On the Complexity of Reliable Communication on the Erasure Channel

Aamod Khandekar
California Institute of Technology
Pasadena, CA 91125, U.S.A.
email:aamod@systems.caltech.edu

Robert J. McEliece
California Institute of Technology
Pasadena, CA 91125, U.S.A.
email:rjm@systems.caltech.edu

Abstract — **We discuss the complexity of achieving channel capacity on the binary erasure channel (BEC) in view of recent advances. We also extrapolate to conjecture complexity bounds on more general channels.**

I. Introduction. The Classical Results

Consider a discrete memoryless channel with capacity C. We ask "how hard is it to achieve channel capacity?" This question is as old as the channel coding theorem, of course, but in the wake of the turbo coding revolution, its answer appears to be far less discouraging than previously suspected. However, to date the only channel model for which "turbo-like" codes are known rigorously to get all the way to capacity is the binary erasure channel. In this paper, therefore, we largely limit our remarks to the BEC.

Let us denote by $\chi_E(\epsilon,\pi)$ and $\chi_D(\epsilon,\pi)$ the minimum possible encoding and decoding complexity, measured in *operations per decoded bit*, for an encoder-decoder pair that achieves a decoded error probability of π or less at rate $(1-\epsilon)C$ or greater. We are interested in the behavior of $\chi_E(\epsilon,\pi)$, and especially $\chi_D(\epsilon,\pi)$, for a fixed value of π, as $\epsilon \to 0$.

It is not hard to use the classical results on the channel reliability exponent [2] to prove the following general result.

Theorem 1 *On any symmetric binary-input channel of capacity C, for any fixed $\pi > 0$, for the ensemble of binary linear codes of rate $R = C(1-\epsilon)$, with maximum-likelihood decoding, as $\epsilon \to 0$,*

$$\begin{aligned}\bar{\chi}_E(\epsilon,\pi) &= O(1/\epsilon^2)\\ \bar{\chi}_D(\epsilon,\pi) &= O(2^{1/\epsilon^2}).\end{aligned}$$

For the binary erasure channel, it is well known that we can say much more, since one can solve simultaneous linear equations for the erased positions.

Theorem 2 *On a binary erasure channel of capacity C, for any fixed $\pi > 0$, for the ensemble of linear codes of rate $R = C(1-\epsilon)$, with maximum-likelihood decoding, as $\epsilon \to 0$,*

$$\begin{aligned}\bar{\chi}_E(\epsilon,\pi) &= O(1/\epsilon^2)\\ \bar{\chi}_D(\epsilon,\pi) &= O(1/\epsilon^4).\end{aligned}$$

II. The New Results

The landmark work of Luby et al. [4], followed by the work in [5] and [6], established that the class of irregular low-density parity-check (ILDPC) codes can achieve channel capacity on the BEC with low complexity message-passing iterative (MPI) decoding. A closer look at ILDPC codes in fact establishes the following vast improvement on Theorem 2.

Theorem 3 (Shokrollahi [6]) *For the binary erasure channel, for the ensemble of irregular LDPC codes with MPI decoding,*

$$\lim_{\pi\to 0} \bar{\chi}_D(\epsilon,\pi) = O(\log 1/\epsilon).$$

Recently, we introduced the class of *irregular repeat-accumulate* (IRA) codes [1] [3], and this class too was shown to achieve channel capacity on the BEC. Extending these results, we can prove:

Theorem 4 *For the binary erasure channel, for the ensemble of IRA codes with MPI decoding,*

$$\lim_{\pi\to 0} \bar{\chi}_D(\epsilon,\pi) = O\left(\frac{1}{\epsilon}\log\frac{1}{\epsilon}\right).$$

A comparison of Theorems 3 and 4 suggests that for a given level of performance ILDPC codes are superior (in terms of decoding complexity) to IRA codes. In fact, a numerical study of IRA codes, which we cannot yet verify theoretically, suggests otherwise, and leads us to the following conjecture.

Conjecture 1 *For the binary erasure channel, for the ensemble of IRA codes with MPI decoding,*

$$\lim_{\pi\to 0} \bar{\chi}_D(\epsilon,\pi) = O(\log 1/\epsilon).$$

However, these complexity figures are in some sense misleadingly small because the number of iterations do not play a role in them. We have carried out an analysis of the number of iterations required, which leads us to the following conjecture.

Conjecture 2 *For any "typical" channel, for the ensemble of either ILDPC or IRA codes with MPI decoding,*

$$\bar{\chi}_D(\epsilon,\pi) = O\left(\log\frac{1}{\pi}\right) + O\left(\frac{1}{\epsilon}\log\frac{1}{\epsilon}\right).$$

References

[1] D. Divsalar, H. Jin, and R. J. McEliece, "Coding theorems for 'turbo-like' codes," pp. 201-210 in *Proc. 36th Allerton Conf. on Communication, Control, and Computing.* (Allerton, Illinois, Sept. 1998).

[2] R. G. Gallager, *Information Theory and Reliable Communication.* New York: John Wiley and Sons, 1968.

[3] H. Jin, A. Khandekar, and R. J. McEliece, "Irregular Repeat-Accumulate Codes," Proc. 2nd Int. Symp. Turbo Codes (Sept. 2000), pp. 1–8.

[4] M. Luby, M. Mitzenmacher, A. Shokrollahi, D. Spielman, and V. Stemann, "Practical loss-resilient codes," Proc. 29th ACM Symp. on the Theory of Computing (1997), pp. 150-159.

[5] M. Luby, M. Mitzenmacher, A. Shokrollahi, and D. Spielman, "Analysis of low-density codes and improved designs using irregular graphs," Proc. 30th ACM Symp. on the Theory of Computing (1998), pp. 249-258.

[6] M. A. Shokrollahi, "New sequences of linear time erasure codes approaching channel capacity," Proc. 1999 ISITA (Honolulu, Hawaii, November 1999) pp. 65–76.

0-7803-7123-2/01/$10.00 ©2001 IEEE