#### Reed-Muller Codes Achieve Capacity on BMS Channels

Galen Reeves<sup>1,2</sup> and Henry Pfister<sup>1,3</sup>

<sup>1</sup>Department of ECE <sup>2</sup>Department of Statistical Science <sup>3</sup>Department of Mathematics Duke University

Recent Advances in Coding Theory Workshop 54th Annual ACM Symposium on Theory of Computing Rome, Italy June 23, 2022

#### Outline

#### Introduction

Extrinsic Information Analysis

Ideas in Proof for BMS Channels

Conclusion

## Reed-Muller (RM) Codes

Codes by Muller, efficient suboptimal decoder by Reed, both in 1954

[N, K, D] binary code  $\mathsf{RM}(r, m)$  is indexed by integers  $0 \le r \le m$  with  $N = 2^m, \qquad K = \sum_{i=0}^r \binom{m}{i}, \qquad D = 2^{m-r}$ 

RM(r, m) is a multivariate polynomial evaluation code. defined by

$$\{ \boldsymbol{c} \in \mathbb{F}_2^N | c_{\tau(\boldsymbol{v})} = f(\boldsymbol{v}), \boldsymbol{v} \in \mathbb{F}_2^m, f \in \mathcal{F}_{r,m} \},$$

where  $\mathcal{F}_{r,m}$  is the set of multilinear polynomials in m vars  $(v_0, \ldots, v_{m-1})$  with binary coefs and degree  $\leq r$ , and  $\tau \colon \mathbb{F}_2^m \to [N]$  defines the bit order

#### Conjectured to Achieve Capacity...

- First discussed in 1990s by Lin, 1993 and Dumer, Farrell, 1994
- Stated explicitly for Gaussian noise by Costello, Forney, 2007
- Discussed further following polar codes Arikan, 2010
- ▶ Proved for BEC/BSC if rate  $\rightarrow 0/1$  by Abbe, Shpilka, Widgerson, 2014
- Open problem at 2015 Simons Institute Program on Information Theory
- Proved for BEC by Kudekar, Kumar, Mondelli, Pfister, Şaşoğlu, Urbanke, 2016
- RM codes polarize and "Twin RM" codes achieve capacity Abbe, Ye, 2020
- Reliable on BSC but gap to capacity by Hazła, Samorodnitsky, Sberlo, 2021

This list is not exhaustive and we apologize for any neglected references

Binary Memoryless Symmetric (BMS) Channels



Binary input, real output:

$$\boldsymbol{X} = (X_0, \dots, X_{N-1}) \in \{\pm 1\}^N, \qquad \boldsymbol{Y} = (Y_0, \dots, Y_{N-1}) \in \mathbb{R}^N$$

• Memoryless:  

$$p(y_0, \dots, y_{N-1} \mid x_0, \dots, x_{N-1}) = \prod_{i=0}^{N-1} w(y_i \mid x_i)$$

Symmetric:

$$w(y \mid +1) = w(-y \mid -1)$$

• Generated by IID multiplicative noise  $\mathbf{Z} = (Z_0, \ldots, Z_{N-1}) \in \mathbb{R}^N$ :

$$Y_i = X_i Z_i \quad \Leftrightarrow \quad \mathbf{Y} = \mathbf{X} \odot \mathbf{Z},$$
  
BSC(p):  $p = \Pr(Z_i = -1) = 1 - \Pr(Z_i = 1)$ 

#### Capacity of Binary Memoryless Symmetric (BMS) Channels

- ▶ Defined by single channel use with uniform input  $X \in \{\pm 1\}$  and output Y $C = 1 - H(X \mid Y)$
- Consider a family of BMS channels  $\{W_t : 0 \le t \le 1\}$  with capacity C(t)
  - Ordered by degradation from perfect (t = 0) to uninformative (t = 1)
  - **•** Examples include BEC(t), BSC(t/2), and BIAWGN with  $\sigma^2 = \frac{t}{1-t}$
- Shannon's theorem: Random codes have sharp threshold for block error at  $t_B^*$ :



#### Main Result

#### Theorem

Consider a BMS channel with capacity  $C \in (0,1)$ . For every RM(r,m) code with rate R < C, the bit-error rate under bit-MAP decoding satisfies

$$\mathsf{BER}(X_i \mid \boldsymbol{Y}) \le \frac{3\ln(m) + 17}{5\sqrt{m}(C - R)}$$

for all  $i \in [N] := \{0, 1, \dots, N-1\}$ . Thus, there exists a sequence of RM codes with increasing blocklength  $N = 2^m$  and rate converging to C such that the BER under bit-MAP decoding converges to zero.

This is proved in arXiv:2110.14631 and these slides outline some of the key steps.



Introduction

Extrinsic Information Analysis

Ideas in Proof for BMS Channels

Conclusion

#### Group Symmetry Refresher

The Permutation Automorphism Group  $\mathcal{G}$  of code  $\mathcal{C}$  is defined to be

 $\mathcal{G} = \{ \pi \in S_N \mid \forall \, \boldsymbol{c} \in \mathcal{C}, \ (c_{\pi(0)}, c_{\pi(1)}, \dots, c_{\pi(N-1)}) \in \mathcal{C} \}$ 

#### Transitive Permutation Groups

▶  $\mathcal{G}$  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 all distinct  $i, j, k \in [N]$ , there exists  $\pi \in \mathcal{G}$  such that  $\pi(i) = i$  and  $\pi(j) = k$ 



#### Extrinsic Information Idea and Analysis

- Used to describe turbo decoding by Berrou, Glavieux, and Thitimajshima, 1993
- Focuses on recovering a single input  $X_i$  from all other outputs  $Y_{\sim i}$ 
  - Independent of i for codes with transitive symmetry
  - Related to bit-error probability rather than block-error probability
- Analysis by ten Brink, 1999 and Ashikhmin, Kramer, ten Brink, 2004

▶ The key idea is the Area Theorem for the BEC(*t*):

$$\frac{d}{dt}\frac{1}{N}H(\boldsymbol{X}|\boldsymbol{Y}(t)) = \underbrace{\frac{1}{N}\sum_{i=1}^{N}H(X_i \mid Y_{\sim i}(t))}_{\text{EXIT function}}$$

Prove capacity via sharp threshold with jump localized by Area Theorem

$$\int_0^1 H\bigl(X_0 \,|\, Y_{\sim 0}(t)\bigr) \,dt = \frac{1}{N} H(\boldsymbol{X}) = \text{code rate}.$$

## Proof for Binary Erasure Channel [KKMPSU16]

- ▶ Let  $E \in \{0,1\}^N$  be the erasure indicator vector (i.e.,  $E_i = 1$  iff  $Y_i = ?$ )
- Linear code + BEC(t)  $\Rightarrow$  Conditioned on  $Y_{\sim i}$  there are only two cases:

 $X_i$  can be decoded or  $X_i$  is uniform (no information)

- " $X_i$  is uniform" iff  $g(E_{\sim i}) = 1$  for a monotone Boolean function g
  - $\blacktriangleright \mathbb{E}[g(E_{\sim i})] = h_i(t) \coloneqq H(X_i | Y_{\sim i})$
  - Area Theorem:  $\int_0^1 h_i(t) dt = R$  by transitive symmetry

All symmetric monotone Boolean functions have a sharp threshold!

Stated by Friedgut, Kalai 1996 for monotone graph properties

Thus, sequences of doubly transitive codes achieve capacity on BEC!

#### A Few Open Questions related to the BEC Result

- ▶ For RM codes on BEC, this proof fails for rate  $1-N^{-\alpha}$  with  $\alpha \in (0,1)$ . Can one extend boolean function argument to a wider range?
- ▶ For RM codes, does the EXIT function have transition width  $\tilde{O}(N^{-1/2})$ ?
- No known counterexamples for transitive codes with D<sub>min</sub>, D<sup>⊥</sup><sub>min</sub>→∞. Do all reasonable transitive code sequences achieve capacity?



Introduction

Extrinsic Information Analysis

Ideas in Proof for BMS Channels

Conclusion

#### Area Theorem for Generalized EXIT Function

Integral of derivative def by Méasson, Montanari, Richardson, Urbanke, 2009

$$NR = \underbrace{H(\boldsymbol{X} \mid \boldsymbol{Y}(t=1))}_{\log_2 \# \text{messages}} - \underbrace{H(\boldsymbol{X} \mid \boldsymbol{Y}(t=0))}_{=0} = \int_0^1 \frac{d}{dt} H(\boldsymbol{X} \mid \boldsymbol{Y}(t)) dt$$

Total derivative + chain rule for entropy + transitive symmetry gives



#### Going Beyond the Erasure Channel

What measure of uncertainty to analyze?

- ► The "GEXIT function" satisfies the area theorem but lacks interpretability
- Standard generalizations of hypercontractivity do not imply a sharp threshold

Key observation:

▶ Nesting property: RM codes contain shorter RM codes of nearly the same rate

Our approach:

Minimum mean-square error (MMSE) has almost all the right properties

$$\mathsf{mmse}(X_i|O) \coloneqq \mathbb{E}\Big[ (X_i - \mathbb{E}[X_i|O])^2 \Big]$$

- Use variance decomposition, generalized influence and estimation inequalities to analyze difference between short and long RM codes with similar rates
- New information inequalities connect the MMSE to entropy and code rate

#### Nested Structure of Reed-Muller Codes



- ► This diagram illustrates a copy of RM(r, m) inside RM(r, m + k) for k = 2. It is generated by degree-≤r monomials in variables v<sub>0</sub>,..., v<sub>m-1</sub>.
- $A = \{1, ..., 2^{m-k} 1\}$  and  $B = \{2^{m-k}, ..., 2^m 1\}$  index bits in RM(r, m+k)
- A second copy is generated by degree- $\leq r$  monomials in variables  $v_0, \ldots, v_{m-k-1}$ ,  $v_m, \ldots, v_{m+k-1}$  and supported on  $\{0\} \cup A \cup C$  with

$$C = \bigcup_{j=1}^{2^{k}-1} \left( \{0, 1, \dots, 2^{m-k} - 1\} + j2^{m} \right)$$

#### Rate Difference for Nearby Reed-Muller Codes

• The rate of RM(r, m) is given by

$$R(r,m) \coloneqq \frac{1}{2^m} \sum_{i=0}^r \binom{m}{i}$$

If Q<sub>m</sub> ~ Binomial(m, <sup>1</sup>/<sub>2</sub>), then R(r, m) = Pr(Q<sub>m</sub> ≤ r)
 By the CLT, (Q<sub>m</sub> - <sup>m</sup>/<sub>2</sub>)/√<sup>m</sup>/<sub>4</sub> → N(0, 1)

For  $k \ge 1$ , improved CLT for symmetric binomial shows that

$$R(r,m) - R(r,m+k) \le \frac{3k+4}{5\sqrt{m}}$$

- Thus, the rate difference vanishes for sequences where  $k = o(\sqrt{m})$ .
- ► This is quite surprising because it means that there is a puncturing pattern for RM(r, m + k), keeping only a fraction 2<sup>-k</sup> of the code bits, that does not appreciably change the code rate.

#### The Extrinsic MMSE – Definition and Properties

▶ Define the extrinsic MMSE as a function of channel parameter *t*:

$$M(t) \coloneqq \mathsf{mmse}(X_i \mid Y_{\sim i}) = 1 - \left\| \mathbb{E}[X_i \mid Y_{\sim i}] \right\|_2^2,$$

where  $\|\cdot\|_p \coloneqq \mathbb{E}[(\,\cdot\,)^p]^{1/p}$  and i can be dropped by transitive symmetry

For a seq. of codes, the extrinsic MMSE has a sharp threshold if and only if  $\lim_{N\to\infty}\int_0^1 M(t)(1-M(t))\,dt=0$ 

i.e., M(t) converges to a 0/1 step function

#### Extrinsic MMSE Analysis

▶ Input  $X = (X_0 \dots X_{2^m-1})$  is an  $\mathsf{RM}(r, m)$  codeword

- Output  $\mathbf{Y}(t) = (Y_0(1) \dots Y_{2^m-1}(t))$  is from a family of BMS channels, ordered from perfect (t = 0) to uninformative (t = 1)
- Extrinsic MMSE

$$M(t) \coloneqq \mathsf{mmse}(X_i \mid Y_{\sim i}) = 1 - \left\| \mathbb{E}[X_i \mid Y_{\sim i}] \right\|_2^2$$

Goal is to show sharp threshold and then localize jump via "area theorem"



#### Visualizing a Sharp Threshold



## Preliminary Intuition for Sharp Threshold Argument

- For  $k \ge 1$ , RM(r, m+k) can be punctured in multiple ways to get RM(r, m)
- $\blacktriangleright$  Consider estimation of  $X_0$  using either the long code or two short codes
- Hand Waving Argument
  - Choose t so that R(r, m+k) < C(t) < R(r, m)
  - C(t) < R(r,m) implies RM(r,m) estimate is imperfect (i.e., M(t) > 0)
  - For RM(r, m+k), combine two RM(r, m) estimates to reduce MMSE
  - For the code sequence  $RM(r_m, m)$ , we either have:
    - (A) the limit of the mmse $(X_0|Y_A, Y_B, Y_C)$  for RM $(r_m, m+k)$  will be strictly lower than the limit of mmse $(X_0|Y_A, Y_B)$  for RM $(r_m, m)$
    - (B) OR the two RM( $r_m, m$ ) estimates will be equal in the limit. More specifically, we will have  $\|\mathbb{E}[X_0|Y_A, Y_B] \mathbb{E}[X_0|Y_A, Y_C]\| \to 0$ .
- Our current proof is quite different but comes from this rough intuition

#### Decomposition of Variance

BMS + linear code gives the variance identity

$$M(t)(1 - M(t)) = \frac{1}{2} \left\| \mathbb{E}[X_i | Y_{\sim i}] - \mathbb{E}[X_i | Y'_{\sim i}] \right\|_2^2$$

where  $oldsymbol{Y}'=(Y_1',\ldots,Y_N')$  is resampled output with the same input.

- ▶ Resampling  $\boldsymbol{Y}$  should only change estimate only if  $M(t) \in [\delta, 1-\delta]$  for  $\delta > 0$
- Efron-Stein Inequality: For any partition  $\{A, B\}$  of  $\{1, \ldots, N\}\setminus i$ , the above term is bounded from above by

$$\frac{\frac{1}{2} \left\| \mathbb{E}[X_i | Y_A, Y_B] - \mathbb{E}[X_i | Y'_A, Y_B] \right\|_2^2}{\prod_{f_A := \text{ influence of } A} + \underbrace{\frac{1}{2} \left\| \mathbb{E}[X_i | Y_A, Y_B] - \mathbb{E}[X_i | Y_A, Y'_B] \right\|_2^2}_{\prod_{f_B := \text{ influence of } B}}.$$

Can be seen as generalized influence functions for sets (See O'Donnell, 2014)

# Proof of Sharp Threshold

For 
$$A = \{1, \dots, 2^{m-k} - 1\}$$
 and  $B = \{2^{m-k}, \dots, 2^m - 1\}$  we show that  

$$\underbrace{\int_0^1 \operatorname{Inf}_A dt \leq 2^{-k}}_{\text{double transitivity}} \quad \text{and} \quad \underbrace{\int_0^1 \operatorname{Inf}_B dt \leq \frac{k}{\sqrt{m}}}_{\text{RM nesting property}}$$

Choosing 
$$k=\lceil\frac{1}{2}\log_2 m\rceil$$
 yields 
$$\int_0^1 M(t)(1-M(t))\lesssim \frac{\log m}{\sqrt{m}}$$

#### From Influence to Difference in MMSE



How Much Better is the Longer Code?



# Proof of (♥) via Nesting Property



$$\begin{split} \sqrt{2 \operatorname{Inf}_B} &= \left\| \mathbb{E}[X_0 \mid Y_A, Y_B] - \mathbb{E}[X_0 \mid Y_A, Y_B'] \right\|_2 \\ &= \left\| \mathbb{E}[X_0 \mid Y_A, Y_B] - \mathbb{E}[X_0 \mid Y_A, Y_C] \right\|_2 & \text{nesting property} \\ &= \left\| \mathbb{E}[X_0 \mid Y_A, Y_B] - \hat{X}_0 - \mathbb{E}[X_0 \mid Y_A, Y_C] + \hat{X}_0 \right\|_2 & \hat{X}_0 \coloneqq \mathbb{E}[X_0 \mid Y_1 \dots Y_{2^{m+k}-1}] \\ &\leq \left\| \mathbb{E}[X_0 \mid Y_A, Y_B] - \hat{X}_0 \right\|_2 + \left\| \mathbb{E}[X_0 \mid Y_A, Y_C] - \hat{X}_0 \right\|_2 & \text{triangle inequality} \\ &= 2 \left\| \mathbb{E}[X_0 \mid Y_1 \dots Y_{2^{m}-1}] - \mathbb{E}[X_0 \mid Y_1 \dots Y_{2^{m+k}-1}] \right\|_2 & \text{equal in distribution} \\ &= 2 \sqrt{\left\| \mathbb{E}[X_0 \mid Y_1 \dots Y_{2^{m+k}-1}] \right\|_2^2 - \left\| \mathbb{E}[X_0 \mid Y_1 \dots Y_{2^{m}-1}] \right\|_2^2} & \text{nested expectation} \\ &= 2 \sqrt{\operatorname{mmse}(X_0 \mid Y_1 \dots Y_{2^{m}-1}) - \operatorname{mmse}(X_0 \mid Y_1 \dots Y_{4^{-1}})} & \text{definition of mmse} \end{split}$$

## From Difference in MMSE to Difference in Entropy

#### Lemma

Consider a family of BMS channels  $\{W_t : 0 \le t \le 1\}$ :

Ordered by degradation from perfect (t = 0) to uninformative (t = 1)

 <sup>d</sup>/<sub>dt</sub> mmse(X<sub>0</sub> | Y<sub>0</sub>(t)) ≥ constant

Then

$$M(t) - M^{+}(t) \lesssim \frac{d}{dt} \left( \frac{H(\boldsymbol{X} \mid \boldsymbol{Y}(t))}{2^{m}} - \frac{H(\boldsymbol{X}^{+} \mid \boldsymbol{Y}^{+}(t))}{2^{m+k}} \right) \quad (\clubsuit)$$

where  $(\mathbf{X}^+, \mathbf{Y}^+(t))$  is input-output pair for  $\mathsf{RM}(r, m+k)$  code.

Extrinsic Series Expansion of GEXIT Function

Law of total derivative + chain rule + transitive symmetry

$$\frac{d}{dt} \frac{H(\boldsymbol{X} \mid \boldsymbol{Y}(t))}{2^m} = \underbrace{\frac{\partial}{\partial s} H(X_0 \mid Y_0(s), Y_{\sim 0}(t))}_{\text{GEXIT function}} \Big|_{s=t}$$

▶ Series expansion of entropy with positive coefficients  $c_n > 0$ .

$$H\left(X_0 \,|\, Y_0(s), Y_{\sim 0}(t)\right) = \sum_{n=1}^{\infty} c_n \left(1 - \underbrace{\left\|\mathbb{E}[X_0 \,|\, Y_0(s)]\right\|_{2n}^2}_{\text{direct}}\right) \left(1 - \underbrace{\left\|\mathbb{E}[X_0 \,|\, Y_{\sim 0}(t)]\right\|_{2n}^2}_{\text{extrinsic}}\right)$$

Proof of (♠) via Series Expansion + Channel Ordering

$$\begin{split} \frac{d}{dt} \bigg( \frac{H(\mathbf{X} \mid \mathbf{Y}(t))}{2^m} &- \frac{H(\mathbf{X}^+ \mid \mathbf{Y}^+(t))}{2^{m+k}} \bigg) \\ &= \sum_{n=1}^{\infty} c_n \bigg( \underbrace{-\frac{d}{ds} \big\| \mathbb{E}[X_0 \mid Y_0(s)] \big\|_{2n}^{2n} \big|_{s=t}}_{\geq 0 \text{ by channel ordering}} \bigg) \bigg( \underbrace{ \underbrace{ \big\| \mathbb{E}[X_0 \mid Y^+_{\sim 0}(t)] \big\|_{2n}^{2n} - \big\| \mathbb{E}[X_0 \mid Y_{\sim 0}(t)] \big\|_{2n}^{2n}}_{\geq 0 \text{ by data processing inq.}} \bigg) \\ &\geq c_1 \bigg( \underbrace{-\frac{d}{ds} \big\| \mathbb{E}[X_0 \mid Y_0(s)] \big\|_2^2 \big|_{s=t}}_{\frac{d}{dt} \text{ mmse}(X_0 \mid Y_0(t))} \bigg) \bigg( \underbrace{ \big\| \mathbb{E}[X_0 \mid Y^+_{\sim 0}(t)] \big\|_2^2 - \big\| \mathbb{E}[X_0 \mid Y_{\sim 0}(t)] \big\|_2^2 }_{M(t) - M^+(t)} \bigg) \end{split}$$

#### Putting the Pieces Together

$$\begin{split} \int_{0}^{1} \operatorname{Inf}_{B} dt \lesssim \int_{0}^{1} \left( M(t) - M^{+}(t) \right) dt & (\checkmark) \\ \lesssim \int_{0}^{1} \frac{d}{dt} \left( \frac{H(\boldsymbol{X} \mid \boldsymbol{Y}(t))}{2^{m}} - \frac{H(\boldsymbol{X}^{+} \mid \boldsymbol{Y}^{+}(t))}{2^{m+k}} \right) dt & (\bigstar) \\ &= \frac{H(\boldsymbol{X})}{2^{m}} - \frac{H(\boldsymbol{X}^{+})}{2^{m+k}} & t = 0 \text{ perfect, } t = 1 \text{ useless} \\ &= R(r,m) - R(r,m+k) & \text{uniform codewords} \\ &\leq \frac{3k+4}{5\sqrt{m}} & \text{rate difference lemma} \end{split}$$

Average influence of large set vanishes if  $k = o(\sqrt{m})$ 

## Summary

- This talk outlined some key steps to prove a sharp threshold for M(t)
- What parts did we skip?
  - Going from extrinsic MMSE to entropy requires the channel with  $t = \text{mmse}(X_i|Y_i)$  and we skipped argument that extends to all channels.
  - Localizing the M(t) jump to the capacity limit. For this, we derive a few simple bounds connecting M(t) and the GEXIT function. The GEXIT area theorem allows one to localize the jump similar to the BEC case.
  - ▶ Bounding the contribution of each term in A set to the quantity  $\int M(t)(1 M(t)) dt$ . This uses an extra look argument and bounds the GEXIT (with an extra look) using an entropy series expansion. The final bound uses the GEXIT area theorem via symmetrization.

#### Outline

Introduction

Extrinsic Information Analysis

Ideas in Proof for BMS Channels

Conclusion

#### Conclusions and Open Questions

Summary of main results:

- Proof that RM codes achieve capacity on BMS channels i.e., vanishing fraction of incorrectly decoded inputs
- Approach based on analyzing extrinsic information
- > Unlike previous result for erasure channel, does not rely on hypercontractivity
- Proof combines a nesting property of RM codes with new information inequalities for GEXIT functions and the extrinsic MMSE

Open Questions:

- Does the block error probability goes to zero? Prove it.
- Can we extend this to code families beyond Reed-Muller?

#### References I

- [AKtB04] A. Ashikhmin, G. Kramer, and S. ten Brink. Extrinsic information transfer functions: model and erasure channel properties. *IEEE Trans. Inform. Theory*, 50(11):2657–2674, Nov. 2004.
- [BGT93] Claude Berrou, Alain Glavieux, and Punya Thitimajshima. Near Shannon limit error-correcting coding and decoding: Turbo-codes. In Proc. IEEE Int. Conf. Commun., volume 2, pages 1064–1070, Geneva, Switzerland, May 1993. IEEE.
- [FK96] Ehud Friedgut and Gil Kalai. Every monotone graph property has a sharp threshold. Proc. Amer. Math. Soc., 124(10):2993–3002, 1996.
- [MMRU09] C. Méasson, A. Montanari, T. J. Richardson, and R. Urbanke. The generalized area theorem and some of its consequences. *IEEE Trans. Inform. Theory*, 55(11):4793–4821, Nov. 2009.
- [MMU08] Cyril Méasson, Andrea Montanari, and Rüdiger L. Urbanke. Maxwell construction: The hidden bridge between iterative and maximum a posteriori decoding. IEEE Trans. Inform. Theory, 54(12):5277–5307, Dec. 2008.

#### References II

#### [MU03] C Méasson and R Urbanke. An upper-bound for the ML threshold of iterative coding systems over the BEC. In Proc. Annual Allerton Conf. on Commun., Control, and Comp., page 3, 2003.

#### [tB01] S. ten Brink.

Exploiting the chain rule of mutual information for the design of iterative decoding schemes.

In Proc. 39th Annual Allerton Conf. on Commun., Control, and Comp., Monticello, IL, USA, Oct. 2001.