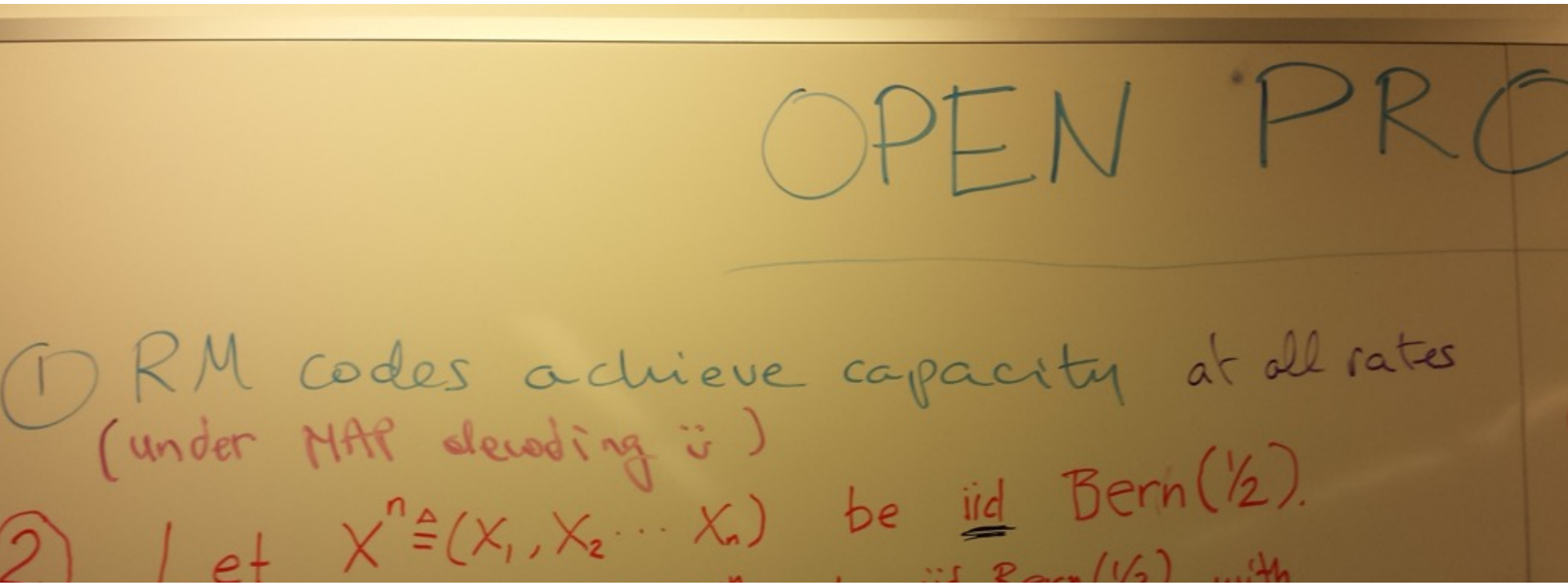
# Reed-Muller Codes Achieve Capacity on Erasure Channels

Henry D. Pfister
with S. Kudekar, S. Kumar, M. Mondelli, E. Şaşoğlu, R. Urbanke

48th Annual Symposium on the Theory of Computing
Boston, MA
June 20th, 2016


OPEN PRO
(1) RM codes achieve capacity at all rates
(under MAP decoding ü)
2) Let $X^n \triangleq (X_1, X_2 \cdots X_n)$ be iid Bern(½).


SIMONS
INSTITUTE
for the Theory of Computing

# Reed-Muller (RM) Codes (I)

- Codes by Muller, decoder by Reed, both in 1954
  - Multivariate polynomial evaluation codes over the binary field:

$$\mathrm{RM}(v,n) \triangleq \left\{ \underline{c} \in \mathbb{F}_2^{2^n} \,\middle|\, c_{\underline{x}} = f(\underline{x}), \underline{x} \in \mathbb{F}_2^n, f \in \mathbb{F}_2[x_1,\ldots,x_n], \deg(f) \leq v \right\}$$

# Reed-Muller (RM) Codes (I)

- Codes by Muller, decoder by Reed, both in 1954
  - Multivariate polynomial evaluation codes over the binary field:

$$\mathrm{RM}(v,n) \triangleq \left\{ \underline{c} \in \mathbb{F}_2^{2^n} \,\middle|\, c_{\underline{x}} = f(\underline{x}), \underline{x} \in \mathbb{F}_2^n, f \in \mathbb{F}_2[x_1,\ldots,x_n], \deg(f) \leq v \right\}$$

- Very popular in theoretical computer science (TCS)
  - locally decodable, locally testable, probabilistic proof systems

# Reed-Muller (RM) Codes (I)

- Codes by Muller, decoder by Reed, both in 1954
  - Multivariate polynomial evaluation codes over the binary field:

$$\mathrm{RM}(v,n) \triangleq \left\{ \underline{c} \in \mathbb{F}_2^{2^n} \,\middle|\, c_{\underline{x}} = f(\underline{x}), \underline{x} \in \mathbb{F}_2^n, f \in \mathbb{F}_2[x_1,\ldots,x_n], \deg(f) \leq v \right\}$$

- Very popular in theoretical computer science (TCS)
  - locally decodable, locally testable, probabilistic proof systems
- Capacity-Achieving Conjectures
  - By Shu Lin: "RM Codes are Not So Bad" (Tokyo ITW, 1988)
  - By Costello and Forney for Rate-1/2 and BI-AWGN, 2007

# Reed-Muller (RM) Codes (I)

- Codes by Muller, decoder by Reed, both in 1954
  - Multivariate polynomial evaluation codes over the binary field:

$$\mathrm{RM}(v,n) \triangleq \left\{ \underline{c} \in \mathbb{F}_2^{2^n} \,\middle|\, c_{\underline{x}} = f(\underline{x}), \underline{x} \in \mathbb{F}_2^n, f \in \mathbb{F}_2[x_1,\ldots,x_n], \deg(f) \leq v \right\}$$

- Very popular in theoretical computer science (TCS)
  - locally decodable, locally testable, probabilistic proof systems
- Capacity-Achieving Conjectures
  - By Shu Lin: "RM Codes are Not So Bad" (Tokyo ITW, 1988)
  - By Costello and Forney for Rate-1/2 and BI-AWGN, 2007
- First known conjecture in print by Dumer and Farrell in 1994
  - They show BCH codes achieve capacity on BEC as rate $\to 1$
  - Open problem stated for Reed-Muller codes with constant rate

# Reed-Muller (RM) Codes (II)

- Closely related to polar codes
  - From Hadamard matrix, one choice of rows generates Reed-Muller and some other polar codes

In fact Arikan remarked:

*It is interesting that the possibility of RM codes being capacity-achieving codes under ML decoding seems to have received no attention in the literature*

- Under MAP, Reed-Muller observed to be better than polar (Arikan and Mondelli-Hassani-Urbanke)

# Reed-Muller (RM) Codes (II)

- Closely related to polar codes
  - From Hadamard matrix, one choice of rows generates Reed-Muller and some other polar codes

In fact Arikan remarked:

*It is interesting that the possibility of RM codes being capacity-achieving codes under ML decoding seems to have received no attention in the literature*

- Under MAP, Reed-Muller observed to be better than polar (Arikan and Mondelli-Hassani-Urbanke)
- In 2014, Abbe-Shpilka-Wigderson showed capacity achieving for rates $\to 0, 1$ (erasures) and rates $\to 0$ (errors)

# Reed-Muller (RM) Codes (II)

- Closely related to polar codes
  - From Hadamard matrix, one choice of rows generates Reed-Muller and some other polar codes

In fact Arikan remarked:

*It is interesting that the possibility of RM codes being capacity-achieving codes under ML decoding seems to have received no attention in the literature*

- Under MAP, Reed-Muller observed to be better than polar (Arikan and Mondelli-Hassani-Urbanke)
- In 2014, Abbe-Shpilka-Wigderson showed capacity achieving for rates $\to 0, 1$ (erasures) and rates $\to 0$ (errors)
- Do Reed-Muller codes achieve capacity for constant rates?

# A Brief Note on Symmetry

- Consider a set $\mathcal{C} \subset \mathcal{X}^N$ of length-$N$ vectors
  - The permutation group of $\mathcal{C}$ is defined to be

$\mathcal{G} \triangleq \{\pi \in S_N \,|\, \pi(\underline{c}) \in \mathcal{C} \;\forall\; \underline{c} \in \mathcal{C}\}$ where $\underline{d} = \pi(\underline{c}) \Leftrightarrow d_{\pi(i)} = c_i$

# A Brief Note on Symmetry

- Consider a set $\mathcal{C} \subset \mathcal{X}^N$ of length-$N$ vectors
  - The permutation group of $\mathcal{C}$ is defined to be

$\mathcal{G} \triangleq \{\pi \in S_N \,|\, \pi(\underline{c}) \in \mathcal{C} \;\forall\; \underline{c} \in \mathcal{C}\}$ where $\underline{d} = \pi(\underline{c}) \Leftrightarrow d_{\pi(i)} = c_i$

- For example,

$$\mathcal{C} = \left\{ \begin{array}{cccc} (0 & 0 & 0 & 0) \\ (0 & 0 & 1 & 1) \\ (1 & 1 & 0 & 0) \\ (1 & 1 & 1 & 1) \end{array} \right\} \quad \Longrightarrow \quad \mathcal{G} = \left\langle \left( \begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{smallmatrix} \right) \left( \begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{smallmatrix} \right) \right\rangle$$

# A Brief Note on Symmetry

- Consider a set $\mathcal{C} \subset \mathcal{X}^N$ of length-$N$ vectors
  - The permutation group of $\mathcal{C}$ is defined to be

$\mathcal{G} \triangleq \{\pi \in S_N \,|\, \pi(\underline{c}) \in \mathcal{C} \;\forall\; \underline{c} \in \mathcal{C}\}$ where $\underline{d} = \pi(\underline{c}) \Leftrightarrow d_{\pi(i)} = c_i$

  - A permutation group $\mathcal{G}$ is transitive if, for all $i, j \in [N]$, there exists $\pi \in \mathcal{G}$ such that $\pi(i) = j$

- For example, $\mathcal{C}$ is transitive

$$\mathcal{C} = \left\{ \begin{array}{cccc} (0 & 0 & 0 & 0) \\ (0 & 0 & 1 & 1) \\ (1 & 1 & 0 & 0) \\ (1 & 1 & 1 & 1) \end{array} \right\} \quad \Longrightarrow \quad \mathcal{G} = \left\langle \left( \begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{smallmatrix} \right) \left( \begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{smallmatrix} \right) \right\rangle$$

# A Brief Note on Symmetry

- Consider a set $\mathcal{C} \subset \mathcal{X}^N$ of length-$N$ vectors
  - The permutation group of $\mathcal{C}$ is defined to be

$$\mathcal{G} \triangleq \{\pi \in S_N \,|\, \pi(\underline{c}) \in \mathcal{C} \;\forall\; \underline{c} \in \mathcal{C}\} \text{ where } \underline{d} = \pi(\underline{c}) \Leftrightarrow d_{\pi(i)} = c_i$$

  - A permutation group $\mathcal{G}$ is transitive if, for all $i, j \in [N]$, there exists $\pi \in \mathcal{G}$ such that $\pi(i) = j$
  - $\mathcal{G}$ is doubly transitive if, for any $i, j, k, l \in [N]$ with $i \neq j$ and $k \neq l$, there exists $\pi \in \mathcal{G}$ such that $\pi(i) = k$ and $\pi(j) = l$.
- For example, $\mathcal{C}$ is transitive but not doubly transitive

$$\mathcal{C} = \left\{ \begin{array}{cccc} (0 & 0 & 0 & 0) \\ (0 & 0 & 1 & 1) \\ (1 & 1 & 0 & 0) \\ (1 & 1 & 1 & 1) \end{array} \right\} \quad \Longrightarrow \quad \mathcal{G} = \left\langle \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{smallmatrix}\right) \right\rangle$$

# Capacity via Symmetry for Erasure Channels

Theorem: Let $\{\mathcal{C}_n\}$ be a sequence of binary linear codes with

- blocklengths $N_n \to \infty$ and rates $r_n \to r \in (0, 1)$ where
- the permutation group of each $\mathcal{C}_n$ is doubly transitive.

Then, $\{C_n\}$ achieves capacity on the BEC under bit-MAP decoding

# Capacity via Symmetry for Erasure Channels

Theorem: Let $\{\mathcal{C}_n\}$ be a sequence of binary linear codes with

- blocklengths $N_n \to \infty$ and rates $r_n \to r \in (0, 1)$ where
- the permutation group of each $\mathcal{C}_n$ is doubly transitive.

Then, $\{C_n\}$ achieves capacity on the BEC under bit-MAP decoding

## Important Consequences and Extensions

- Permutation groups of RM codes are doubly transitive [KLP]

  $\implies$ Reed-Muller codes achieve capacity
- Extends to linear affine-invariant codes over $\mathbb{F}_q$
- Primitive narrow-sense BCH codes achieve capacity
- Extends to block-MAP decoding for Reed-Muller and BCH

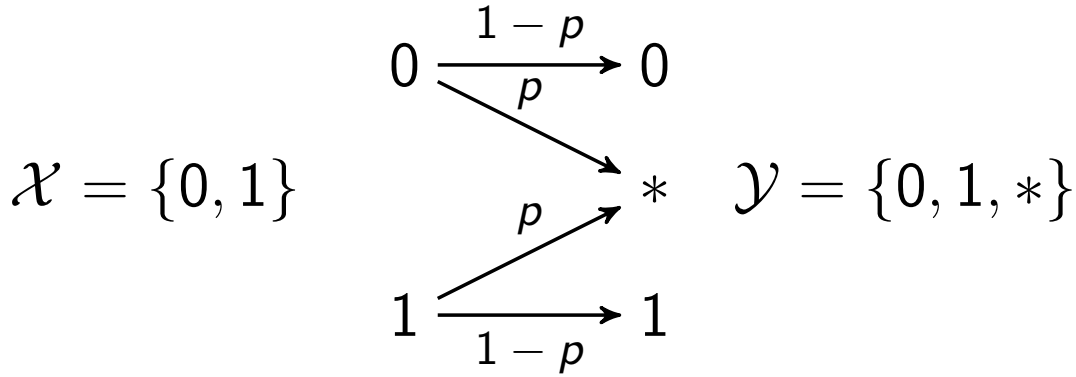
# Few Remarks

- Scope of the work
  - Linear Codes, Erasure Channels, MAP Decoding
- Three Main Ingredients
  - EXIT functions (from iterative decoding)
  - Monotone boolean functions (from computer science)
  - Automorphism/Permutation groups (from algebraic coding)

# Proof

# Basic Setup

- Binary linear code $\mathcal{C} \subset \{0,1\}^N$ is a $K$-dim. subspace of $\mathbb{F}_2^N$
- Binary Erasure Channel, parametrized by $p$




- $\underline{X} = (X_1, \ldots, X_N) \longleftrightarrow$ uniform codeword from $\mathcal{C}$
- $\underline{Y} = (Y_1, \ldots, Y_N) \longleftrightarrow$ received sequence from $\underline{X}$

# MAP Decoding on Erasure Channels

## Set of Consistent Codewords

$$\mathcal{C}(\underline{y}) = \{\underline{x} \in \mathcal{C} \quad | \quad x_i = y_i \quad \text{when } y_i \neq *\}$$

# MAP Decoding on Erasure Channels

## Set of Consistent Codewords

$$\mathcal{C}(\underline{y}) = \{\underline{x} \in \mathcal{C} \quad | \quad x_i = y_i \quad \text{when } y_i \neq *\}$$

## MAP Decoding of $\underline{X}$ versus $X_i$

- $|\mathcal{C}(\underline{y})| = 1 \longleftrightarrow$ one can recover codeword $\underline{X}$

# MAP Decoding on Erasure Channels

## Set of Consistent Codewords

$$\mathcal{C}(\underline{y}) = \{\underline{x} \in \mathcal{C} \quad | \quad x_i = y_i \quad \text{when } y_i \neq *\}$$

## MAP Decoding of $\underline{X}$ versus $X_i$

- $|\mathcal{C}(\underline{y})| = 1 \longleftrightarrow$ one can recover codeword $\underline{X}$
- If $x_i$ is the same for all $\underline{x} \in \mathcal{C}(\underline{y}) \longleftrightarrow$ one can recover $X_i$
  - $H(X_i|\underline{Y} = \underline{y}) = 0$

# MAP Decoding on Erasure Channels

## Set of Consistent Codewords

$$\mathcal{C}(\underline{y}) = \{\underline{x} \in \mathcal{C} \quad | \quad x_i = y_i \quad \text{when } y_i \neq *\}$$

## MAP Decoding of $\underline{X}$ versus $X_i$

- $|\mathcal{C}(\underline{y})| = 1 \longleftrightarrow$ one can recover codeword $\underline{X}$
- If $x_i$ is the same for all $\underline{x} \in \mathcal{C}(\underline{y}) \longleftrightarrow$ one can recover $X_i$
  - $H(X_i|\underline{Y} = \underline{y}) = 0$
- Otherwise
  - Half of codewords in $\mathcal{C}(\underline{y})$ have $x_i = 0$ and half have $x_i = 1$
  - uniform codeword $\longleftrightarrow$ uniform posterior
  - $H(X_i|\underline{Y} = \underline{y}) = 1$

# MAP Decoding on Erasure Channels

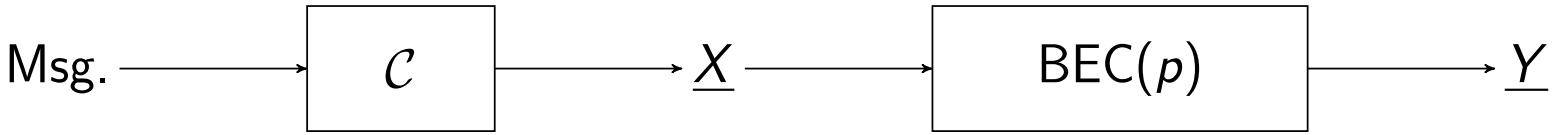
## Set of Consistent Codewords

$$\mathcal{C}(\underline{y}) = \{\underline{x} \in \mathcal{C} \quad | \quad x_i = y_i \quad \text{when } y_i \neq *\}$$

## MAP Decoding of $\underline{X}$ versus $X_i$

- $|\mathcal{C}(\underline{y})| = 1 \longleftrightarrow$ one can recover codeword $\underline{X}$
- If $x_i$ is the same for all $\underline{x} \in \mathcal{C}(\underline{y}) \longleftrightarrow$ one can recover $X_i$
  - $H(X_i|\underline{Y} = \underline{y}) = 0$
- Otherwise
  - Half of codewords in $\mathcal{C}(\underline{y})$ have $x_i = 0$ and half have $x_i = 1$
  - uniform codeword $\longleftrightarrow$ uniform posterior
  - $H(X_i|\underline{Y} = \underline{y}) = 1$
- $H(X_i|\underline{Y} = \underline{y})$ is either 0 or 1 (Boolean)

# First Ingredient: MAP EXIT Functions




EXtrinsic Information Transfer Function

## Definition

(Bit-$i$ MAP Erasure Prob.) $P_{b,i} = H(X_i \mid \underline{Y})$

(MAP Erasure Probability) $P_b = \frac{1}{N}\sum_{i=1}^{N} P_{b,i}$

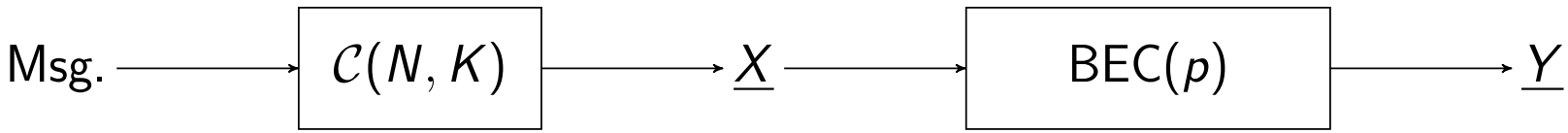
(Bit-$i$ EXIT Function) $h_i(p) = H(X_i \mid \underline{Y}_{\sim i})$

(Average EXIT Function) $h(p) = \frac{1}{N}\sum_{i=1}^{N} h_i(p)$

- Note: $\underline{Y}_{\sim i} = (Y_1, \ldots, Y_{i-1}, Y_{i+1}, \ldots, Y_N)$
- Closely related to each other:

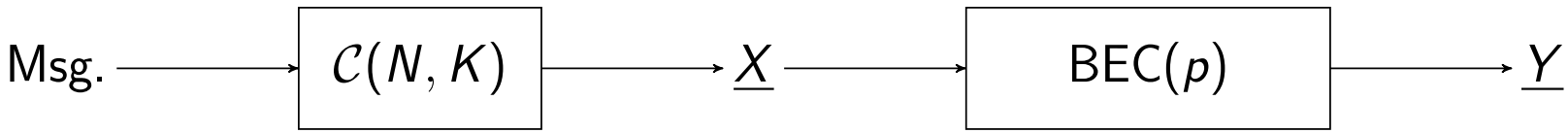
$$P_{b,i}(p) = p h_i(p) \qquad P_b(p) = p h(p)$$

# EXIT Functions and the Area Theorem




$$h_i(p) = H(X_i|\underline{Y}_{\sim i}) \qquad h(p) = \frac{1}{N}\sum_{i=1}^{N} h_i(p)$$

# EXIT Functions and the Area Theorem

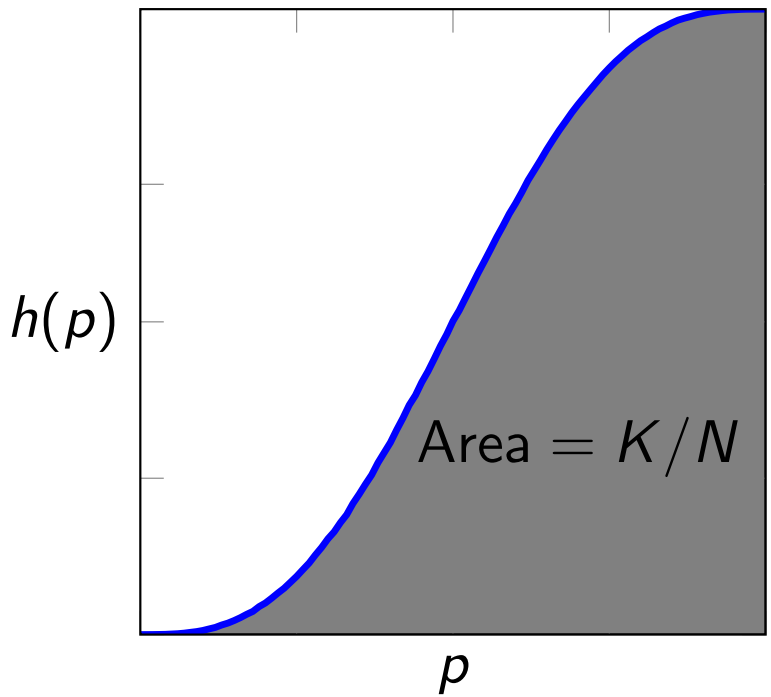



$$h_i(p) = H(X_i|\underline{Y}_{\sim i}) \qquad h(p) = \frac{1}{N}\sum_{i=1}^{N} h_i(p)$$

## Area Theorem

$$\int_0^1 h(p)dp = K/N$$

- Conservation Principle by Ashikhmin, ten Brink, and Kramer
- Not satisfied by $P_b$



# Capacity and EXIT Functions

A sequence of codes $\{\mathcal{C}_n\}$ with rates $r_n \to r$

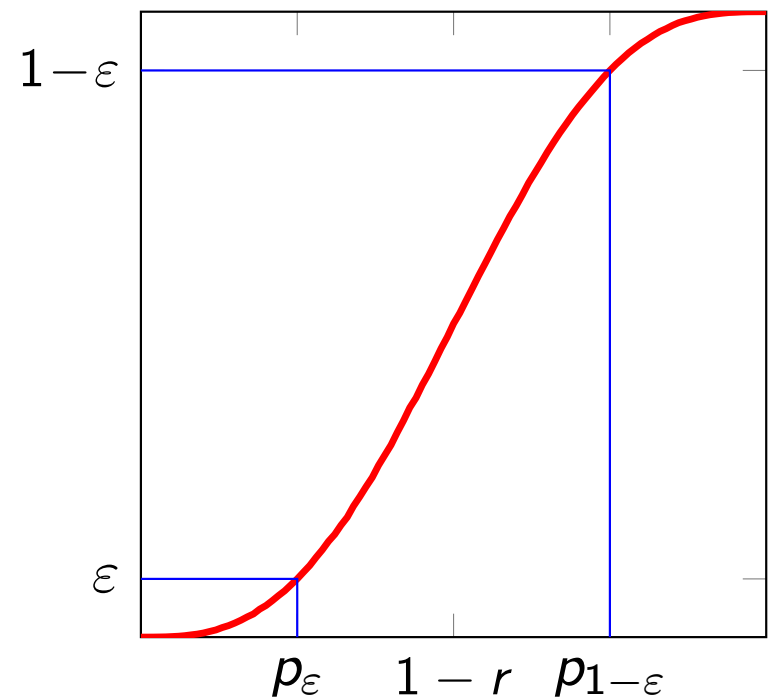
is capacity-achieving if $P_b^{(n)}(p) \to 0$ for all $p < 1 - r$.

The following are equivalent:

- $\{\mathcal{C}_n\}$ is capacity achieving
- $h^{(n)}(p) \to \begin{cases} 0, & \text{if } p < 1 - r, \\ 1, & \text{if } p > 1 - r. \end{cases}$
- Transition width vanishes

  For all $\varepsilon > 0$, $p_{1-\varepsilon}^{(n)} - p_{\varepsilon}^{(n)} \to 0$,

  where $p_\epsilon \triangleq h^{-1}(\epsilon)$



# Second Ingredient: Monotone Boolean Functions

## Definition

A boolean function $f_i : \{0,1\}^{N-1} \to \{0,1\}$ is uniquely defined by the set $\Omega_i \triangleq \{\underline{z} \in \{0,1\}^{N-1} \mid f_i(\underline{z}) = 1\}$ and called monotone if

$$\underline{z} \leq \underline{z}' \text{ implies } f_i(\underline{z}) \leq f_i(\underline{z}').$$

Consider the expectation $\mathbb{E}[f_i(\underline{Z})]$ when $\underline{Z}$ is an i.i.d. $B(p)$ vector

Let set of erasure patterns that prevent recovery of $X_i$ from $\underline{Y}_{\sim i}$ be

$$\Omega_i \triangleq \{\underline{z}_{\sim i} \in \{0,1\}^{N-1} \mid \exists\, \underline{x} \in \mathcal{C}, x_i = 1, \underline{x}_{\sim i} \leq \underline{z}_{\sim i}\},$$

Since adding erasures cannot help recover $X_i$, $f_i$ is monotone and

$$h_i(p) = \mathbb{P}(\underline{Z} \in \Omega_i) = \mathbb{E}[f_i(\underline{Z})]$$

# Symmetric Montone Boolean Functions

$f_i$ "symmetric" $\Leftrightarrow$ permutation group of $\Omega_i$ is transitive

- In this case, $h_i(p)$ has a sharp transition!
  ( Friedgut-Kalai, Talagrand, Bourgain-Kahn-Kalai-Linial )

$$p_{1-\varepsilon} - p_\varepsilon \leq 2C \frac{\log \frac{1}{\varepsilon}}{\log N}, \qquad p_{1-\varepsilon} - p_\varepsilon \to 0.$$

# Symmetric Montone Boolean Functions

$f_i$ "symmetric" $\Leftrightarrow$ permutation group of $\Omega_i$ is transitive

- In this case, $h_i(p)$ has a sharp transition!
  ( Friedgut-Kalai, Talagrand, Bourgain-Kahn-Kalai-Linial )

$$p_{1-\varepsilon} - p_{\varepsilon} \leq 2C \frac{\log \frac{1}{\varepsilon}}{\log N}, \qquad p_{1-\varepsilon} - p_{\varepsilon} \to 0.$$

Also

Avg. EXIT Function $h$, not $h_i$, satisfies Area Theorem

Bit-i EXIT Function $h_i$, not $h$, is monotone boolean

# Symmetric Montone Boolean Functions

$f_i$ "symmetric" $\Leftrightarrow$ permutation group of $\Omega_i$ is transitive

- In this case, $h_i(p)$ has a sharp transition!
  ( Friedgut-Kalai, Talagrand, Bourgain-Kahn-Kalai-Linial )

$$p_{1-\varepsilon} - p_{\varepsilon} \leq 2C \frac{\log \frac{1}{\varepsilon}}{\log N}, \qquad p_{1-\varepsilon} - p_{\varepsilon} \to 0.$$

Also

Avg. EXIT Function $h$, not $h_i$, satisfies Area Theorem

Bit-i EXIT Function $h_i$, not $h$, is monotone boolean

**Symmetry to the rescue!**

# Third Ingredient: Group Symmetry

The permutation group $\mathcal{G}$ of code $\mathcal{C}$ is defined to be

$$\mathcal{G} = \{\pi \in S_N \mid \pi(\underline{x}) \in \mathcal{C} \quad \forall\, \underline{x} \in \mathcal{C}\}$$

# Third Ingredient: Group Symmetry

The permutation group $\mathcal{G}$ of code $\mathcal{C}$ is defined to be

$$\mathcal{G} = \{\pi \in S_N \mid \pi(\underline{x}) \in \mathcal{C} \quad \forall\, \underline{x} \in \mathcal{C}\}$$

## Proposition

- If $\mathcal{G}$ is transitive, then

$$h_i(p) = h_j(p) = h(p) \quad \text{for all } 0 \leq p \leq 1$$

# Third Ingredient: Group Symmetry

The permutation group $\mathcal{G}$ of code $\mathcal{C}$ is defined to be

$$\mathcal{G} = \{\pi \in S_N \mid \pi(\underline{x}) \in \mathcal{C} \quad \forall\, \underline{x} \in \mathcal{C}\}$$

## Proposition

- If $\mathcal{G}$ is transitive, then

$$h_i(p) = h_j(p) = h(p) \quad \text{for all } 0 \leq p \leq 1$$

- If $\mathcal{G}$ is doubly transitive, then

$f_i$ is "symmetric" (i.e., permutation group of $\Omega_i$ is transitive)
and $h_i$ has a sharp transition

# EXIT Functions Under Double Transitivity

Under double transitivity: $h_i = h$ and $f_i$ is symmetric

# EXIT Functions Under Double Transitivity

Under double transitivity: $h_i = h$ and $f_i$ is symmetric

Symmetric Monotone Boolean Functions
Exhibit Sharp $0 - 1$ Transitions

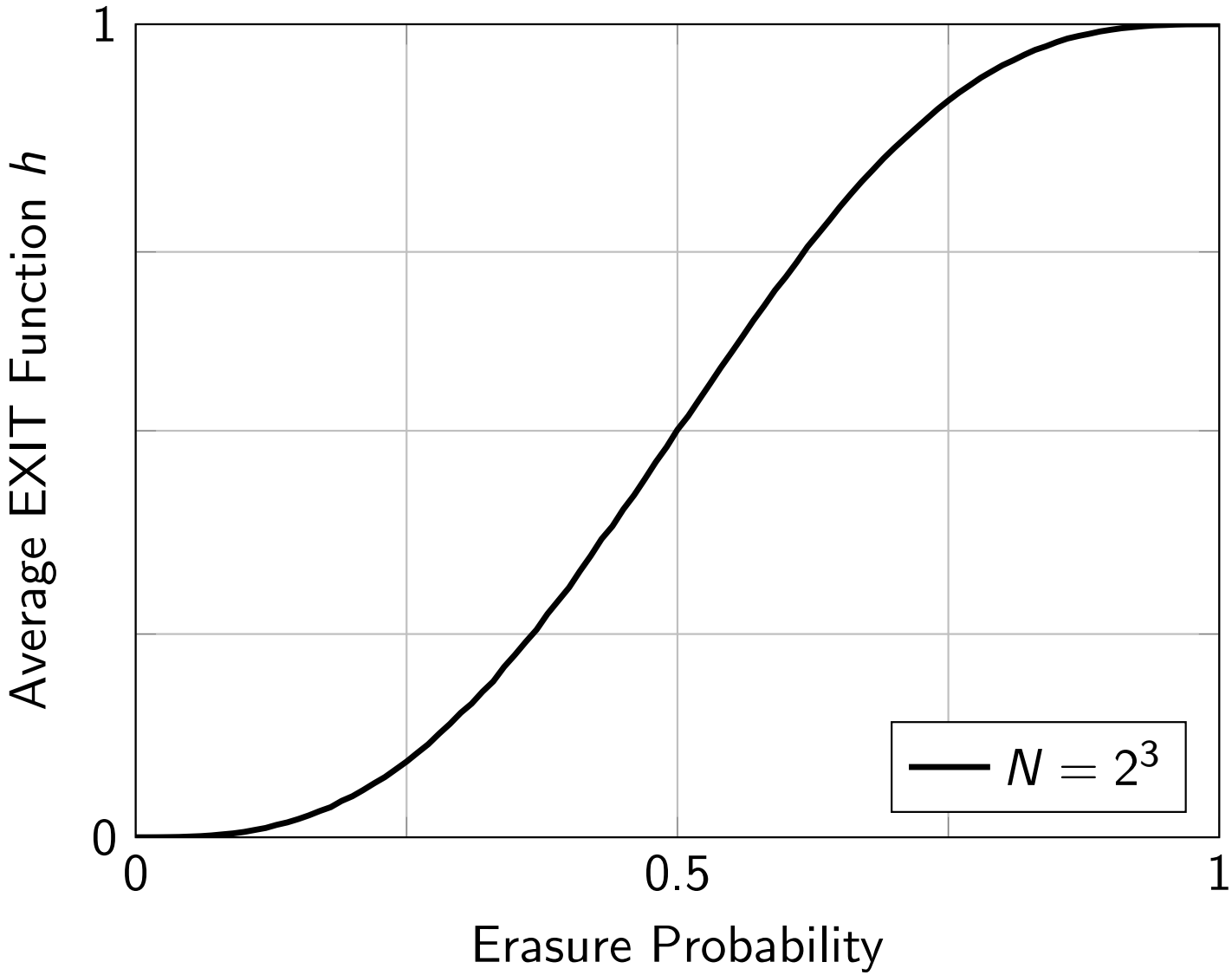
# EXIT Functions Under Double Transitivity

Under double transitivity: $h_i = h$ and $f_i$ is symmetric

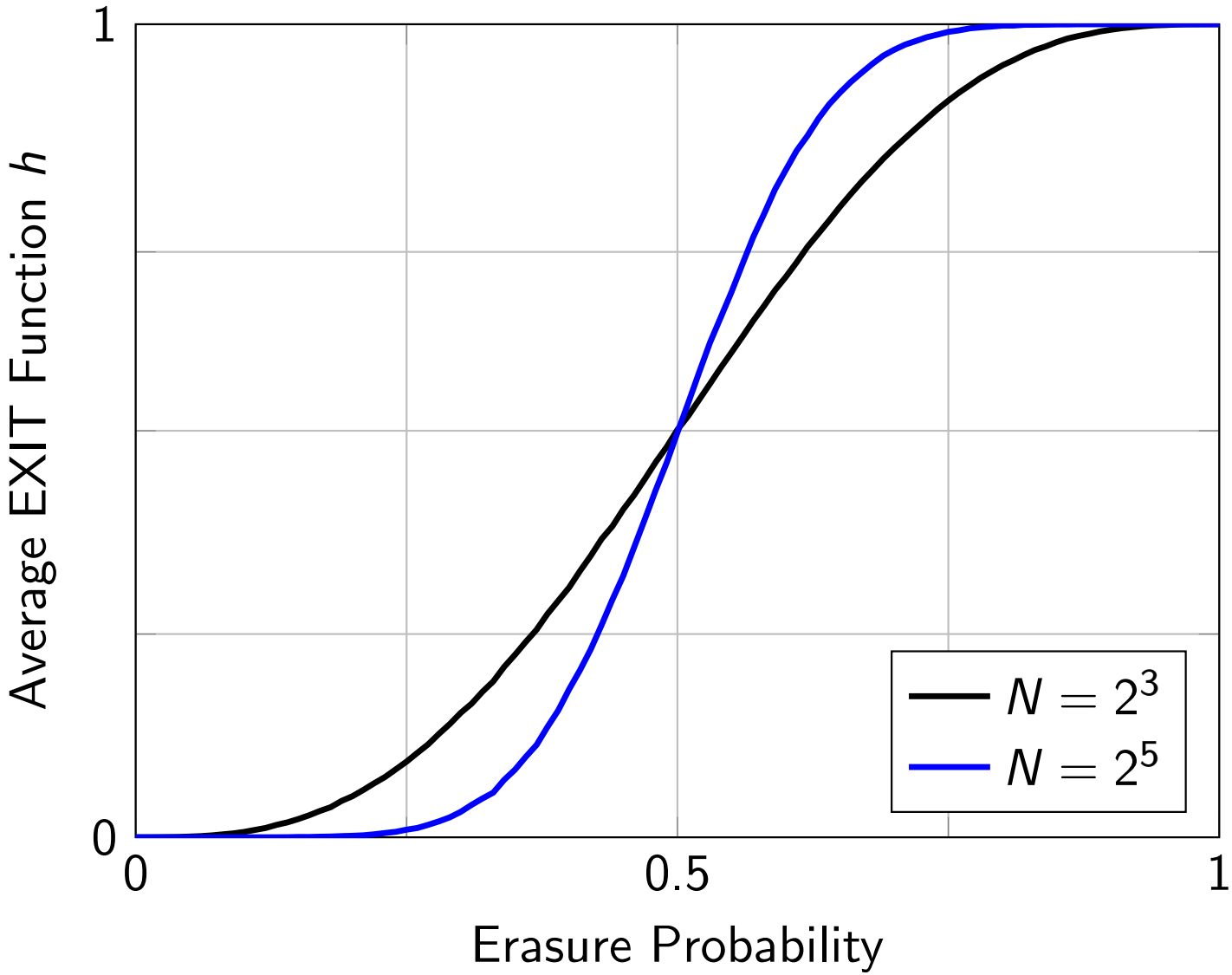
Symmetric Monotone Boolean Functions
Exhibit Sharp $0-1$ Transitions

Avg. EXIT Function $h$ has a sharp $0-1$ transition
Area theorem implies transition at $1-r$

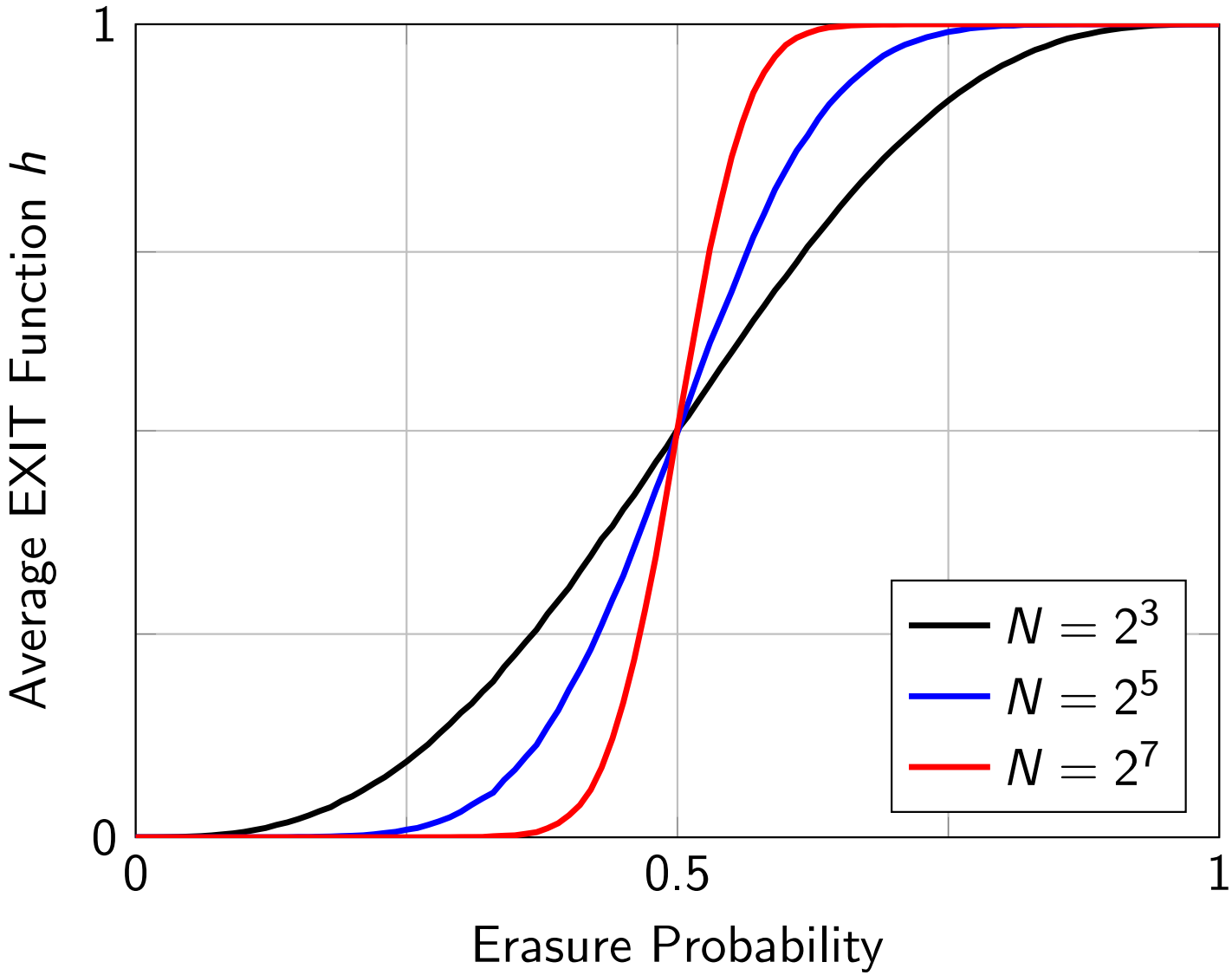
# Rate-1/2 Reed-Muller Codes



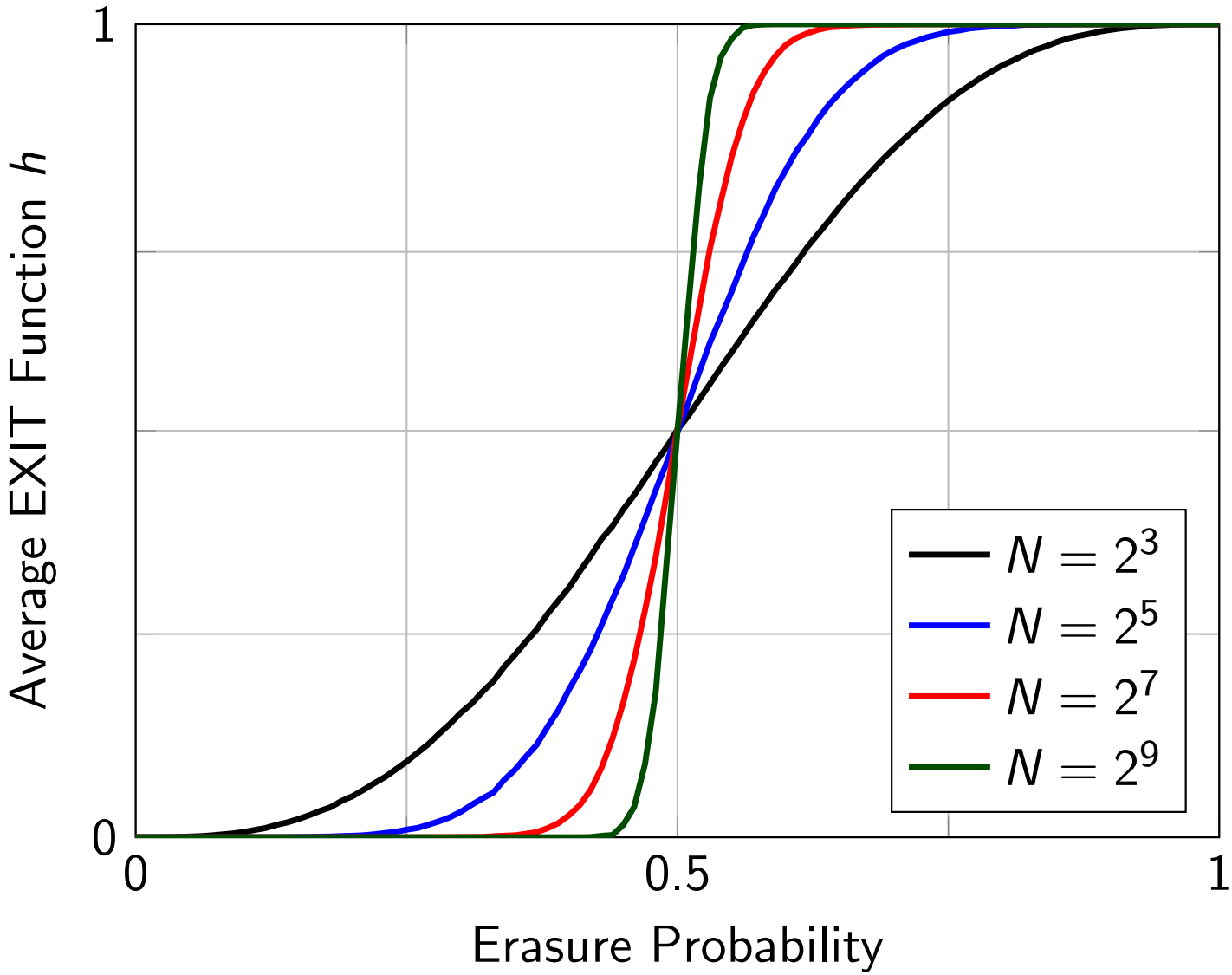
# Rate-1/2 Reed-Muller Codes



# Rate-1/2 Reed-Muller Codes



# Rate-1/2 Reed-Muller Codes



# Capacity via Symmetry

## Generality

- How general is this phenomenon?
- Proof heavily exploits MAP decoding on erasure channels
- Abbe et al. have shown for BSC when rate $\to 0$ [ASW]
- Extends to block-error rate for RM and BCH codes [BK]

## Open Questions

- Extension to general BMS channels
  - All ingredients except the sharp transition generalize naturally
- Practical decoders that achieve capacity for non-trivial rates
- Extension for BEC to rates converging to 0 or 1
  - Friedgut extended sharp threshold result to $p \to 0$ for $K$-SAT

# Thank You!