An Improved Upper Bound on the Block Coding Error Exponent for Binary Input Discrete Memoryless Channels

R. J. McEliece
Communications Systems Research Section

J. K. Omura
University of California at Los Angeles

For coded telemetry systems it is important to know the tradeoff between the error probability and the complexity of implementation. For systems using block codes, the block coding error exponent is a good way to estimate this tradeoff. In this article we show how the new upper bounds on the minimum distance of binary codes obtained by McEliece et al. result in improved upper bounds on the coding error exponents for binary input memoryless channels.

Consider a binary-input memoryless channel with input alphabet $A = \{0,1\}$ output alphabet B, and transition probabilities $\{p(y\,|\,x) : x \in A, y \in B\}$. Let $C = \{\mathbf{x}_1,\mathbf{x}_2 \cdots ,\mathbf{x}_M\}$ be a binary code of length n and rate $R = n^{-1} \log_2 M$ for this channel, and assume that each of the M codewords is sent with probability $1/M$. Let $d_{min}(C)$ denote the minimum Hamming distance between distinct codewords, and let $P_e(C)$ denote the probability of maximum-likelihood decoder error when the code C is used on the given channel.

Now define

$$\delta(n,R) = \frac{1}{n} \max d_{min}(C) \tag{1}$$

$$P_e(n,R) = \min P_e(C) \tag{2}$$

where the maximum and minimum in (1) and (2) are taken over the set of all codes of length n and rate $\geq R$. And finally define[1]

$$\delta(R) = \lim_{n \to \infty} \delta(n,R) \tag{3}$$

$$E(R) = \lim_{n \to \infty} - \log_2 P_e(n,R). \tag{4}$$

The maximum minimum distance $\delta(R)$ is unknown except at the points $R = 0, 1 : \delta(0) = 1/2, \delta(1) = 0$. The block coding error exponent $E(R)$ is known only for $R = 0$ and

[1]These limits are not known to exist. However, in what follows every upper bound is an upper bound on the corresponding lim sup's, and the lower bounds are lower bounds on the lim inf's, so there is no harm in pretending the limits exist.

$R \geq R_{crit}$, R_{crit} being a number to be defined below. We shall now briefly survey the known upper and lower bounds on $E(R)$, and indicate how the new upper bound $\delta^*(R)$ on $\delta(R)$ obtained in Ref. 1 can be used to improve the known upper bounds on $E(R)$ for small values of R.

First, the *sphere-packing* bound $E_{sp}(R)$ and the *random coding* bound $E_r(R)$, valid for all rates R less than channel capacity (Refs. 2, 3):

$$E_r(R) \leq E(R) \leq E_{sp}(R). \tag{5}$$

The two bounds in (5) are equal for sufficiently large R, and in fact the number R_{crit} cited above is the point where these two bounds meet. (Formulas for E_r and E_{sp} for binary symmetric and binary erasure channels are given in the Appendix.)

Next, we have bounds which depend on the *Bhattacharyya* parameter (Refs. 4, 5) for the channel, which is defined by

$$\alpha = -\ell\log_2 \sum_{y \epsilon b} (p(y|0)p(y|1))^{1/2}.$$

These bounds are

$$\alpha D \leq E(R) \leq \alpha\delta(R) \tag{6}$$

where $0 \leq D \leq 1/2$ is defined implicitly by $R = 1 - H_2(D)$, where $H_2(x)$ is the binary entropy function. (The lower bound in (6) is called the *expurgated* bound $E_{ex}(R)$; it is only valid for $0 \leq R \leq R'$, where R' is the rate at which the expurgated bound meets the random coding bound.) As mentioned, the function $\delta(R)$ is unknown, so the upper bound in (6) is ineffective. However, by using the bound $\delta(R) \leq \delta^*(R)$ obtained in Ref. 1 (for numerical values of $\delta^*(R)$, see Table 1 in Ref. 1), we obtain an upper bound

$$E(R) \leq \alpha\delta^*(R) \tag{7}$$

which can be evaluated, and which is already better than any previously known upper bound for small values of R.

Finally, Shannon et al. (Ref. 3) have shown that if $E_0(R)$ is any upper bound to $E(R)$, then so is the convex hull of the curves $E_0(R)$ and $E_{sp}(R)$. In particular, by taking $E_0(R) = (1/2)\alpha$ (from (6) and the fact that $\delta(0) = 1/2$), we see that $E(R)$ is bounded from above by the line passing through the point $(0,(1/2)\alpha)$ which is tangent to $E_{sp}(R)$. This bound is called the *straight-line* bound $E_{sl}(R)$. However by taking $E_0(R) = \alpha\delta^*(R)$ (cf. (7)) we can obtain an upper bound which is significantly better than $\min(E_{sl}(R), E_{sp}(R))$ for a considerable range of R's. We illustrate this in Fig. 1 with a binary symmetric channel with crossover probability $\epsilon = 0.01$, $\alpha = -\ell\log_2 \sqrt{4\epsilon(1-\epsilon)} = 2.329$, and in Fig. 2 with a binary erasure channel with erasure probability $\epsilon = 0.01$, $\alpha = -\ell\log_2 \epsilon = 6.644$. In both figures the unknown region for $0 \leq R \leq R_{crit}$ in which $E(R)$ lies is shaded. A final point worth mentioning is that the new upper bound (7) on $E(R)$ always matches the expurgated bound $E_{ex}(R)$ in slope at $R = 0$. (Both slopes are $-\infty$; this is well known for the expurgated bound, and follows for the bound (7) from the results of Ref. 1.) This fact supports the conjecture that $E(R) = E_{ex}(R)$ for $R \leq R_{crit}$ for binary input channels.

References

1. McEliece, R. J., Rodemich, E. R., Rumsey, H., Jr., and Welch, L. R., "New upper bounds on the rate of a code via the Delsarte–MacWilliams inequalities," *IEEE Trans. Inform. Theory*, Vol. IT-23, Mar. 1977 (in press).
2. Gallager, R. G., "A simple derivation of the coding theorem and some applications," *IEEE Trans. Inform. Theory*, Vol. IT-11, pp. 3–18, Jan. 1965.
3. Shannon, C. E., Gallager, R. G., and Berlekamp, E. R., "Lower bounds to error probability for coding on discrete memoryless channels," *Inform. Contr.*, Vol. 10, pp. 65–103 (Part I), pp. 522–552 (Part II), Jan. 1967.
4. Omura, J. K., "Expurgated bounds, Bhattacharyya distance, and rate distortion functions," *Inform. Contr.*, Vol. 24, pp. 358–383, Apr. 1974.
5. Omura, J. K, "On general Gilbert bounds," *IEEE Trans Inform. Theory*, Vol. IT-19, pp. 661–665, Sept. 1973.

Appendix

$E_r(R)$ and $E_{sp}(R)$ for Binary Symmetric and Binary Erasure Channels

For a binary symmetric channel with crossover probability ϵ, the random coding exponent is given by

$$E_r(R) = \begin{cases} 1 - R - \log_2(1 + \sqrt{4\epsilon(1-\epsilon)} & 0 \le R \le 1 - H_2(\sqrt{\epsilon}/(\sqrt{\epsilon} + \sqrt{1-\epsilon})) \\ T_\epsilon(D) - H_2(D) & 1 - H_2(\sqrt{\epsilon}/(\sqrt{\epsilon} + \sqrt{1-\epsilon})) \le R \le 1 - H_2(\epsilon) \end{cases}$$

where $T_\epsilon(D) = -D\log_2\epsilon - (1-D)\log_2(1-\epsilon)$, and D satisfies (7). The sphere packing exponent is

$$E_{sp}(R) = T_\epsilon(D) - H_2(D) \qquad 0 \le R \le 1 - H_2(\epsilon).$$

(Hence $R_{crit} = 1 - H_2(\sqrt{\epsilon}/(\sqrt{\epsilon} + \sqrt{1-\epsilon}))$ and $E(R) = E_r(R) = E_{sp}(R)$ for $R \ge R_{crit}$.) For the binary erasure channel with erasure probability ϵ:

$$E_r(R) = \begin{cases} 1 - R - \log_2(1+\epsilon) & 0 \le R \le 1 - 2\epsilon/(1+\epsilon) \\ E_{sp}(R) & 1 - 2\epsilon/(1+\epsilon) \le R \le 1 - \epsilon, \end{cases}$$

where

$$E_{sp}(R) = \frac{\rho\epsilon 2^\rho}{(1-\epsilon) + \epsilon 2^\rho} - \log_2((1-\epsilon) + \epsilon 2^\rho),$$

where ρ is determined by $R = 1 - \epsilon 2^\rho/(1 - \epsilon + \epsilon 2^\rho)$.

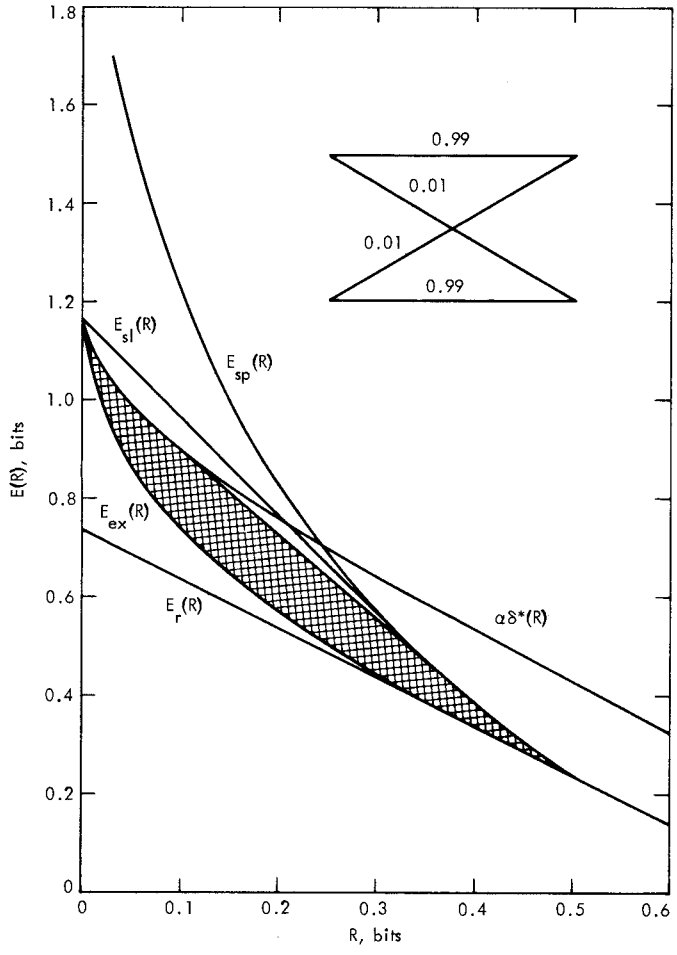

Fig. 1. A binary symmetric channel

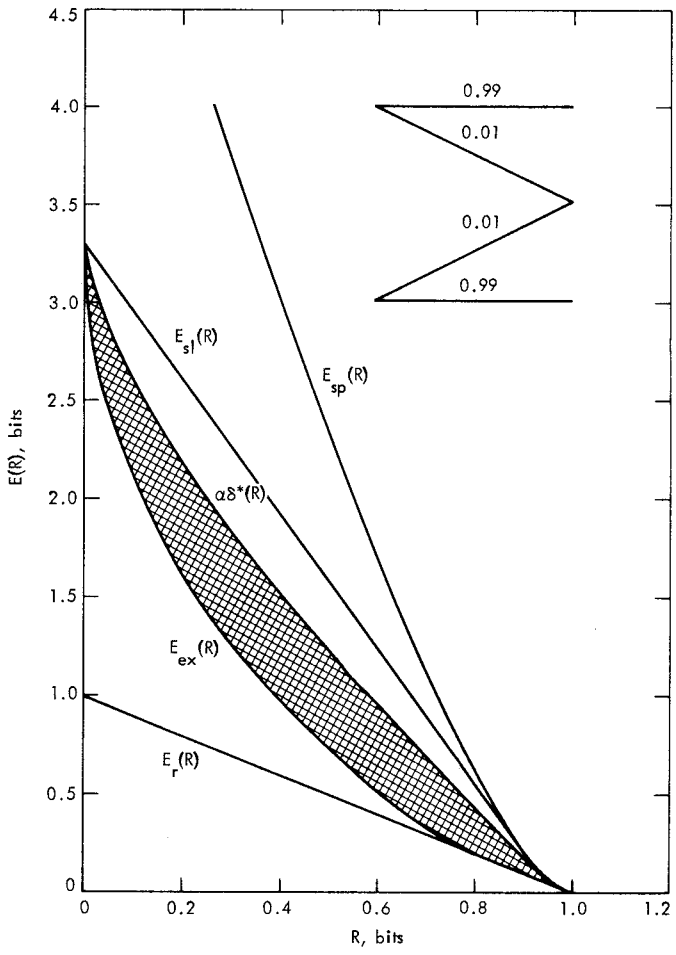

Fig. 2. A binary erasure channel