6-2003

More on the Reliability Function of the BSC

Alexander Barg

Rutgers University - New Brunswick/Piscataway, and Harvard University

Andrew McGregor

University of Pennsylvania, andrewm@cis.upenn.edu

Follow this and additional works at: https://repository.upenn.edu/cis_papers

Part of the [Computer Sciences Commons](#)

Recommended Citation

Alexander Barg and Andrew McGregor, "More on the Reliability Function of the BSC", . June 2003.

Suggested Citation:

Barg, A. and A. McGregor. (2003). "More on the reliability function of the BSC." *Proceedings of the International Symposium on Information Theory* Yokohama, Japan. June 29-July 4, 2003.

©2003 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.

This paper is posted at ScholarlyCommons. https://repository.upenn.edu/cis_papers/443
For more information, please contact repository@pobox.upenn.edu.

More on the Reliability Function of the BSC

Abstract

An improved upper bound is given for the maximum attainable exponent of the error probability of maximum likelihood decoding on a binary symmetric channel (the reliability function of the channel).

Disciplines

Computer Sciences | Physical Sciences and Mathematics

Comments

Suggested Citation:

Barg, A. and A. McGregor. (2003). "More on the reliability function of the BSC." *Proceedings of the International Symposium on Information Theory* Yokohama, Japan. June 29-July 4, 2003.

©2003 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.

More on the reliability function of the BSC

Alexander Barg
DIMACS, Rutgers U., and DEAS,
Harvard
e-mail: abarg@ieee.org

Andrew McGregor
University of Pennsylvania
200 South 33rd St.
Philadelphia, PA 19104
e-mail: andrewm@cis.upenn.edu

Abstract — An improved upper bound is given for the maximum attainable exponent of the error probability of max-likelihood decoding on a binary symmetric channel (the reliability function of the channel).

I. INTRODUCTION

Let $C(n, M = 2^{Rn}) \subset \{0, 1\}^n$ be a code of rate R used over a binary symmetric channel with crossover probability p . Denote by $P_e(C, p)$ the average error probability of maximum likelihood decoding of C . The best attainable exponent $E(R, p)$ of that probability (optimized over the choice of codes for a given channel) is called the *reliability function* of the channel. The best known lower bounds on $E(R, p)$ were derived by Elias and Gallager. In particular, for R between the critical rate of the channel $R_{\text{crit}} = \sqrt{p}/(\sqrt{p} + \sqrt{1-p})$ and the channel capacity $C = 1 - h(p)$ the function $E(R, p)$ is known exactly (here $h(p)$ is the binary entropy function).

Sequential improvements of the upper bounds on $E(R, p)$ for low rates were obtained in [2], [3], [4]. The purpose of this paper is to present a new, tighter upper bound on $E(R, p)$.

II. THE RESULTS

We will need the following notation:

$$G(\alpha, \tau) = 2 \frac{\alpha(1-\alpha) - \tau(1-\tau)}{1 + 2\sqrt{\tau(1-\tau)}}$$

$$h(\tau) = 1 - R - h(\alpha), \quad \delta_{\text{LP}}(R) := \min_{0 \leq \tau \leq \alpha \leq \frac{1}{2}} G(\alpha, \tau)$$

$$A(\omega) = \omega \log 2\sqrt{p(1-p)}.$$

The results of [1] and [3] for low rates can be stated as follows

$$-A(\delta_{\text{GV}}(R)) \leq E(R, p) \leq -A(\delta_{\text{LP}}(R)).$$

Recent improvements of error exponents for the BSC and the Gaussian channel [4, 5, 6] were obtained based on estimates of the distance distribution of an arbitrary code of a given rate R . Let $B_w, w = 0, 1, \dots, n$ be the average distance distribution of the code C . In [4] it is proved that for any family of codes of sufficiently large length n and rate R and any $\alpha \in [0, 1/2]$ there exists a value $0 \leq \omega \leq G(\alpha, \tau)$ such that

$$n^{-1} \log B_{\omega n} \geq \mu(R, \alpha, \omega) - o(1) \quad (1)$$

(the exact expression for μ is rather cumbersome and is omitted). We rely on the bound (1) together with a version of the estimation method of [6] to prove the following result.

Theorem 1

$$E(R, p) \leq -A(\delta_{\text{LP}}(R)) - R + 1 - h(\delta_{\text{LP}}(R)) \quad 0 \leq R \leq R_0^* \quad (2)$$

where R_0^* is a certain value of the code rate, depending on p . For $R \geq R_0^*$

$$E(R, p) \leq \max_{0 \leq \lambda \leq \delta_{\text{LP}}(R)} \max_{\lambda \leq \omega \leq \delta_{\text{LP}}(R)} B(\omega, \lambda) - A(\lambda) \quad (3)$$

where

$$B(\omega, \lambda) = -\omega - (1-\omega)h(p) + \max_{\eta \in [\frac{\lambda p}{2}, \min(\frac{\lambda}{2}, p(1-\omega))]} \left(\lambda h\left(\frac{2\eta}{\lambda}\right) + (\omega - \lambda/2)h\left(\frac{\omega - 2\eta}{2\omega - \lambda}\right) + (1 - \omega - \lambda/2)h\left(\frac{p(1-\omega) - \eta}{1 - \omega - \lambda/2}\right) \right).$$

Remarks 1. The bound (2) simply states that the error probability $P_e(C, p)$ for any code C of large length n cannot be smaller than the probability of incorrect decoding to a codeword at a distance $n\delta_{\text{LP}}$ from the transmitted codeword, multiplied by the number of such codewords in a random code.

2. An improvement of Theorem 1 over the results of [4] is in the range of code rates where the bound (2) can be claimed to be true. For instance, for $p = 0.01$ analysis of the results in [4] shows that (2) holds for $0 \leq R \leq 0.271$. Theorem 1 extends that range to $0 \leq R \leq R_0^* \approx 0.388$.

We can also apply the same estimation technique to codes with the binomial weight distribution: $B_w = \binom{n}{w} 2^{Rn-n}$. This question is of interest because almost all codes in the ensemble of all linear codes of rate R for large n have the weight distribution B_w . The result is as follows: there exists some value R_0^{**} , a function of p , such that for $R \leq R_0^{**}$ the lower bound on the error exponent of such a code coincides with the expurgation exponent $-A(\delta_{\text{GV}}(R))$. This complements the result of [7].

REFERENCES

- [1] R. G. Gallager, *Low-density parity-check codes*, MIT Press, Cambridge, MA, 1963.
- [2] C. E. Shannon, R. G. Gallager, and E. R. Berlekamp, "Lower bounds to error probability for codes on discrete memoryless channels, II", *Information and Control* **10** (1967), 522–552.
- [3] R. J. McEliece, E. R. Rodemich, H. Rumsey, and L. R. Welch, "New upper bound on the rate of a code via the Delsarte-MacWilliams inequalities," *IEEE Trans. Inform. Theory* **23** (1977), no. 2, 157–166.
- [4] S. Litsyn, "New upper bounds on error exponents," *IEEE Trans. Inform. Theory* **45** (1999), no. 2, 385–398.
- [5] A. Ashikhmin, A. Barg, and S. Litsyn, "A new upper bound on the reliability function of the Gaussian channel," *IEEE Trans. Inform. Theory* **46** (2000), no. 6, 1945–1961.
- [6] M. Burnashev, "On the relation between the code spectrum and the decoding error probability," *Problemy Peredachi Informatsii* **36** (2000), no. 4, 3–24.
- [7] R. G. Gallager, "The random coding bound is tight for the average code," *IEEE Trans. Inform. Theory* **19** (1973), no. 2, 244–246.