$ and $I(P^-)$

Properties of I_n

$I_0 = I(W)$ is a constant

$I_n \in [0, 1]$; so I_n is bounded

Conditional on $B_1, B_2, \ldots, B_n$, and with $P = W^{B_1, B_2, \ldots, B_n}$, I_{n+1} can only take on the two values $I(P^+)$ and $I(P^-)$

Further, $E[I_{n+1} \mid B_1, B_2, \ldots, B_n] = (I(P^+) + I(P^-))/2 = I(P)$, so $\{I_n\}$ is a (bounded) martingale

Properties of I_n

Properties of I_n

a bounded martingale converges almost surely

Properties of I_n

a bounded martingale converges almost surely

$I_\infty = \lim_{n\to\infty} I_n$ exists almost surely; $E[I_\infty]=I_0=I(W)$

Properties of I_n

a bounded martingale converges almost surely

$I_\infty = \lim_{n\to\infty} I_n$ exists almost surely; $E[I_\infty]=I_0=I(W)$

$\Pr\{|I_{n+1}-I_n|\leq\varepsilon\}\to 1$; but $|I_{n+1}-I_n|=(I(P^+)- I(P^-))/2$

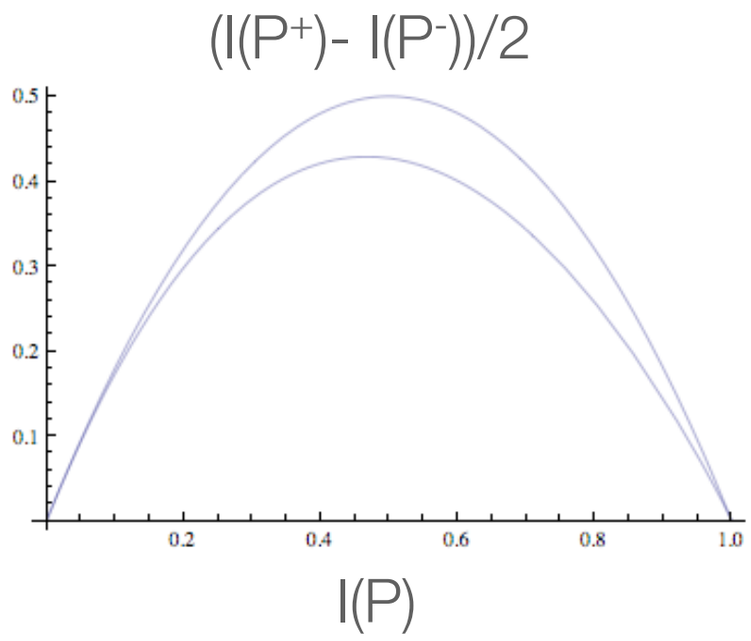
Properties of I_n

a bounded martingale converges almost surely

$I_\infty = \lim_{n\to\infty} I_n$ exists almost surely; $E[I_\infty]=I_0=I(W)$

$\Pr\{|I_{n+1}-I_n|\leq\varepsilon\}\to 1$; but $|I_{n+1}-I_n|=(I(P^+)- I(P^-))/2$

from extremes of information combining we know that $(I(P^+)-I(P^-))/2 \leq\varepsilon$ implies that $I(P)\notin(\delta, 1-\delta)$



Properties of I_n

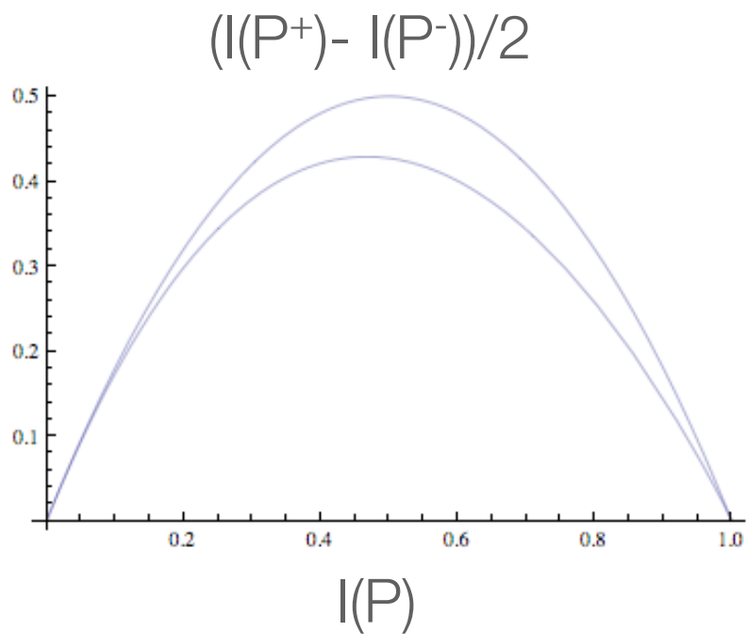
a bounded martingale converges almost surely

$I_\infty = \lim_{n\to\infty} I_n$ exists almost surely; $E[I_\infty]=I_0=I(W)$

$\Pr\{|I_{n+1}-I_n|\leq\varepsilon\}\to 1$; but $|I_{n+1}-I_n|=(I(P^+)- I(P^-))/2$

from extremes of information combining we know that $(I(P^+)-I(P^-))/2 \leq\varepsilon$ implies that $I(P)\notin(\delta, 1-\delta)$

we conclude that I_∞ takes values only in {0, 1}



Summary of Known Results

Summary of Known Results

achieve capacity on memoryless channels Arikan 2007

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008

Why $P_B(N) \approx 2^{-N^{\frac{1}{2}}}$

Why $P_B(N) \approx 2^{-N^{\frac{1}{2}}}$

Consider BEC for simplicity:

Why $P_B(N) \approx 2^{-N^{\frac{1}{2}}}$

Consider BEC for simplicity:

In this case the Bhattacharyya parameter, call it Z,
is just the erasure probability.

Why $P_B(N) \approx 2^{-N^{\frac{1}{2}}}$

Consider BEC for simplicity:

In this case the Bhattacharyya parameter, call it Z,
is just the erasure probability.

We have seen that given that it is Z at some point, the two new values are Z^2 and Z(2-Z)

Why $P_B(N) \approx 2^{-N^{\frac{1}{2}}}$

Consider BEC for simplicity:

In this case the Bhattacharyya parameter, call it Z,
is just the erasure probability.

We have seen that given that it is Z at some point, the two new values are Z^2 and Z(2-Z)

Imagine that Z is already very small; Z^2 is a big change but Z->Z(2-Z) ~ 2 Z is only a small change

Why $P_B(N) \approx 2^{-N^{\frac{1}{2}}}$

Consider BEC for simplicity:

In this case the Bhattacharyya parameter, call it Z,
is just the erasure probability.

We have seen that given that it is Z at some point, the two new values are Z^2 and Z(2-Z)

Imagine that Z is already very small; Z^2 is a big change but Z->Z(2-Z) ~ 2 Z is only a small change

Look therefore at the process with Z-> Z^2 or Z->Z

Why $P_B(N) \approx 2^{-N^{\frac{1}{2}}}$

Consider BEC for simplicity:

In this case the Bhattacharyya parameter, call it Z,
is just the erasure probability.

We have seen that given that it is Z at some point, the two new values are Z^2 and Z(2-Z)

Imagine that Z is already very small; Z^2 is a big change but Z->Z(2-Z) ~ 2 Z is only a small change

Look therefore at the process with Z-> Z^2 or Z->Z

Take twice the log of this; now we have a random walk, where with probability 1/2 we go one step to the right and with probability 1/2 we stay where we are; so our average speed is half the number of steps taken; this corresponds to the

$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$

Summary of Known Results

Summary of Known Results

achieve capacity on memoryless channels Arikan 2007

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008
$P_B(N) \approx 2^{-(N)^{E_C(G)}}$	Korada, Sasoglu, and U. 2009

Polar Codes Based on Larger Matrices

In [Arıkan08] generator matrix is constructed from the rows of $G_2^{\otimes m}$, where

$$G_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

Polar Codes Based on Larger Matrices

In [Arıkan08] generator matrix is constructed from the rows of $G_2^{\otimes m}$, where

$$G_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

Consider codes constructed from $G^{\otimes m}$, where G is an $\ell \times \ell$ matrix. Blocklength $N = \ell^m$, $\bar{x} = \bar{u}G^{\otimes m}$

Characterization of Exponent

Theorem (Korada,Şaşoğlu,Urbanke)

For any $R < I(W)$, and $\ell \times \ell$ matrix G,

$$P_B(N) \approx 2^{-(N)^{\mathbf{E}_c(G)}},$$

where $\mathbf{E}_c(G) = \frac{1}{\ell} \sum_{i=1}^{\ell} \log_\ell d_i$.

$$G = \begin{bmatrix} g_1 \\ \vdots \\ g_i \\ g_{i+1} \\ \vdots \\ g_\ell \end{bmatrix} \qquad d_i = \mathtt{dmin}(g_i, \langle g_{i+1}, \ldots, g_\ell \rangle)$$

Exponent: Example

Exponent: Example

$$G = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

Exponent: Example

$$G = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

$$d_1 = 1,$$

Exponent: Example

$$G = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

$$d_1 = 1, d_2 = 2,$$

Exponent: Example

$$G = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

$$d_1 = 1, d_2 = 2, d_3 = 2$$

Exponent: Example

$$G = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

$$d_1 = 1,\ d_2 = 2,\ d_3 = 2$$

$$\mathbf{E}_c(G) = \frac{1}{3}(\log_3 1 + \log_3 2 + \log_3 2) = 0.42062$$

Results

Results

$$\mathbf{E}_\ell = \max_{G \in \{0,1\}^{\ell \times \ell}} \mathbf{E}_c(G)$$

Results

$$\mathbf{E}_\ell = \max_{G \in \{0,1\}^{\ell \times \ell}} \mathbf{E}_c(G)$$

For $\ell < 15$, $\mathbf{E}_\ell \leq \frac{1}{2}$

Results

$$\mathbf{E}_\ell = \max_{G \in \{0,1\}^{\ell \times \ell}} \mathbf{E}_c(G)$$

For $\ell < 15$, $\mathbf{E}_\ell \leq \frac{1}{2}$

$$\mathbf{E}_{16} = 0.51828$$

Results

$$\mathbf{E}_\ell = \max_{G \in \{0,1\}^{\ell \times \ell}} \mathbf{E}_c(G)$$

For $\ell < 15$, $\mathbf{E}_\ell \leq \frac{1}{2}$

$$\mathbf{E}_{16} = 0.51828$$

$$\lim_{\ell \to \infty} \mathbf{E}_\ell = 1$$

Summary of Known Results

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008
$P_B(N) \approx 2^{-(N)^{E_C(G)}}$	Korada, Sasoglu, and U. 2009

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008
$P_B(N) \approx 2^{-(N)^{\Xi c(G)}}$	Korada, Sasoglu, and U. 2009
lossy source coding, Wyner-Ziv, Gelfand-Pinsker, ...	Korada and U. 2009

Source Coding

Summary of Known Results

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008
$P_B(N) \approx 2^{-(N)^{\Xi c(G)}}$	Korada, Sasoglu, and U. 2009
lossy source coding, Wyner-Ziv, Gelfand-Pinsker, ...	Korada and U. 2009

Summary of Known Results

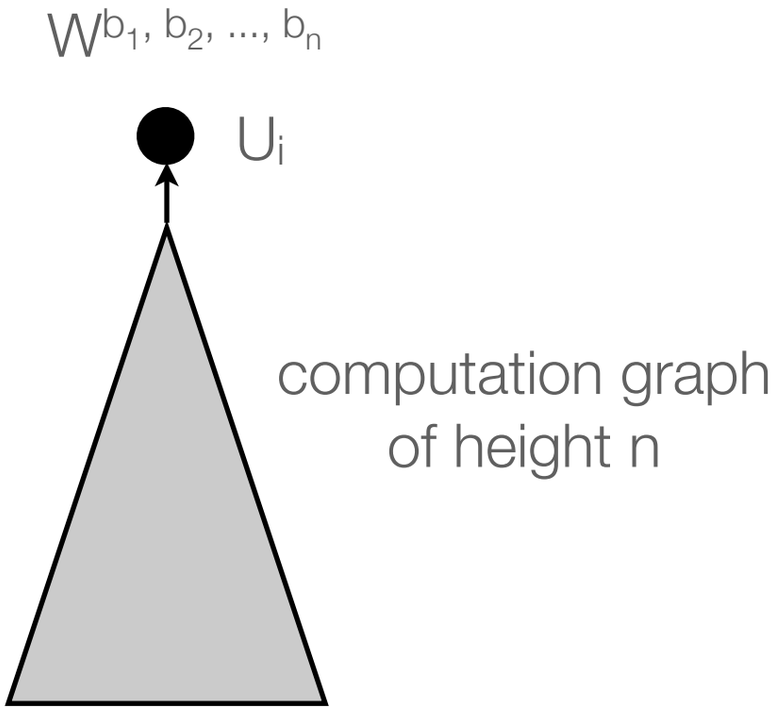
achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008
$P_B(N) \approx 2^{-(N)^{\Xi c(G)}}$	Korada, Sasoglu, and U. 2009
lossy source coding, Wyner-Ziv, Gelfand-Pinsker, ...	Korada and U. 2009
efficient construction	Mori and Tanaka 2009

How do we find good U_is?

Complexity linear IF we assume that we can do infinite precision density evolution at unit cost.

Mori & Tanaka

How do we find good U_is?



Complexity linear IF we assume that we can do infinite precision density evolution at unit cost.

Mori & Tanaka

Summary of Known Results

Summary of Known Results

achieve capacity on memoryless channels Arikan 2007

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008
$P_B(N) \approx 2^{-(N)^{E_C(G)}}$	Korada, Sasoglu, and U. 2009

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008
$P_B(N) \approx 2^{-(N)^{\Xi c(G)}}$	Korada, Sasoglu, and U. 2009
lossy source coding, Wyner-Ziv, Gelfand-Pinsker, ...	Korada and U. 2009

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008
$P_B(N) \approx 2^{-(N)^{\Xi c(G)}}$	Korada, Sasoglu, and U. 2009
lossy source coding, Wyner-Ziv, Gelfand-Pinsker, ...	Korada and U. 2009
efficient construction	Mori and Tanaka 2009

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008
$P_B(N) \approx 2^{-(N)^{\Xi c(G)}}$	Korada, Sasoglu, and U. 2009
lossy source coding, Wyner-Ziv, Gelfand-Pinsker, ...	Korada and U. 2009
efficient construction	Mori and Tanaka 2009
compound coding	Hassani, Korada and U. 2009

Compound Capacity

Compound Capacity

$\mathcal{W}$ set of channels

Compound Capacity

$\mathscr{W}$ set of channels

$$C(\mathscr{W}) = \max_{P} \inf_{W \in \mathscr{W}} I_P(W)$$

Compound Capacity

$\mathcal{W}$ set of channels

$$C(\mathcal{W}) = \inf_{W \in \mathcal{W}} I(W)$$

For BMS channels, uniform distribution is optimal.

Compound Capacity

$\mathscr{W}$ set of channels

$$C(\mathscr{W}) = \inf_{W \in \mathscr{W}} I(W)$$

For BMS channels, uniform distribution is optimal.

Can polar codes achieve the compound capacity for the class of BMS channels?

Trivial Bounds

Trivial Bounds

P

Q

two BMS channels

Trivial Bounds

P

Q

two BMS channels

$$C_{\mathrm{P,SC}}(P,Q) \leq \min\{I(P), I(Q)\}$$

Trivial Bounds

P

Q

two BMS channels

$$C_{\mathrm{P,SC}}(P,Q) \leq \min\{I(P), I(Q)\}$$

$$\begin{aligned} C_{\mathrm{P,SC}}(P,Q) &\geq C_{\mathrm{P,SC}}(\mathrm{BEC}(Z(P)), \mathrm{BEC}(Z(Q))) \\ &= 1 - \max\{Z(P), Z(Q)\}. \end{aligned}$$

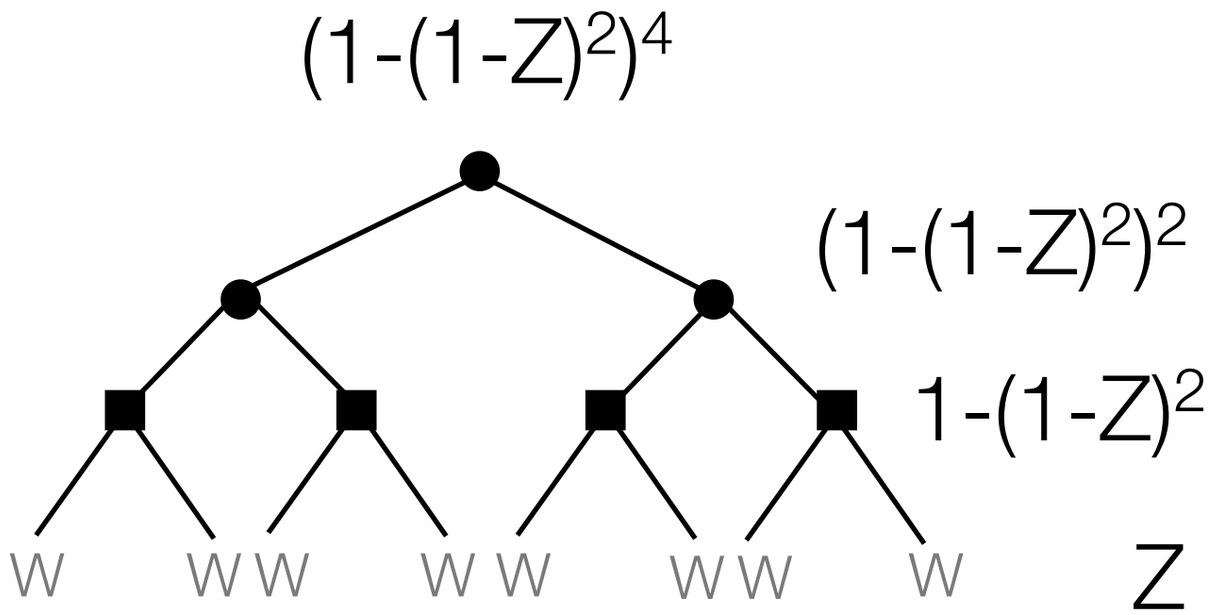
Trivial Bounds

P

Q

two BMS channels

$$C_{\mathrm{P,SC}}(P,Q) \leq \min\{I(P), I(Q)\}$$



$$C_{\mathrm{P,SC}}(P,Q) \geq C_{\mathrm{P,SC}}(\mathrm{BEC}(Z(P)), \mathrm{BEC}(Z(Q)))$$
$$= 1 - \max\{Z(P), Z(Q)\}.$$

Example

Example

$$P = BEC(0.5) \qquad Q = BSC(0.11002)$$

Example

$$P = BEC(0.5) \qquad Q = BSC(0.11002)$$

$$I(P) = I(Q) = 0.5$$

Example

$$P = BEC(0.5) \qquad Q = BSC(0.11002)$$

$$I(P) = I(Q) = 0.5$$

$$Z(BEC(0.5)) = 0.5$$

Example

$$P = BEC(0.5) \qquad Q = BSC(0.11002)$$

$$I(P) = I(Q) = 0.5$$

$$Z(BEC(0.5)) = 0.5$$

$$Z(BSC(0.11002)) = 2\sqrt{0.1102(1 - 0.11002)} \approx 0.6258$$

Example

$$P = BEC(0.5) \qquad Q = BSC(0.11002)$$

$$I(P) = I(Q) = 0.5$$

$$Z(BEC(0.5)) = 0.5$$

$$Z(BSC(0.11002)) = 2\sqrt{0.1102(1-0.11002)} \approx 0.6258$$

$$C_{P,\,SC}(P,Q)) \leq \min\{0.5, 0.5\} = 0.5$$

Example

$$P = BEC(0.5) \qquad Q = BSC(0.11002)$$

$$I(P) = I(Q) = 0.5$$

$$Z(BEC(0.5)) = 0.5$$

$$Z(BSC(0.11002)) = 2\sqrt{0.1102(1-0.11002)} \approx 0.6258$$

$$C_{P,\,SC}(P,Q)) \leq \min\{0.5, 0.5\} = 0.5$$

$$C_{P,\,SC}(P,Q)) \geq 1 - \max\{0.6258, 0.5\} = 0.3742$$

Slightly Less Trivial Bounds

Slightly Less Trivial Bounds

P

Q

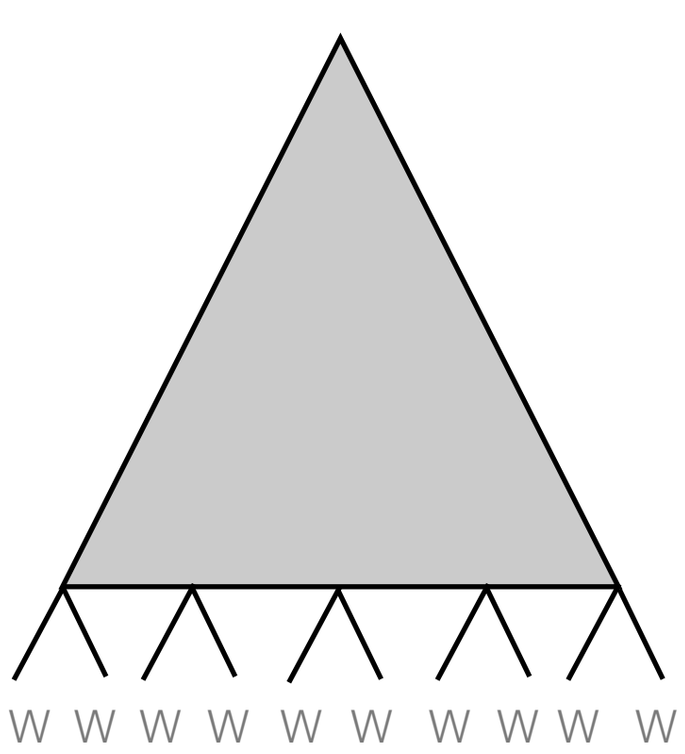
two BMS channels

Slightly Less Trivial Bounds

P

Q

two BMS channels



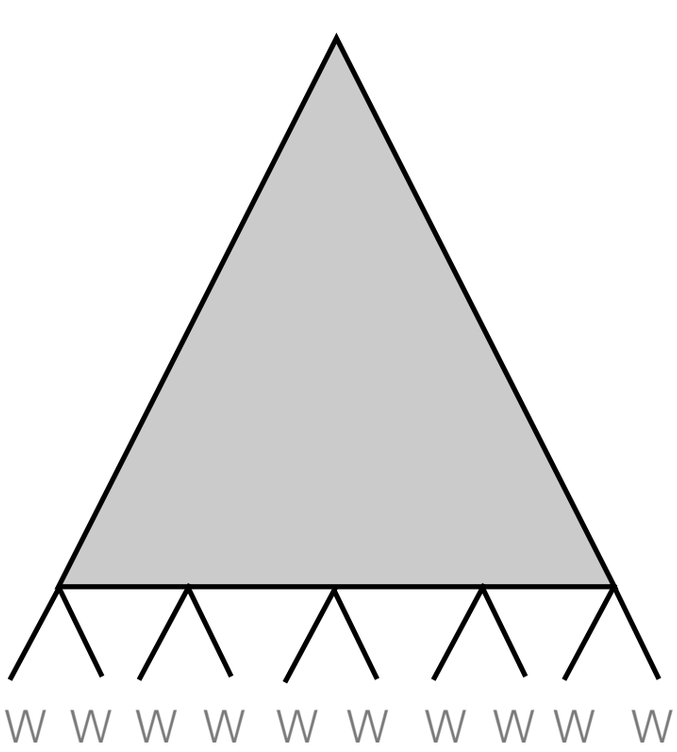
$\sigma = \sigma_1 \sigma_2 \sigma_3 \sigma_4 \sigma_5 \ldots$

Slightly Less Trivial Bounds

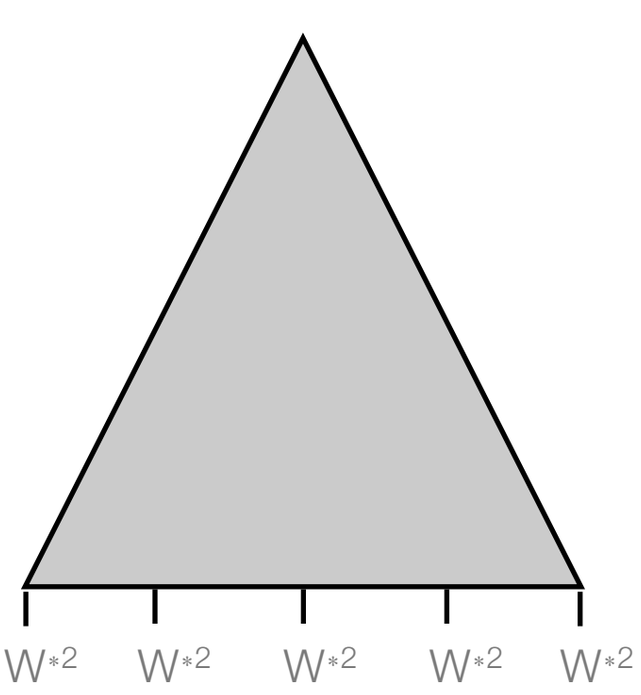
P

Q

two BMS channels



$\sigma = \sigma_1 \sigma_2 \sigma_3 \sigma_4 \sigma_5 \ldots$



$\sigma = \sigma_2 \sigma_3 \sigma_4 \sigma_5 \ldots$

Pairwise Compound Rate

Theorem 5 (Bounds on Pairwise Compound Rate)
Let P and Q be two BMS channels. Then for any $n \in \mathbb{N}$

$$C_{P,SC}(P,Q) \leq \frac{1}{2^n} \sum_{\sigma \in \{0,1\}^n} \min\{I(P^\sigma), I(Q^\sigma)\},$$

$$C_{P,SC}(P,Q) \geq 1 - \frac{1}{2^n} \sum_{\sigma \in \{0,1\}^n} \max\{Z(P^\sigma), Z(Q^\sigma)\}.$$

Further, the upper as well as the lower bounds converge to the compound capacity as n tends to infinity and the bounds are monotone with respect to n.

Example

$BEC(0.5)$ $BSC(0.11002)$

$n=0$	1	2	3	4	5	6
0.500	0.482	0.482	0.482	0.482	0.482	0.482
0.374	0.407	0.427	0.440	0.449	0.456	0.461

Compound Capacity of Whole Family

Compound Capacity of Whole Family

$$C_{P,\,SC}(\{BMS(I = 0.5)\})$$

Compound Capacity of Whole Family

$$C_{P,\,SC}(\{BMS(I=0.5)\})$$

$$\begin{aligned} C_{P,\,SC}(\{BMS(I=0.5)\}) &\leq C(BSC(0.11002), BEC(0.5)) \\ &\leq 0.4817, \end{aligned}$$

Compound Capacity of Whole Family

$$C_{P,\,SC}(\{BMS(I=0.5)\})$$

$$\begin{aligned} C_{P,\,SC}(\{BMS(I=0.5)\}) &\leq C(BSC(0.11002), BEC(0.5)) \\ &\leq 0.4817, \end{aligned}$$

$$C_{P,\,SC}(\{BMS(I=0.5)\}) \geq 1 - Z(BSC(I=0.5)) \approx 0.374$$

Compound Capacity of Whole Family

$$C_{P,\,SC}(\{BMS(I=0.5)\})$$

$$\begin{aligned} C_{P,\,SC}(\{BMS(I=0.5)\}) &\leq C(BSC(0.11002), BEC(0.5)) \\ &\leq 0.4817, \end{aligned}$$

$$C_{P,\,SC}(\{BMS(I=0.5)\}) \geq 1 - Z(BSC(I=0.5)) \approx 0.374$$

$$\begin{aligned} C_{P,\,SC}(\{BMS(I=0.5)\}) &\geq 1 - \frac{1}{2}(0.392 + 0.799) \\ &= 0.404. \end{aligned}$$

Summary of Known Results

Summary of Known Results

achieve capacity on memoryless channels Arikan 2007

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008
$P_B(N) \approx 2^{-(N)^{E_C(G)}}$	Korada, Sasoglu, and U. 2009

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008
$P_B(N) \approx 2^{-(N)^{\Xi c(G)}}$	Korada, Sasoglu, and U. 2009
lossy source coding, Wyner-Ziv, Gelfand-Pinsker, ...	Korada and U. 2009

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008
$P_B(N) \approx 2^{-(N)^{\Xi c(G)}}$	Korada, Sasoglu, and U. 2009
lossy source coding, Wyner-Ziv, Gelfand-Pinsker, ...	Korada and U. 2009
efficient construction	Mori and Tanaka 2009

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008
$P_B(N) \approx 2^{-(N)^{\Xi c(G)}}$	Korada, Sasoglu, and U. 2009
lossy source coding, Wyner-Ziv, Gelfand-Pinsker, ...	Korada and U. 2009
efficient construction	Mori and Tanaka 2009
compound coding	Hassani, Korada and U. 2009

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008
$P_B(N) \approx 2^{-(N)^{\Xi c(G)}}$	Korada, Sasoglu, and U. 2009
lossy source coding, Wyner-Ziv, Gelfand-Pinsker, ...	Korada and U. 2009
efficient construction	Mori and Tanaka 2009
compound coding	Hassani, Korada and U. 2009
non-binary version and asym. channels	Arikan, Sasoglu, and Telatar 2009, Mori and Tanaka 2010

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008
$P_B(N) \approx 2^{-(N)^{\Xi c(G)}}$	Korada, Sasoglu, and U. 2009
lossy source coding, Wyner-Ziv, Gelfand-Pinsker, ...	Korada and U. 2009
efficient construction	Mori and Tanaka 2009
compound coding	Hassani, Korada and U. 2009
non-binary version and asym. channels	Arikan, Sasoglu, and Telatar 2009, Mori and Tanaka 2010
multiple-access channel	Abbe and Telatar 2010

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008
$P_B(N) \approx 2^{-(N)^{\Xi c(G)}}$	Korada, Sasoglu, and U. 2009
lossy source coding, Wyner-Ziv, Gelfand-Pinsker, ...	Korada and U. 2009
efficient construction	Mori and Tanaka 2009
compound coding	Hassani, Korada and U. 2009
non-binary version and asym. channels	Arikan, Sasoglu, and Telatar 2009, Mori and Tanaka 2010
multiple-access channel	Abbe and Telatar 2010
wire-tap channel	Mahdavifar and Vardy, Shamai 2010

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008
$P_B(N) \approx 2^{-(N)^{\Xi c(G)}}$	Korada, Sasoglu, and U. 2009
lossy source coding, Wyner-Ziv, Gelfand-Pinsker, ...	Korada and U. 2009
efficient construction	Mori and Tanaka 2009
compound coding	Hassani, Korada and U. 2009
non-binary version and asym. channels	Arikan, Sasoglu, and Telatar 2009, Mori and Tanaka 2010
multiple-access channel	Abbe and Telatar 2010
wire-tap channel	Mahdavifar and Vardy, Shamai 2010
scaling laws	Dembo, Hassani, Korada, Montanari, Telatar, and U. 2010

Summary of Known Results

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008
$P_B(N) \approx 2^{-(N)^{\Xi c(G)}}$	Korada, Sasoglu, and U. 2009
lossy source coding, Wyner-Ziv, Gelfand-Pinsker, ...	Korada and U. 2009
efficient construction	Mori and Tanaka 2009
compound coding	Hassani, Korada and U. 2009
non-binary version and asym. channels	Arikan, Sasoglu, and Telatar 2009, Mori and Tanaka 2010

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008
$P_B(N) \approx 2^{-(N)^{\Xi c(G)}}$	Korada, Sasoglu, and U. 2009
lossy source coding, Wyner-Ziv, Gelfand-Pinsker, ...	Korada and U. 2009
efficient construction	Mori and Tanaka 2009
compound coding	Hassani, Korada and U. 2009
non-binary version and asym. channels	Arikan, Sasoglu, and Telatar 2009, Mori and Tanaka 2010
multiple-access channel	Abbe and Telatar 2010

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008
$P_B(N) \approx 2^{-(N)^{\Xi c(G)}}$	Korada, Sasoglu, and U. 2009
lossy source coding, Wyner-Ziv, Gelfand-Pinsker, ...	Korada and U. 2009
efficient construction	Mori and Tanaka 2009
compound coding	Hassani, Korada and U. 2009
non-binary version and asym. channels	Arikan, Sasoglu, and Telatar 2009, Mori and Tanaka 2010
multiple-access channel	Abbe and Telatar 2010
wire-tap channel	Mahdavifar and Vardy, Shamai 2010

Summary of Known Results

achieve capacity on memoryless channels	Arikan 2007
$P_B(N) \approx 2^{-N^{\frac{1}{2}}}$	Arikan and Telatar 2008
$P_B(N) \approx 2^{-(N)^{\Xi c(G)}}$	Korada, Sasoglu, and U. 2009
lossy source coding, Wyner-Ziv, Gelfand-Pinsker, ...	Korada and U. 2009
efficient construction	Mori and Tanaka 2009
compound coding	Hassani, Korada and U. 2009
non-binary version and asym. channels	Arikan, Sasoglu, and Telatar 2009, Mori and Tanaka 2010
multiple-access channel	Abbe and Telatar 2010
wire-tap channel	Mahdavifar and Vardy, Shamai 2010
scaling laws	Dembo, Hassani, Korada, Montanari, Telatar, and U. 2010

Summary

+ completely new paradigm of coding

+ very elegant

+ provably achieves capacity

+ low complexity

+ many applications

Summary

+ completely new paradigm of coding

+ very elegant

+ provably achieves capacity

+ low complexity

+ many applications

- currently only competitive for VERY large N