Exponential Error Bounds for Erasure, List, and Decision Feedback Schemes

G. DAVID FORNEY, JR., MEMBER, IEEE

Abstract—By an extension of Gallager's bounding methods, exponential error bounds applicable to coding schemes involving erasures, variable-size lists, and decision feedback are obtained. The bounds are everywhere the tightest known.

Introduction

ONE of the central problems of coding theory is the question of the error probability obtainable by coding on memoryless channels. Coding theory's first result, and still its most important, was Shannon's[1] proof that every memoryless channel has a capacity C, such that arbitrarily small error probabilities can be obtained if and only if the code rate R is less than C. Many years of continuing attempts to make more precise statements about error probabilities[2] culminated in Gallager's elegant derivation[3] of an exponential upper bound on attainable error probabilities, and in a nearly identical lower bound.[4]

The communication situation to which this work has been addressed is one in which the decoder makes a single "hard" decision about which code word was sent, the event of error being the event in which this decision, or estimate, is wrong. In the abstract, this is indeed the archetypical communications problem. However, experience with codes as part of larger systems indicates that it is often useful for the decoder to produce more than just an estimate alone. This paper contains results bearing on the two following situations.

1) The decoder has the option of not deciding at all, of rejecting all estimates. The resulting output is called an erasure. Only if the decoder does make an estimate, and it is wrong, do we have an undetected error.

2) The decoder has the option of putting out more than one estimate. The resulting output is called a list. Only if the correct code word is not on the list do we have a list error.

In the first case, it is clear that by allowing the erasure probability to increase, the undetected error probability can be reduced. In the second, by allowing the average list size to increase, the probability of list error can be reduced. Our results consist of exponential bounds *à la* Gallager[3] on the obtainable tradeoffs between these quantities; these bounds we believe to be quite tight.

In what follows, we shall first discuss at greater length the situations in which the erasure and list options may be useful. We shall then present the results themselves with geometrical and analytical interpretations of their character. Some of the less instructive proofs are relegated to the Appendix. Finally, we shall return to a consideration of the implications of these results in the communications situations now to be described.

Manuscript received April 3, 1967. This paper was presented at the 1967 International Symposium on Information Theory, San Remo, Italy. This work was supported by the Rome Air Development Center, Griffiss AFB, N. Y., under Contract AF30(602)-4071.

The author is with Codex Corporation, Watertown, Mass. 02172

Use of the Erasure and List Options

We now discuss circumstances in which the erasure and list options may be useful: when the transmitted data contains some redundancy, when a feedback channel is available, or when further stages of coding (concatenation) are contemplated.

A. Redundant Data

In the usual theoretical communications situation the incoming data are imagined to be completely random as, for example, a stream of independent bits each equally likely to be zero or one. In theory, if there were redundancy in the data, it could be removed by suitable source encoding. In practice, source encoding is frequently not considered worth the effort, and the communications system is given redundant data.

The erasure option is then useful whenever an erased code word can be reconstituted from knowledge of other code words. For example, in telemetry, each code word may contain samples from one or a number of sensors; if one code word is erased, the missing sensor readings can be interpolated from neighboring readings whenever the process being measured is not changing rapidly. Such redundancy may be called external redundancy.

On the other hand, the list option is useful whenever incorrect code words can be recognized by internal evidence. For example, in the transmission of English text, any incorrect code words on the list will generally look like garble and thus can be discarded. Such redundancy may be called internal redundancy.

With either internal or external redundancy, the list or erasure option therefore permits a considerable reduction in the probability of actual error, without reduction of the effective rate of information transfer, or equivalently an increase in rate, with no increase in error probability.

B. Feedback Channel

If the receiver has some way of signaling to the transmitter, the erasure option can be used in a simple strategy called decision feedback. Here an erasure results in a request for a repeat transmission, whereupon the transmitter

sends the same code word again. Although it has been shown[5] that feedback cannot increase the capacity of a memoryless channel, our results indicate that the error probability can be dramatically decreased for rates near capacity, without any sacrifice in the effective rate of information transfer. Furthermore, decision feedback is rather simple to implement, simpler in many cases than one-way transmission with ordinary decoding.

One could also use the occurrence of two or more code words on a list as a signal for repeat request but, in general, of the erasure criteria one could use, this will not be the optimum one. Another way of using lists would be in a kind of information feedback in which the transmitter would be made aware of the entries on the decoder's list, either by their direct transmission, or by feeding back what was actually received and letting the transmitter deduce by decoding what the decoder's list must be; the transmitter would then transmit only enough information to resolve the uncertainty. We shall see, however, that this additional complication fails to improve on the decision feedback error probability.

C. Concatenation

In concatenation[6] the code words of one code are used as symbols in a higher-order second-stage code. For example, on a binary-input channel, the basic code might be the (15, 5) Bose–Chaudhuri code, say, which has 32 code words. The second-stage code would then have symbols from the finite field with 32 elements, $GF(32)$, say, a (24, 46) Reed–Solomon code, which has minimum distance 9. Up to 4 decoding errors in 32 decodings of the (15, 5) code could then be corrected by the second-stage code. (This amounts to introduction of systematic external redundancy, rather than fortuitous, as mentioned earlier.) We have shown[6] that such a two-stage approach may yield the same performance as a single code, with less complexity.

If we allow the basic decoder an erasure option, then we generally reduce the number of decoding errors at the cost of introducing some decoding erasures. Algebraic erasure and error-correcting algorithms[7] can then be used to pick up the resulting erasures and errors. The resulting overall error probability is lower than that attainable with error correction alone, though in at least one interesting case[6] the improvement is small.

Additional improvements can be obtained, at the cost of increased complexity, by the use of a method called generalized minimum distance decoding.[8] Here the basic decoder puts out not an erasure or estimate alone, but an estimate with a reliability indicator, for which the optimum choice is the threshold for which the word would have been erased, had an erasure option been used. Therefore, our bounds give us information on this scheme as well.

Finally, if the basic decoder uses the list option, the second-stage decoder may in a number of trials attempt error correction with all the possibilities on all the lists. Obviously, if the average list size becomes large, the number of trials required becomes staggering; however, our results show that the average list size remains manageable for an interesting range of parameters.

Decision Regions and Optimum Criteria

We are concerned only with block codes on discrete memoryless channels; generalizations may be expected. A discrete memoryless channel has K inputs x_k, $1 \leq k \leq K$, and J outputs y_j, $1 \leq j \leq J$, and is characterized by its transition probability matrix $p_{jk} = \Pr(y_j \mid x_k)$, which gives the probability that y_j will be the output when x_k is the input. A block code of rate R (nats) and length N for such a channel consists of $M = \exp NR$ sequences $\mathbf{x}_m$ of N inputs x_{mi}, $1 \leq i \leq N$, called code words. A sequence of N outputs y_i is called a received word $\mathbf{y}$. The probability of receiving $\mathbf{y}$ given the transmission of $\mathbf{x}_m$ is then given by

$$\Pr(\mathbf{y} \mid \mathbf{x}_m) = \prod_{i=1}^{N} \Pr(y_i \mid x_{mi}), \tag{1}$$

where the product expression follows from the fact that successive probabilities are independent, which in turn follows by definition from the memorylessness of the channel.

Any of the decoding options we have described may be characterized in terms of decision regions R_m defined over the space of received words, which have the significance that the decoder puts out the code word $\mathbf{x}_m$ as an estimate if the received word $\mathbf{y}$ is in the region R_m. Fig. 1 is a schematic illustration of typical decision region configurations for ordinary decoding, decoding with an erasure option, and decoding with a list option. In the former case, the decision regions are disjoint and exhaust the space; each received word $\mathbf{y}$ is in one and only one region, so that the output is always a single estimate. With the erasure option, the regions remain disjoint, but not exhaustive; some received words therefore lie in no decision region and result in erasures. With the list option, the regions are no longer disjoint; a received word may lie in zero, one, or two or more decision regions, and thus may be decoded into a list of any size.

With ordinary decoding, an error occurs if $\mathbf{x}_m$ is sent and the received word lies in some decision region $R_{m'}$, where $m' \neq m$. The probability of error is therefore

$$\Pr(\mathcal{E}) = \sum_{m} \sum_{m' \neq m} \sum_{\mathbf{y} \in R_{m'}} \Pr(\mathbf{y}, \mathbf{x}_m), \tag{2}$$

where the sum over $(\mathbf{y} \in R_{m'})$ means over all $\mathbf{y}$ in $R_{m'}$. Since $\Pr(\mathbf{y}, \mathbf{x}_m) = \Pr(\mathbf{x}_m \mid \mathbf{y}) \Pr(\mathbf{y})$, the standard problem of choosing the decision regions R_m to minimize the probability of error $\Pr(\mathcal{E})$ is obviously solved by maximum a posteriori probability decoding, in which

$$\mathbf{y} \in R_m \text{ iff } \Pr(\mathbf{x}_m \mid \mathbf{y}) > \Pr(\mathbf{x}_{m'} \mid \mathbf{y}), \quad \text{all} \quad m' \neq m. \tag{3}$$

Any $\mathbf{y}$ for which two or more $\Pr(\mathbf{x}_m \mid \mathbf{y})$ tie for largest is a boundary point.

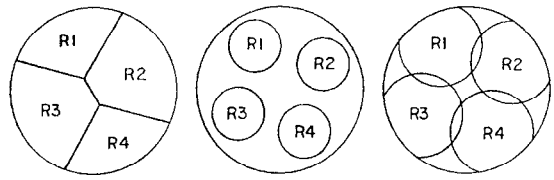

Fig. 1. Schematic representation of typical decision regions: (a) ordinary decoding, (b) erasure option, and (c) list option.

Equivalently, one can say that an error occurs if $\mathbf{y}$ lies in R_m and some code word $\mathbf{x}_{m'}$, $m' \neq m$, was actually transmitted. For our later convenience, we define this event as the event E_2; then

$$\Pr(E_2) = \sum_m \sum_{\mathbf{y} \in R_m} \sum_{m' \neq m} \Pr(\mathbf{y}, \mathbf{x}_{m'}). \tag{4}$$

Of course $\Pr(\mathcal{E}) = \Pr(E_2)$, the transformation between (2) and (4) being effected by a rearrangement of the order of summation and an interchange of the dummy variables m and m'.

When the erasure option is introduced, E_2 is the event of undetected error, so that (2) and (4) continue to give the undetected error probability. However, we must now contend with a nonzero erasure probability. Let us define the event E_1 as the event in which the received word $\mathbf{y}$ does not fall in the decision region R_m corresponding to the transmitted code word $\mathbf{x}_m$; the probability of E_1 is

$$\Pr(E_1) = \sum_m \sum_{\mathbf{y} \notin R_m} \Pr(\mathbf{y}, \mathbf{x}_m), \tag{5}$$

where the sum over $(\mathbf{y} \notin R_m)$ means over all $\mathbf{y}$ not in R_m. If E_1 occurs, either an undetected error or an erasure must ensue; therefore, the probability of an erasure X is simply

$$\Pr(X) = \Pr(E_1) - \Pr(\mathcal{E}). \tag{6}$$

As the probability of undetected error will normally be much less than the probability of erasure, $\Pr(E_1)$ is not only an upper bound but also an excellent approximation to $\Pr(X)$.

The question of how to choose the decision regions R_m so as to minimize $\Pr(E_1)$ for a given $\Pr(E_2)$, or vice versa, may be seen by comparison of (4) and (5) to be the standard decision theoretic one of minimizing one quantity within a region and another outside it. The solution would be given by the Neyman–Pearson theorem, except that one of the quantities is not a probability. We therefore in the Appendix trivially generalize the Neyman–Pearson theorem as follows.

Theorem 1

Let $f_0(y)$ and $f_1(y)$ be two non-negative functions defined on the discrete space Y, and define

$$\begin{aligned} P_0(R) &= \sum_{y \in R} f_0(y), \\ P_1(Y - R) &= \sum_{y \notin R} f_1(y), \end{aligned} \tag{7}$$

where R is any region of Y. Let R_1 then be the region containing all y such that

$$\frac{f_1(y)}{f_0(y)} \geq \eta, \tag{8}$$

and let R_2 be any other region such that

$$P_0(R_2) \leq P_0(R_1). \tag{9}$$

Then

$$P_1(Y - R_2) \geq P_1(Y - R_1). \tag{10}$$

Corollary: Let the decision regions R_m be defined by

$$\mathbf{y} \in R_m \text{ iff } \frac{\Pr(\mathbf{y}, \mathbf{x}_m)}{\sum_{m' \neq m} \Pr(\mathbf{y}, \mathbf{x}_{m'})} \geq \exp NT, \tag{11}$$

where N is the code length and T is an arbitrary parameter. Then there is no other set of decision regions which gives both a lower $\Pr(E_1)$ and a lower $\Pr(E_2)$ than this set does.

The proof of the corollary simply involves substituting $f_1(y) = \Pr(\mathbf{y}, \mathbf{x}_m)$ and $f_0(y) = \sum_{m' \neq m} \Pr(\mathbf{y}, \mathbf{x}_{m'})$ in (5) and (4), and using Theorem 1 for each m.

The corollary proves that the criterion (11) gives the optimum tradeoff between $\Pr(E_1)$ and $\Pr(E_2)$, or equivalently between $\Pr(\mathcal{E})$ and $\Pr(X)$ [since with $\Pr(\mathcal{E}) = \Pr(E_2)$ fixed, minimizing $\Pr(E_1)$ minimizes $\Pr(X)$]. The arbitrary parameter T governs the relative magnitudes of $\Pr(E_1)$ and $\Pr(E_2)$; clearly as T increases, $\Pr(E_1)$ increases while $\Pr(E_2)$ decreases, since the decision regions R_m shrink. We observe that in order for the decision regions to be necessarily disjoint T must be positive, for then (11) cannot be satisfied by more than one received word $\mathbf{y}$.

A suboptimum criterion of some practical utility comes from the observation that the probability $\Pr(\mathbf{y}, \mathbf{x}_{m2})$ of the second most likely code word $\mathbf{x}_{m2}$ is usually much larger than that of all the rest, excluding the first, so that the criterion

$$\mathbf{y} \in R_m \text{ iff } \frac{\Pr(\mathbf{y}, \mathbf{x}_m)}{\Pr(\mathbf{y}, \mathbf{x}_{m2})} \geq \exp NT \tag{11a}$$

is a fairly good approximation to (11) for erasure schemes.

Now let us consider the list option, where the decision regions overlap. The event of a list error is the event in which the transmitted code word is not on the list, or thus in which the received word $\mathbf{y}$ is not in the decision region R_m corresponding to the transmitted code word $\mathbf{x}_m$. But this is precisely the event E_1. On the other hand, the probability that some code word $\mathbf{x}_m$ will be on the list although some other code word $\mathbf{x}_{m'}$, $m' \neq m$, was sent, is

$$\Pr(\mathbf{x}_m \text{ on list and incorrect}) = \sum_{\mathbf{y} \in R_m} \sum_{m' \neq m} \Pr(\mathbf{y}, \mathbf{x}_{m'}). \tag{12}$$

The average number of incorrect words on the list $\bar{N}_I$ is then

$$\begin{aligned}\bar{N}_I &= \sum_m \Pr(\mathbf{x}_m \text{ on list and incorrect}) \\ &= \sum_m \sum_{\mathbf{y}\varepsilon R_m} \sum_{m'\neq m} \Pr(\mathbf{y}, \mathbf{x}_{m'}).\end{aligned} \tag{13}$$

We observe that if we extend the definition (4) of $\Pr(E_2)$ to include overlapping decision regions, where $\Pr(E_2)$ is no longer a probability, then $\bar{N}_I = \Pr(E_2)$. Therefore, the problem of choosing decision regions for the optimum tradeoff between list-error probability and average number of incorrect words on the list is identical to that already considered; again (11) is the optimum criterion. The distinction is that in order to obtain lists, T must be allowed to become negative. The list option and the erasure option are two sides of the same coin, the only difference being in the sign of T.

The likelihood ratio criterion of (11) is therefore the one to use both with erasures and lists. Since

$$\frac{\Pr(\mathbf{y}, \mathbf{x}_m)}{\sum_{m'\neq m} \Pr(\mathbf{y}, \mathbf{x}_{m'})} = \frac{\Pr(\mathbf{y}, \mathbf{x}_m)}{\Pr(\mathbf{y}) - \Pr(\mathbf{y}, \mathbf{x}_m)} = \frac{\Pr(\mathbf{x}_m \mid \mathbf{y})}{1 - \Pr(\mathbf{x}_m \mid \mathbf{y})}, \tag{14}$$

an equivalent criterion is

$$\mathbf{y} \varepsilon R_m \text{ iff } \Pr(\mathbf{x}_m \mid \mathbf{y}) \geq \eta, \tag{15}$$

where

$$\eta = \frac{\exp NT}{1 + \exp NT}. \tag{16}$$

The a posteriori probability is, therefore, an optimum erasure or list criterion. To recapitulate, in ordinary decoding, guess that code word $\mathbf{x}_m$ for which $\Pr(\mathbf{x}_m \mid \mathbf{y})$ is greatest. With the erasure option, guess that code word $\mathbf{x}_m$ for which $\Pr(\mathbf{x}_m \mid \mathbf{y})$ is greatest, as long as $\Pr(\mathbf{x}_m \mid \mathbf{y}) \geq \eta$, $\eta \geq \frac{1}{2}$; otherwise erase. With list decoding, to minimize the average list size (the average number of incorrect words on the list plus one) for a given list-error probability, put on the list all code words $\mathbf{x}_m$ for which $\Pr(\mathbf{x}_m \mid \mathbf{y}) \geq \eta$, $\eta < \frac{1}{2}$.

Review of Gallager's Results

For ordinary decoding, Gallager[3] has proved that there exists a block code of length N and rate R nats such that with maximum a posteriori probability decoding the error probability is bounded by

$$\Pr(\varepsilon) < \exp[-NE(R)], \tag{17}$$

where $E(R)$, the error exponent, is given at high rates by

$$\begin{aligned}E(R) &= \max_{0\leq\rho\leq 1, \mathbf{p}} E_0(\rho, \mathbf{p}) - \rho R, \\ E_0(\rho, \mathbf{p}) &= -\ln \sum_j \Big[\sum_k p_k p_{jk}^{1/1+\rho}\Big]^{1+\rho},\end{aligned} \tag{18}$$

where $\mathbf{p}$ is any vector of input probabilities p_k. At low rates $E(R)$ is given by the "expurgated" exponent

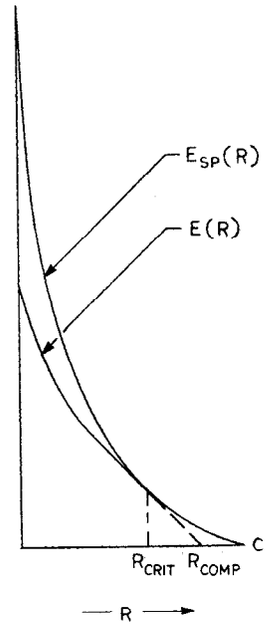

Fig. 2. Ordinary error and sphere-packing exponents.

$$\begin{aligned}E(R) &= \max_{\rho\geq 1, \mathbf{p}} E_x(\rho, \mathbf{p}) - \rho R, \\ E_x(\rho, \mathbf{p}) &= -\rho \ln \sum_k \sum_{k'} p_k p_{k'} \Big[\sum_j p_{jk}^{1/2} p_{jk'}^{1/2}\Big]^{1/\rho}.\end{aligned} \tag{19}$$

We note that

$$E_0(1, \mathbf{p}) = E_x(1, \mathbf{p}); \tag{20}$$

at intermediate rates, therefore, $E(R)$ is given by the straight line

$$\begin{aligned}E(R) &= R_{\text{comp}} - R, \\ R_{\text{comp}} &= \max_{\mathbf{p}} E_0(1, \mathbf{p}),\end{aligned} \tag{21}$$

where R_{comp} is the limiting computational cutoff rate of sequential decoding.[9] These bounds are known[4] to be exponentially tight at zero rate, and at all rates for which $E(R)$ equals the sphere-packing exponent

$$E_{sp}(R) = \max_{\rho\geq 0, \mathbf{p}} E_0(\rho, \mathbf{p}) - \rho R, \tag{22}$$

which, in general, will be at all rates between some critical rate R_{crit} and capacity C.

Fig. 2 depicts $E(R)$ and $E_{sp}(R)$ for a typical case, that of a binary symmetric channel with crossover probability $p = 0.01$.

The Bounds

In the Appendix, we show that similar, two-parameter exponential error bounds govern the quantities $\Pr(E_1)$ and $\Pr(E_2)$, which we recall are the erasure and undetected-error probabilities for erasure schemes, or the list-error probability and average number of incorrect words on the list for list schemes. These bounds are given by Theorem 2.

Theorem 2

There is a block code of length N and rate R nats such that when the likelihood ratio criterion of (11) is used with a threshold T, one can simultaneously obtain

$$\Pr(E_1) < \exp[-NE_1(R, T)],$$
$$\Pr(E_2) < \exp[-NE_2(R, T)], \tag{23}$$

where $\Pr(E_1)$ and $\Pr(E_2)$ are given by (5) and (4), $E_1(R, T)$ is given at high rates by

$$E_1(R, T) = \max_{0\le s\le\rho\le 1, \mathbf{p}} E_0(s, \rho, \mathbf{p}) - \rho R - sT,$$
$$E_0(s, \rho, \mathbf{p}) = -\ln \sum_j \Big[\sum_k p_k p_{jk}^{1-s}\Big] \Big[\sum_{k'} p_{k'} p_{jk'}^{s/\rho}\Big]^{\rho}, \tag{24}$$

and at low rates by

$$E_1(R, T) = \max_{0\le s\le 1, \rho\ge 1, \mathbf{p}} E_x(s, \rho, \mathbf{p}) - \rho R - sT,$$
$$E_x(s, \rho, \mathbf{p}) = -\rho \ln \sum_k \sum_{k'} p_k p_{k'} \Big[\sum_j p_{jk}^{1-s} p_{jk'}^{s}\Big]^{1/\rho}, \tag{25}$$

and $E_2(R, T)$ is given by

$$E_2(R, T) = E_1(R, T) + T. \tag{26}$$

As with the ordinary error exponent, we note that

$$E_0(s, 1, \mathbf{p}) = E_x(s, 1, \mathbf{p}), \tag{27}$$

so that for fixed T the two bounds are joined at intermediate rates by a straight line of slope -1.

Properties of the Bounds

We can easily show that when $T = 0$ the optimum value of s is $\rho/(1 + \rho)$ in $E_0(s, \rho, \mathbf{p})$ and $\frac{1}{2}$ in $E_x(s, \rho, \mathbf{p})$. With these substitutions our exponents reduce to Gallager's ordinary error exponent $E(R)$, as one would hope. Actually, our result is a bit stronger, in that the error exponent $E(R)$ has been shown to be attainable not only with maximum a posteriori probability decoding (or, since all code words are assumed equally likely in the proof, maximum likelihood decoding, i.e., choose $\mathbf{x}_m$ if $\Pr(\mathbf{y} \mid \mathbf{x}_m) > \Pr(\mathbf{y} \mid \mathbf{x}_{m'})$, all $m' \neq m$), but also with a slightly weaker erasure-type decoding (choose $\mathbf{x}_m$ if $\Pr(\mathbf{y} \mid \mathbf{x}_m) \ge \sum_{m'\neq m} \Pr(\mathbf{y} \mid \mathbf{x}_{m'})$; otherwise erase). However, the stronger result is also obtained easily with a small change in Gallager's derivation.

A lower bound to these exponents, which is a good approximation for T near zero, comes from leaving s at the value which is optimum for $T = 0$; at high rates

$$E_1(R, T) = \max_{0\le s\le\rho\le 1, \mathbf{p}} E_0(s, \rho, \mathbf{p}) - \rho R - sT$$
$$\ge \max_{0\le\rho\le 1, \mathbf{p}} E_0\Big(\frac{\rho}{1+\rho}, \rho, \mathbf{p}\Big) - \rho R - \frac{\rho}{1+\rho} T$$
$$= E(R) - \frac{\rho}{1+\rho} T;$$

$$E_2(R, T) \ge E(R) + \frac{1}{1+\rho} T. \tag{28}$$

Similarly, at low rates,

$$E_1(R, T) \ge E(R) - \tfrac{1}{2}T;$$
$$E_2(R, T) \ge E(R) + \tfrac{1}{2}T. \tag{29}$$

These results had been proved earlier[6] by a variation in Gallager's derivation. They show that as T increases, $E_2(R, T)$ (the undetected-error exponent) increases at least as fast as $E_1(R, T)$ (the erasure exponent) decreases, which implies that if we permit the erasure probability to increase by a factor of 10, say, the undetected-error probability will decrease by more than a factor of 10. Since ρ goes to zero as R approaches the capacity C, we see that the tradeoff is expecially favorable for rates near capacity. Conversely, at least for small T, the list error exponent increases more slowly than the average incorrect list-size exponent decreases as T decreases below zero, with the tradeoff being especially unfavorable near capacity.

In the Appendix, we derive sharper bounds on the achievable tradeoff between the exponents given by (24) and (26) in the high-rate region. These bounds are expressed in terms of the fixed-$\mathbf{p}$ sphere-packing exponent $E_{sp}(R, \mathbf{p})$, defined as

$$E_{sp}(R, \mathbf{p}) = \max_{\rho\ge 0} E_0(\rho, \mathbf{p}) - \rho R. \tag{30}$$

For many channel models commonly used, there will be a single optimum $\mathbf{p}$ for all R; for this $\mathbf{p}$, $E_{sp}(R, \mathbf{p})$ equals the sphere-packing exponent $E_{sp}(R)$ of (22), and the latter may be used in the bound. Unfortunately, this is not the case for all channels. Also, if $R(\rho, \mathbf{p})$ is the rate at which $E_{sp}(R, \mathbf{p})$ has slope $-\rho$ [the rate for which ρ is optimum in (30)], then we define the conjugate rate $\bar{R}$ of $R(\rho, \mathbf{p})$ to be $R(1/\rho, \mathbf{p})$. We then have the following theorem.

Theorem 3

For any $\mathbf{p}$ and any R' greater than the conjugate rate $\bar{R}$ of R and less than $R(0, \mathbf{p})$, there is a threshold T such that

$$E_1(R, T) = E_{sp}(R', \mathbf{p}),$$
$$E_2(R, T) \ge E_{sp}(R, \mathbf{p}) - R + R'. \tag{31}$$

The proof of Theorem 3 shows that equality holds when the quantity

$$q_j(x) = \sum_k p_k p_{jk}^{x} \tag{32}$$

is independent of j. In particular this is true for channels symmetric from input and output, such as the binary symmetric channel, where the $\mathbf{p}$ is the optimum equiprobable input distribution. Of course, for this $\mathbf{p}$ $E_{sp}(R, \mathbf{p}) = E_{sp}(R)$. For such totally symmetric channels, we therefore have Theorem 3(a).

Theorem 3(a)

For totally symmetric channels, there is a threshold T such that for any rate R' greater than the conjugate rate $\tilde{R}$ of R and less than C,

$$E_1(R, T) = E_{sp}(R'),$$
$$E_2(R, T) = E_{sp}(R) - R + R'. \tag{33}$$

Theorem 3 suggests the following construction. Draw the sphere-packing exponent $E_{sp}(R', \mathbf{p})$, and through it draw a straight line of slope $+1$ intersecting $E_{sp}(R', \mathbf{p})$ at the rate R. Then as we vary R' in the range $\tilde{R} \leq R' \leq R(0, \mathbf{p})$, the two curves bound the obtainable tradeoff between $E_1(R, T)$ and $E_2(R, T)$. Fig. 3 illustrates this construction with the sphere-packing exponent of the binary symmetric channel of Fig. 2. The construction is performed for two rates conjugate to one another.

The following heuristic picture may help to understand Theorem 3. Suppose that we had a code of rate R' that was effectively sphere-packed, with error exponent $E_{sp}(R')$. Suppose further that it were possible to use a subset of words in the code as an effectively sphere-packed code of rate $R < R'$. Then if the decision regions belonging to the original code continued to be used for the new code, the erasure probability would continue to be exp $[-NE_{sp}(R')]$. An error could not be made, however, unless the received word were outside the new code's proper sphere, an event of probability exp $[-NE_{sp}(R)]$. Even in the latter event, no error would occur unless the received word fell in some other decision region. But the percentage of the total space covered by decision regions proper to code words in the new code is the ratio of the number of words in the new code to those in the original, or exp $[-N(R' - R)]$. Assuming that this is indeed approximately the probability of error, given that the received word falls outside the correct exclusive sphere, we would arrive at an undetected-error probability of exp $\{-N[E_{sp}(R) - R + R']\}$.

We obtain similar results for the very noisy channel, defined as any channel with transition probability matrix

$$p_{jk} = (1 + \epsilon_{jk})q_j, \tag{34}$$

where $\epsilon_{jk} \ll 1$ for all j and k. To second order in the ϵ_{jk}, the capacity of the very noisy channel is[10]

$$C = \max_{\mathbf{p}} \tfrac{1}{2} \sum_j q_j [\sum_k p_k \epsilon_{jk}^2 - (\sum_k p_k \epsilon_{jk})^2]. \tag{35}$$

By substitution of (34) into (24) and (25), we find that for the optimum $\mathbf{p}$ and to second order in the ϵ_{jk},

$$E_0(s, \rho) = \left(2s - s^2 - \frac{s^2}{\rho}\right) C,$$
$$E_x(s, \rho) = (2s - 2s^2)C. \tag{36}$$

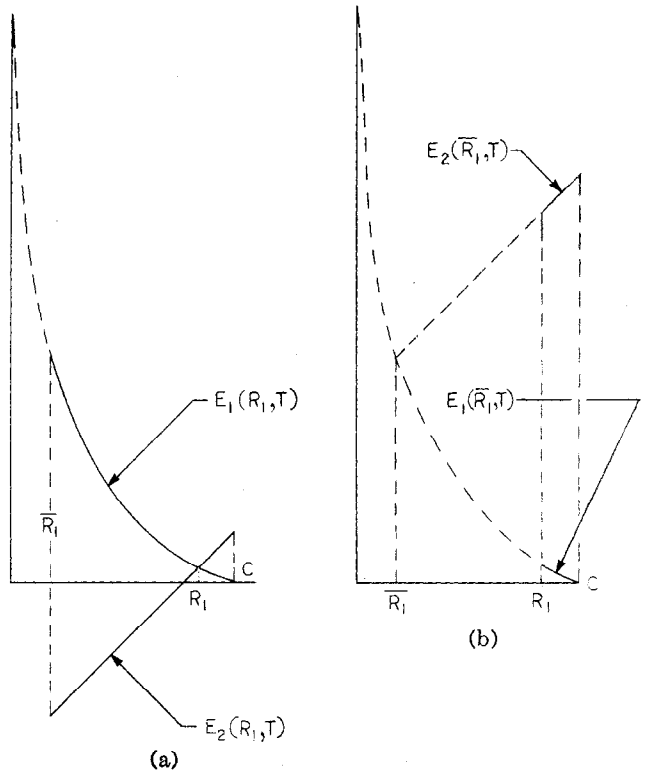

Fig. 3. Construction of exponents E_1 and E_2 from sphere-packing exponents in high-rate region for two conjugate rates R_1 and $\tilde{R}_1$.

We see immediately that the expurgated exponent is of no use, since $E_x(s, \rho) = E_x(s, 1) = E_0(s, 1)$. In the high-rate region, we obtain the parametric equations

$$R(s, \rho) = \frac{\partial E_0}{\partial \rho} = \frac{s^2}{\rho^2} C,$$
$$T(s, \rho) = \frac{\partial E_0}{\partial s} = \left[2 - 2s - \frac{2s}{\rho}\right] C,$$
$$E_1(s, \rho) = s^2 C, \tag{37}$$
$$E_2(s, \rho) = \left[s^2 - 2s + 2 - \frac{2s}{\rho}\right] C.$$

The sphere-packing bound is obtained in parametric form from the substitution $s = \rho/(1 + \rho)$

$$E_{sp}(\rho) = \left(\frac{\rho}{1 + \rho}\right)^2 C,$$
$$R(\rho) = \left(\frac{1}{1 + \rho}\right)^2 C. \tag{38}$$

We can therefore write

$$E_1(s, \rho) = E_{sp}\left(\frac{s}{1 - s}\right),$$
$$E_2(s, \rho) = E_{sp}\left(\frac{\rho - s}{s}\right) - R\left(\frac{\rho - s}{s}\right) + R\left(\frac{s}{1 - s}\right), \tag{39}$$
$$R(s, \rho) = R\left(\frac{\rho - s}{s}\right).$$

It follows that, despite the fact that the very noisy channel may not be symmetric, we nonetheless obtain the expressions of Theorem 3(a) for the high-rate exponents in terms of the sphere-packing exponents.

Outside the high-rate region, the optimum value for ρ is 1, and we obtain the semiparametric expressions

$$\begin{aligned} T(s) &= 2(1 - 2s)C, \\ E_1(s, R) &= 2s^2C - R, \\ E_2(s, R) &= 2(1 - s)^2C - R. \end{aligned} \tag{40}$$

We see that an interchange between s and $(1 - s)$ reverses the sign of T while switching the values of E_1 and E_2, so that wherever these expressions apply, the exponents in the erasure and list regions are mirror images of one another. This result can be shown to hold in general in the expurgated region, from the symmetric appearance of s and $(1 - s)$ in (25).

There are some methods more general than that of Fig. 3 for displaying exponents; we now use the very noisy channel to illustrate them because of the particularly simple exponent expressions which apply. Basically, the exponent $E_1(R, T)$ is simply a surface in three dimensions. Fig. 4(a) displays $E_1(R, T)$, the erasure exponent, for $T \geq 0$, and $E_2(R, T)$, the average incorrect list-size exponent, for $T \leq 0$; the complementary exponents must be imagined by adding the magnitude of T to the illustrated exponent. The exponents are shown in the list region only for $E_2(R, T) \geq 0$, though of course the average incorrect list size exponent may validly go negative.

Since T is not a basic coding parameter, we can alternatively solve for T and obtain a surface in the three dimensions R, E_1, and E_2, thus giving the attainable tradeoff between the two exponents E_1 and E_2 directly for every R. Fig. 4(b) illustrates this approach.

We might mention one last way of expressing these relationships which seems to add nothing but a certain symmetry. It could be called a thermodynamic approach, since it involves defining a state function

$$E_0'(\lambda, s', \rho', \mathbf{p}) = \lambda E_0\left(\frac{s'}{\lambda}, \frac{\rho'}{\lambda}, \mathbf{p}\right) \tag{41}$$

from which all the significant variables can be determined by partial differentiation:

$$R = \frac{\partial E_0'}{\partial \rho'}, \quad T = \frac{\partial E_0'}{\partial s'}, \quad E = \frac{\partial E_0'}{\partial \lambda}. \tag{42}$$

We have yet to find any use for this curiosity.

Finally, we wish to mention a class of channels for which the exponents assume very different form. This class consists of all channels with transition probability matrix satisfying

$$p_{jk} = \beta_j \, \delta_{jk}, \tag{43}$$

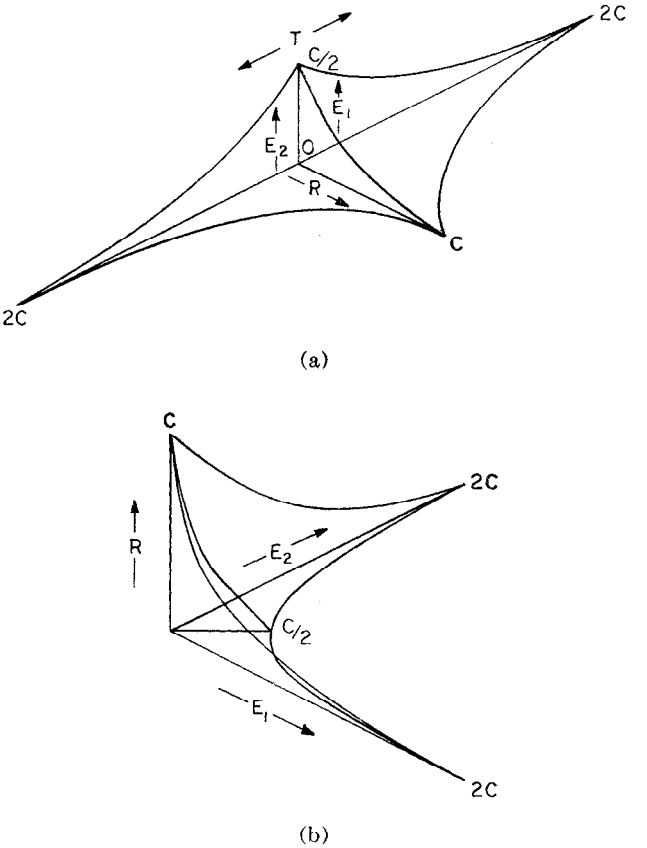

Fig. 4. Very noisy channel exponents.

where δ_{jk} equals either zero or one. We call these channels erasure-type channels, since their archetype is the binary erasure channel, for which the erasure output has $\beta_j = p$, the erasure probability, with δ_{jk} equal to one for both inputs x_k; while for the other two outputs only one δ_{jk} equals one and $\beta_j = 1 - p$. In the erasure-type channel, the occurrence of an output y_j rules out all code words which have in that position any input x_k such that $\delta_{jk} = 0$, but in no way discriminates between the remaining code words. Decoding with such a channel is then a sieve-like process, in which each output allows the discard of a certain percentage of the code words previously under consideration. After N outputs, either only one code word will be left, in which case that will be the correct one, or there will be a list of several, with no basis for choosing between them.

When we substitute (43) into (24) and (25) to obtain exponents for erasure-type channels, we find that

$$\begin{aligned} E_0(s, \rho, \mathbf{p}) &= -\ln \sum_j \left[\sum_k p_k \delta_{jk}\right]^{1+\rho}, \\ E_x(s, \rho, \mathbf{p}) &= -\rho \ln \sum_k \sum_{k'} p_k p_{k'} \left[\sum_j \beta_j \delta_{jk} \delta_{jk'}\right]^{1/\rho}. \end{aligned} \tag{44}$$

The salient observation to be made is that neither of these expressions depends on s. Therefore, for $T > 0$, the optimum s is the smallest one, $s = 0$, while for $T < 0$, the optimum s is the largest one, $s = \rho$ or $s = 1$ as the

case may be, and thus

$$E_1(R, T) = \max_{0 \le s \le \rho \le 1, \mathbf{p}} E_0(s, \rho, \mathbf{p}) - \rho R - sT$$
$$= \max_{0 \le \rho \le 1, \mathbf{p}} E_0(\rho, \mathbf{p}) - \rho R \qquad (45)$$
$$= E(R), \quad T \ge 0 \quad \text{and} \quad R \ge R_{crit}.$$

Similarly,

$$E_1(R, T) = E(R), \quad T \ge 0 \quad \text{and} \quad R \le R_{crit}. \qquad (46)$$

Thus by increasing T, the undetected-error exponent $E_2(R, T) = E_1(R, T) + T$ can be made as small as desired, without affecting the erasure exponent $E_1(R, T)$, which is simply the ordinary error exponent $E(R)$.

In the list region,

$$E_2(R, T) = \max_{0 \le \rho \le 1, \mathbf{p}} E_0(\rho, \mathbf{p}) - \rho(R + T) + T$$
$$= \begin{cases} E(R + T) + T, & T \le 0 \quad \text{and} \quad R + T \ge R_{crit}, \\ R_{crit} - R, & T \le 0 \quad \text{and} \quad R_{crit} \le R \le R_{crit} - T, \\ E(R), & T \le 0 \quad \text{and} \quad R \le R_{crit}. \end{cases} \qquad (47)$$

The typical appearance of these curves is illustrated in Fig. 5.

A plausible interpretation of this result is readily found. In the erasure region, by letting T become infinite, we can get an undetected-error probability of zero, while the erasure probability remains the same as the ordinary error probability. The explanation is that all ordinary decoding errors are detectable as erasures, since they correspond to decoded lists of size greater than one. On the list side, the average incorrect list size is equal to the erasure probability for rates below R_{crit}, which says that when decoded lists do occur they are small, with size increasing less than exponentially with N. At higher rates, given that a decoded list does occur, the average list size increases exponentially with N; in general, the average list size, given a list, seems to go as $\exp N[R - R_{comp} + E(R)]$.

Implications for Decision Feedback

One of the most interesting applications of our bounds is the determination of the performance attainable with decision feedback. We recall that when a feedback channel is available, each erasure triggers a request for repeat of a code word. If the erasure probability is $\Pr(X)$, then the probability that a code word will be repeated i or more times is $[\Pr(X)]^i$, and the average number of times a code word is repeated is

$$1 + \Pr(X) + [\Pr(X)]^2 + \cdots = \frac{1}{1 - \Pr(X)}. \qquad (48)$$

Therefore, if the code rate is R, the effective rate of information transfer is reduced to

$$R[1 - \Pr(X)]. \qquad (49)$$

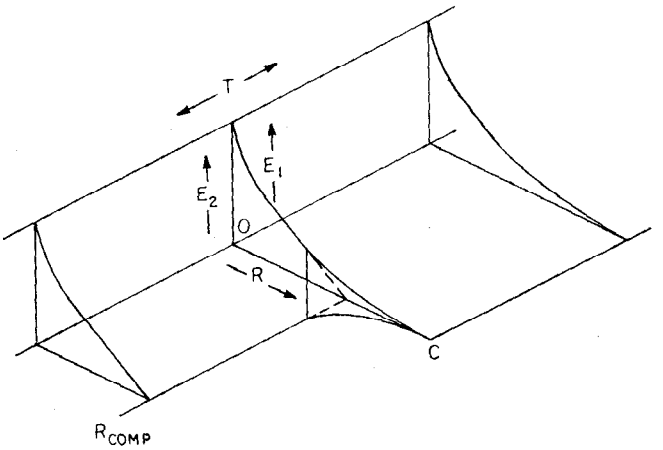

Fig. 5. Exponents for erasure-type channels.

Clearly, for any T such that $E_1(R, T) > 0$, the effective rate of information transfer can be made as close to R as desired by increasing N, since

$$\Pr(X) < \exp[-NE_1(R, T)]. \qquad (50)$$

Meanwhile, the undetected-error probability per code word is bounded by

$$\Pr(\varepsilon) < \exp[-NE_2(R, T)]. \qquad (51)$$

These considerations lead to the definition of the feedback exponent $E_f(R)$ as the limiting value of $E_2(R, T)$ as $E_1(R, T)$ approaches zero. This value is determined by solving for T in (24) and (26), obtaining

$$E_2 = \max_{0 \le s \le \rho \le 1, \mathbf{p}} \frac{1}{s} E_0(s, \rho, \mathbf{p}) - \frac{\rho}{s} R - \frac{1 - s}{s} E_1. \qquad (52)$$

As E_1 approaches zero, this maximum is attained for fixed R by letting s and ρ both go to zero at the constant ratio $\rho/s = \nu \ge 1$. Since $E_0(s, \rho, \mathbf{p})$ also goes to zero as this happens, we must use L' Hôpital's rule

$$\lim_{s \to 0} \frac{1}{s} E_0(s, \rho, \mathbf{p})$$
$$= \frac{\partial}{\partial s} E_0(s, \nu s, \mathbf{p}) \Big|_{s=0}$$
$$= \sum_i \sum_k p_k p_{ik} [\ln p_{ik} - \ln (\sum_{k'} p_{k'} p_{ik'}^{1/\nu})^\nu] \qquad (53)$$
$$= E_{0f}(\nu, \mathbf{p}),$$

where the last step defines $E_{0f}(\nu, \mathbf{p})$. Then by substitution in (52)

$$E_f(R) = \max_{\nu \ge 1, \mathbf{p}} E_{0f}(\nu, \mathbf{p}) - \nu R. \qquad (54)$$

A careful examination shows that all limits are approached continuously and with continuous derivatives, so that

if $E_2(R, T) = E_f(R) - \delta$, then $E_1(R, T) > 0$ with strict inequality. One can then make a statement of the following type. For any ϵ and δ greater than zero there exists an N such that there is a decision-feedback scheme involving a block code of length N and rate R nats in which the effective rate of information transfer exceeds $R(1 - \epsilon)$, while the probability of error is bounded by

$$\Pr(\mathcal{E}) < \exp\{-N[E_f(R) - \delta]\}. \tag{55}$$

We observe that while the feedback exponent $E_f(R)$ approaches zero as R approaches capacity, as it must, it approaches 0 with a slope of -1, in contrast to the ordinary error exponent $E(R)$, whose slope is generally zero at capacity. This implies that the ratio of the feedback exponent $E_f(R)$ to the ordinary error exponent $E(R)$ becomes infinite as the rate approaches capacity, or, in other words, that near capacity the achievement of low error probabilities is dramatically simplified by decision feedback.

For the totally symmetric and very noisy channels discussed earlier, the feedback exponent may be found at all rates by allowing the R' of Theorem 3(a) to approach C; then $E_{sp}(R')$ goes to zero, and

$$E_f(R) = E_{sp}(R) - R + C, \; C_{0,sp} \leq R \leq C, \tag{56}$$

where $C_{0,sp} = R(\infty)$ is the rate at which the sphere-packing bound becomes infinite. This is a large exponent, even in comparison to the sphere-packing bound, which is the true ordinary error exponent only at high rates. Moreover, by Theorem 3 we see that for any channel, if we choose $\mathbf{p}$ as the distribution which gives $R(0, \mathbf{p}) = C$, then

$$E_f(R) \geq E_{sp}(R, \mathbf{p}) - R + C, \qquad R(\infty, \mathbf{p}) \leq R \leq C. \tag{57}$$

Viterbi and Gallager had shown earlier in unpublished work that $E_f(R) \geq C - R$.

As an example of a case in which the bound of (57) is exceeded, we might cite the erasure-type channels; from Fig. 5 it is clear that $E_f(R)$ is infinite at all rates less than C. In other words, if repeats are demanded whenever ambiguity in decoding remains, any rate less than capacity can be maintained with no errors. In fact, on the binary erasure channel, where $C = 1 - p$ (p being the erasure probability), we can achieve this performance with codes of block length one, simply by asking for a repeat whenever a bit is erased.

For any channel with at least one transition probability equal to zero, there may be a rate greater than zero for which $E_f(R)$ becomes infinite. We call such a rate the feedback zero-error capacity $C_{0,f}$. From these results, $C_{0,f} \leq C$, with equality for erasure-type channels. $C_{0,f}$ must be the limit of $\nu^{-1}E_{0f}(\nu, \mathbf{p})$ as ν becomes large, for then $E_f(R)$ becomes $\nu(C_{0,f} - R)$ for large ν, and in the limit infinite if $R < C_{0,f}$. Again L'Hôpital's rule is required:

$$\begin{aligned} C_{0,f} &= \max_{\mathbf{p}} \frac{\partial}{\partial \nu} E_{0f}(\nu, \mathbf{p}) \Big|_{\nu=\infty} \\ &= \max_{\mathbf{p}} \Big[- \sum_j q_j \ln q_j(0) \Big], \end{aligned} \tag{58}$$

where

$$\begin{aligned} q_j &= q_j(1) = \sum_k p_k p_{jk}, \\ q_j(0) &= \sum_k p_k \theta_{jk}, \\ \theta_{jk} &= \begin{cases} 0, & \text{if } p_{jk} = 0, \\ 1, & \text{otherwise.} \end{cases} \end{aligned} \tag{59}$$

This result may be obtained directly by the following argument. Let us consider the following method of communicating a single one of exp NR messages. First a code word of length N is chosen by picking each letter independently and with probability p_k of being x_k. This represents the correct message, and is transmitted, resulting in the received word $\mathbf{y} = [y_{j(1)}, y_{j(2)}, \cdots, y_{j(N)}]$. The probability of the output y_j occurring in any position in the received word is the q_j of (59), independently of what appears in all other positions. Now the other exp $NR - 1$ code words are chosen, exactly as the correct one was.

To ensure zero-error probability, a sieve-like decoding procedure is necessary, as with erasure-type channels. Each occurrence of the output y_j justifies the discard of all code words which in that position have any letter x_k such that $p_{jk} = 0$; all others must be retained. Given a received output y_j, therefore, the probability that any code word other than the one transmitted will be consistent with y_j is the $q_j(0)$ defined by (59). Given a whole received word $\mathbf{y}$, the probability of retaining a particular incorrect word is then

$$p_r(\mathbf{y}) = \prod_{i=1}^{N} q_{j(i)}(0). \tag{60}$$

If $p_r(\mathbf{y})$ is less than exp $(-NR)$, then chances are that all the incorrect code words will be discarded, with probability approaching one as N becomes large, by the law of large numbers. Conversely, if $p_r(\mathbf{y})$ is greater than exp $(-NR)$, then chances are that at least one of the incorrect code words will not be discarded, again with probability approaching one as N becomes large. The probability that $p_r(\mathbf{y})$ is less than exp $(-NR)$ is

$$\begin{aligned} &\Pr\Big[\prod_{i=1}^{N} q_{j(i)}(0) < \exp(-NR) \Big] \\ &\qquad = \Pr\Big(\sum_{i=1}^{N} \ln q_{j(i)}(0) < -NR \Big), \end{aligned} \tag{61}$$

where the probability is over the ensemble of all $\mathbf{y}$. But the probability that a sum of N independent random

variables exceeds N times a constant goes to one with large N, if the constant is less than the mean of the variables, and to zero otherwise. But the mean of $\ln q_i(0)$ is

$$\begin{aligned}\overline{\ln q_i(0)} &= \sum_i q_i \ln q_i(0) \\ &= C_{0,f},\end{aligned} \tag{62}$$

where the latter equality holds if we choose $\mathbf{p}$ to maximize the mean, as is obviously desirable. Thus if $R < C_{0,f}$, the probability of (61) goes to one with large N. But

$$\begin{aligned}\Pr(\text{repeat}) &= \Pr[\text{repeat} \mid p_r(\mathbf{y}) < \exp(-NR)] \\ &\quad \cdot \Pr[p_r(\mathbf{y}) < \exp(-NR)] \\ &\quad + \Pr[\text{repeat} \mid p_r(\mathbf{y}) \geq \exp(-NR)] \\ &\quad \cdot \Pr[p_r(\mathbf{y}) \geq \exp(-NR)] \\ &= \begin{cases} 0 \cdot 1 + 1 \cdot 0 = 0, & R < C_{0,f}, \quad N \text{ large}, \\ 0 \cdot 0 + 1 \cdot 1 = 1, & R > C_{0,f}, \quad N \text{ large}. \end{cases}\end{aligned} \tag{63}$$

This argument, therefore, shows not only that arbitrarily small repeat probabilities (actually decreasing exponentially with N) can be obtained with zero-error probability when $R < C_{0,f}$, but also that when $R > C_{0,f}$ the repeat probability must approach one if zero-error probability is demanded. (A rigorous converse has been developed by Gallager in unpublished work.)

Implications for List Decoding

Previous work on list decoding has assumed a decoding list of fixed size. It has been shown that for a list size which is large but not exponential in N, a list-error exponent equal everywhere to the sphere-packing exponent could be obtained,[11] and that for list sizes increasing as $\exp NL$, a list-error exponent of $E_{sp}(R - L)$ was achievable.[4] Such large list sizes are of course unattractive for implementation, however. The principal significance of the present results is that by allowing a list of variable size, the average number of words on the list can be kept very small. In fact, we see from Figs. 4 and 5 that over a large range of $R < C$ and $T < 0$, the average number of incorrect words on the list is bounded by a quantity which decreases exponentially with N, and, therefore, that for large N the average list size is effectively one. Of course, the list for any one transmission may be as large as $\exp N(-T)$, so considerable buffering may be required. If provision of such buffering is feasible, however, and the list output useful, then one may obtain a list-error exponent well above the ordinary error exponent attainable at the same rate.

The question of how large a list-error exponent can be attained at a given rate R for a positive average incorrect list-size exponent is of some interest. Let us define $E_l(R)$ as the limiting value of $E_2(R, T)$, as $E_1(R, T)$ approaches zero. Rather than writing out parametric expressions, we note only a few properties which give the general character of $E_l(R)$. First, at zero rate, the parameter ρ may be allowed to become infinite, so the list exponent equals the feedback exponent

$$\begin{aligned}E_l(0) &= \lim_{\substack{s \to 1 \\ \rho \to \infty}} E_x(s, \rho, \mathbf{p}) \\ &= -\sum_k \sum_{k'} p_k p_{k'} \sum_j p_{jk} \ln \frac{p_{jk'}}{p_{jk}} \\ &= E_f(0),\end{aligned} \tag{64}$$

as follows from the mirror symmetry of exponents in the expurgated region. Second, to get an idea of behavior at high rates, let us first examine the list exponent for erasure-type channels, where $E_0(s, \rho, \mathbf{p})$ is independent of s. We recall from (47) that for such channels

$$\begin{aligned}E_1(R, T) &= E(R + T), \\ E_2(R, T) &= E(R + T) + T, \\ T &\leq 0 \quad \text{and} \quad R + T \geq R_{crit}.\end{aligned} \tag{65}$$

Clearly, the threshold T for which $E_2(R, T)$ equals zero can be determined from the ordinary error exponent as that $T(R)$ which solves

$$-T(R) = E[R + T(R)], \tag{66}$$

the list exponent is then simply

$$E_l(R) = E[R + T(R)] = -T(R). \tag{67}$$

Graphically, $E_l(R)$ is therefore the intercept of a line of slope -1 drawn through R with the $E(R)$ curve; Fig. 6 illustrates the construction of $E_l(R)$ in the high-rate region. We note, as was clear from Fig. 5, that $E_l(R)$ is infinite at rates below R_{comp}. However, at rates above R_{comp}, $E_l(R)$ rapidly approaches the $E(R)$ curve, so that little improvement is obtained in this region.

For the general channel, the construction of Fig. 6 represents an upper bound to the attainable list exponent, as we now show. Since from (24) and (26) or (52), in the high-rate region

$$E_1 = \max_{0 \leq s \leq \rho \leq 1, \mathbf{p}} \frac{1}{1 - s} E_0(s, \rho, \mathbf{p}) - \frac{\rho}{1 - s} R - \frac{s}{1 - s} E_2, \tag{68}$$

we have

$$E_l(R) = \max_{0 \leq s \leq \rho \leq 1, \mathbf{p}} \frac{E_0(s, \rho, \mathbf{p}) - \rho R}{1 - s}. \tag{69}$$

Let

$$E_{l0}(R) = \max_{0 \leq \rho \leq 1, \mathbf{p}} \frac{E_0(\rho, \mathbf{p}) - \rho R}{1 - \rho}, \tag{70}$$

which is the curve given by the construction of Fig. 6;

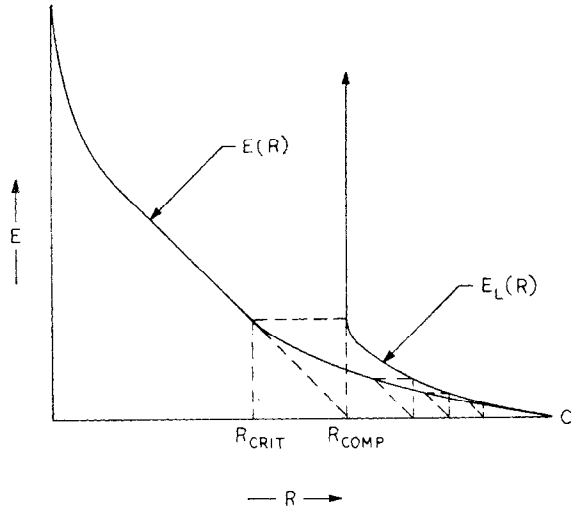

Fig. 6. Construction of list exponent from ordinary error exponent for erasure-type channels.

then we can bound (69) by loosening the restrictions on s:

$$\begin{aligned} E_l(R) &\leq \max_{0\leq s_1\leq\rho\leq 1, 0\leq s_2\leq\rho, \mathbf{p}} \frac{E_0(s_1, \rho, \mathbf{p}) - \rho R}{1 - s_2} \\ &= \max_{0\leq\rho\leq 1, \mathbf{p}} \frac{E_0(\rho, \mathbf{p}) - \rho R}{1 - \rho} \\ &= E_{l0}(R) \end{aligned} \tag{71}$$

with equality for erasure-type channels.

The moral we draw is that at rates above R_{comp}, not much improvement is obtained by going to lists over ordinary decoding. At rates below R_{comp}, however, significant improvement can be achieved, approaching that attainable with feedback at very low rates. Thus, as with sequential decoding,[9] we find that R_{comp} represents a kind of complexity limit for high-performance schemes without feedback.

Finally, we may inquire about the existence of a list zero-error capacity $C_{0,l}$, namely a rate for which with a sieve-like decoding procedure we obtain an average number of incorrect words on the decoding list decreasing exponentially with N, and of course no errors. We find that the $E_l(R)$ of (69) goes to infinity as $s \to \rho \to 1$, where the rate becomes

$$C_{0,l} = \max_{\mathbf{p}} [-\ln \sum_j q_j q_j(0)], \tag{72}$$

where q_j and $q_j(0)$ are defined as in (59). From the fact that $E_{l0}(R)$ bounds $E_l(R)$ above, we have that for any channel

$$C_{0,l} \leq R_{\text{comp}}. \tag{73}$$

Like the feedback zero-error capacity, the list zero-error capacity can be obtained directly. We have already shown that with the random selection procedure of that earlier argument, the probability of an incorrect code word being retained, given $\mathbf{y}$, is the $p_r(\mathbf{y})$ of (60); the average number of incorrect words retained is therefore

$$\begin{aligned} &(\exp NR - 1) \overline{\prod_{i=1}^{N} q_{j(i)}(0)} \\ &= (\exp NR - 1) \prod_{i=1}^{N} \overline{q_{j(i)}(0)} \\ &= (\exp NR - 1) [\sum_j q_j q_j(0)]^N \\ &< \exp N[R - C_{0,l}], \end{aligned} \tag{74}$$

where the second step depends on the $q_j(0)$ being independent, and the last on the use of the optimum $\mathbf{p}$. Thus the average number of incorrect words on the decoder's list decreases exponentially with N whenever $R < C_{0,l}$.

An interesting inequality links the sphere-packing, list, and feedback zero-error capacities. By letting ρ approach infinity in (22), we find that

$$C_{0,sp} = \max_{\mathbf{p}} \{-\ln [\max q_j(0)]\}. \tag{75}$$

We can then express all three capacities in terms of the quantity $M(r)$ defined by

$$M(r) = [\sum_j q_j q_j(0)^r]^{1/r}. \tag{76}$$

It is well known[12] that if $r > r'$, then $M(r) \geq M(r')$, with equality only when $q_j(0)$ is independent of j, as with totally symmetric channels. We observe that

$$\begin{aligned} C_{0,sp} &= \max_{\mathbf{p}} \lim_{r\to\infty} [-\ln M(r)], \\ C_{0,l} &= \max_{\mathbf{p}} [-\ln M(1)], \\ C_{0,f} &= \max_{\mathbf{p}} \lim_{r\to 0} [-\ln M(r)], \end{aligned} \tag{77}$$

from which there follows immediately the inequality

$$C_{0,sp} \leq C_{0,l} \leq C_{0,f}, \tag{78}$$

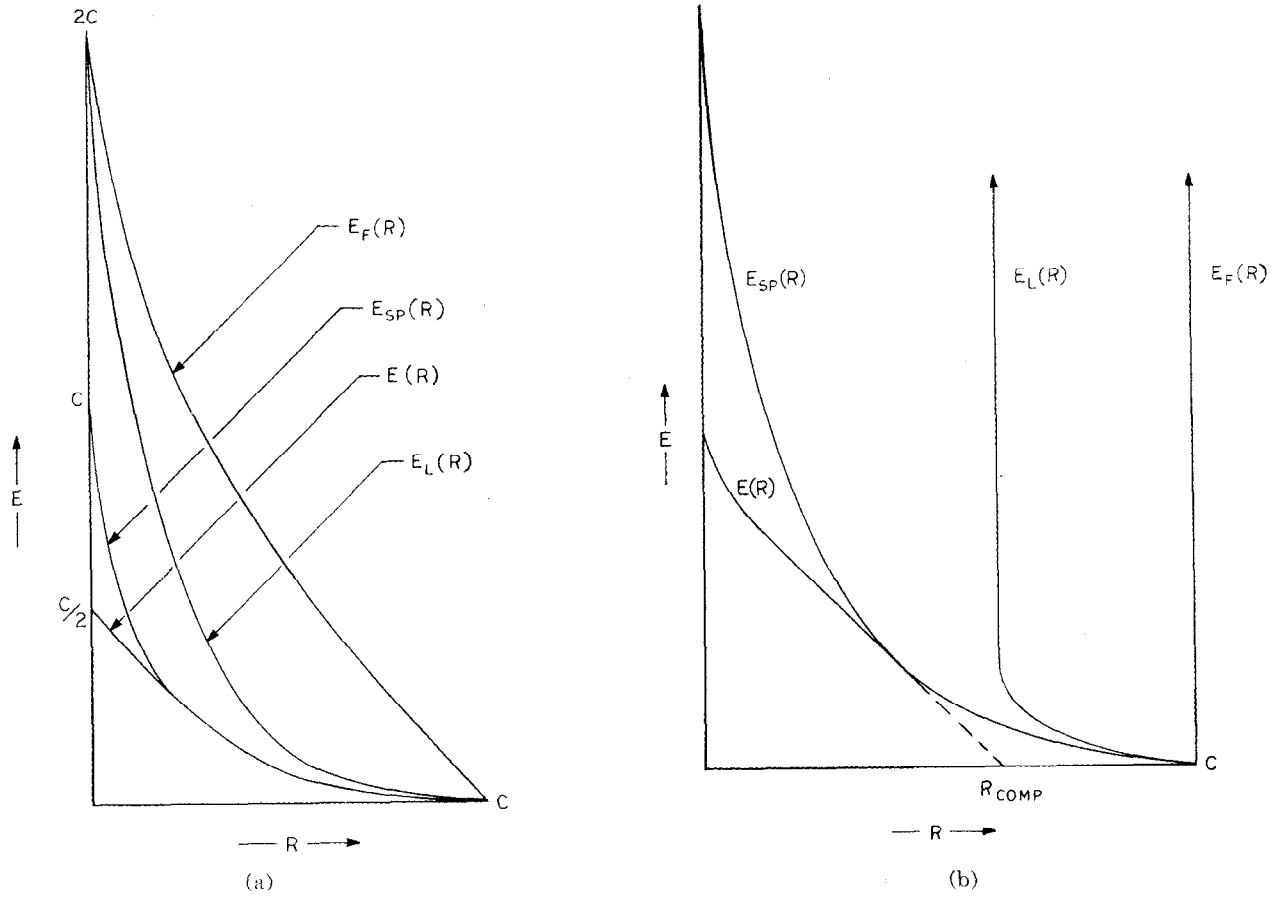

Fig. 7. (a) Very noisy channel exponents:

$$E_f(R) = 2C - 2\sqrt{RC};$$

$$E_l(R) = \begin{cases} 2C - 2\sqrt{2RC}, & R \leq (6 - 4\sqrt{2})C \\ 2\sqrt{RC} - 2C\sqrt{2\sqrt{R/C} - 1}, & R \geq (6 - 4\sqrt{2})C; \end{cases}$$

$$E_{sp}(R) = (\sqrt{C} - \sqrt{R})^2;$$

$$E(R) = \begin{cases} E_{sp}(R), & R \geq C/4 \\ C/2 - R, & R \leq C/4. \end{cases}$$

(b) Erasure-type channel exponents.

where the equalities hold only when $q_i(0)$ is independent of j.

Finally, in Fig. 7 we have plotted the four exponents $E(R)$, $E_{sp}(R)$, $E_l(R)$, and $E_f(R)$ for the very noisy channel and for an erasure-type channel to give some graphic feeling for their relative magnitudes.

Open Questions

One would hope that, at least in the high-rate range, the upper bounds developed here were exponentially tight. One's hopes are encouraged by the similarity of this derivation to that which yields the ordinary error exponent, known to be tight in the high-rate region, and also by the fact that these bounds are equal to, or better than the best previously known in all cases, with no counterexamples yet sighted. Finding a complementary lower bound on attainable probabilities is therefore a theoretical task of considerable interest.

Secondly, we hope that these results, which demonstrate the performance improvements obtainable when the decoder is given flexible decoding options, will stimulate the development of applications. We are pursuing applications in concatenation schemes; many others have been interested in various uses of feedback. Undoubtedly these efforts do not exhaust the potential uses of the ideas treated here.

Appendix

In this Appendix we collect proofs which we felt would have unduly cluttered the main text.

Proof of Theorem 1 (Neyman–Pearson): Our proof follows Davenport and Root.[13] Let U be the region common to the regions R_1 and R_2 defined in the theorem. Then

$$\begin{aligned} P_1(Y - R_1) &= P_1(Y) - P_1(R_1) \\ &= P_1(Y) - P_1(R_1 - U) - P_1(U), \\ P_1(Y - R_2) &= P_1(Y) - P_1(R_2 - U) - P_1(U), \end{aligned} \tag{79}$$

where Y is the whole space and $P_1(\cdot)$ is the measure defined in (7). Since $R_1 - U$ is contained in R_1, (8) applies, so

$$\begin{aligned} P_1(R_1 - U) &= \sum_{y \in R_1 - U} f_1(y) \\ &\geq \sum_{y \in R_1 - U} \eta f_0(y) \\ &= \eta P_0(R_1 - U). \end{aligned} \tag{80}$$

On the other hand, $R_2 - U$ is wholly outside R_1, so that

$$P_1(R_2 - U) \leq \eta P_0(R_2 - U). \tag{81}$$

But with the use of (9) we have that

$$\begin{aligned} P_0(R_2 - U) &= P_0(R_2) - P_0(U) \\ &\leq P_0(R_1) - P_0(U) \\ &= P_0(R_1 - U). \end{aligned} \tag{82}$$

The combination of (79) through (82) gives the inequality (10) of the theorem.

Proof of Theorem 2 (General Bounds): Here we obtain bounds on the quantities Pr (E_1) and Pr (E_2) of (5) and (4) under the decision criterion expressed by (11). For notational economy, we define for this proof only the shorthand notation

$$\begin{aligned} P_m &= \Pr(\mathbf{y} \mid \mathbf{x}_m), \\ Q_m &= \sum_{m' \neq m} \Pr(\mathbf{y} \mid \mathbf{x}_{m'}), \end{aligned} \tag{83}$$

and from the beginning let all code words be equiprobable (Pr $(\mathbf{x}_m) = 1/M$), though this can be delayed for a considerable time in the proof. Then the decision criterion becomes

$$\mathbf{y} \in R_m \text{ iff } P_m/Q_m \geq \exp NT, \tag{84}$$

and

$$\begin{aligned} \Pr(E_1) &= \frac{1}{M} \sum_m \sum_{\mathbf{y} \notin R_m} P_m, \\ \Pr(E_2) &= \frac{1}{M} \sum_m \sum_{\mathbf{y} \in R_m} Q_m. \end{aligned} \tag{85}$$

Our first step is to use (84) in (85)

$$\begin{aligned} \Pr(E_1) &= \frac{1}{M} \sum_m \sum_{\mathbf{y} \notin R_m} P_m^{1-s} Q_m^s (P_m/Q_m)^s \\ &\leq \frac{1}{M} \sum_m \sum_{\mathbf{y} \notin R_m} P_m^{1-s} Q_m^s \exp NTs, \qquad s \geq 0, \\ \Pr(E_2) &= \frac{1}{M} \sum_m \sum_{\mathbf{y} \in R_m} P_m^{1-s} Q_m^s (Q_m/P_m)^{1-s} \\ &\leq \frac{1}{M} \sum_m \sum_{\mathbf{y} \in R_m} P_m^{1-s} Q_m^s \exp[-NT(1-s)], \quad s \leq 1, \end{aligned} \tag{86}$$

where we have introduced s as a parameter. Defining the moment generating function $g_m(-s)$ by

$$g_m(-s) = \sum_{\mathbf{y}} P_m (P_m/Q_m)^{-s}, \tag{87}$$

and observing that $g_m(-s)$ is non-negative, we can further bound Pr (E_1) and Pr (E_2) by allowing the sum to extend over the entire output space, whence

$$\begin{aligned} &\Pr(E_1) \leq \exp NTs \frac{1}{M} \sum_m g_m(-s), \\ &\Pr(E_2) \leq \exp[-NT(1-s)] \frac{1}{M} \sum_m g_m(-s), \\ &\qquad\qquad 0 \leq s \leq 1. \end{aligned} \tag{88}$$

The key to the proof is now Jensen's inequality,[12] which states that

$$[\sum_i a_i^r]^{1/r} \leq \sum_i a_i, \qquad r \geq 1. \tag{89}$$

Introducing a second parameter ρ, we have that

$$\begin{aligned} g_m(-s) &= \sum_{\mathbf{y}} P_m^{1-s} [(\sum_{m' \neq m} P_{m'})^{s/\rho}]^\rho \\ &\leq \sum_{\mathbf{y}} P_m^{1-s} (\sum_{m' \neq m} P_{m'}^{s/\rho})^\rho, \qquad \rho \geq s. \end{aligned} \tag{90}$$

We cannot proceed further without specifying the code. As is customary, we choose a code at random by choosing each input letter of each code word by a random selection in which the probability of choosing input x_k is p_k. Denoting an average over the ensemble of all such codes by an overbar, we can then bound the average moment generating function $\overline{g_m(-s)}$ by Gallager's methods:[3]

$$\overline{g_m(-s)} \leq \overline{\sum_{\mathbf{y}} P_m^{1-s} (\sum_{m' \neq m} P_{m'}^{s/\rho})^\rho} \tag{91a}$$

from (90);

$$= \sum_{\mathbf{y}} \overline{P_m^{1-s} (\sum_{m' \neq m} P_{m'}^{s/\rho})^\rho} \tag{91b}$$

average of a sum equals sum of the averages;

$$= \sum_{\mathbf{y}} \overline{P_m^{1-s}} \, \overline{(\sum_{m' \neq m} P_{m'}^{s/\rho})^\rho} \tag{91c}$$

average of a product of independent variables equals product of the averages; independence ensured by our choice of ensemble;

$$\leq \sum_{\mathbf{y}} \overline{P_m^{1-s}} \, (\overline{\sum_{m' \neq m} P_{m'}^{s/\rho}})^\rho, \qquad \rho \leq 1 \tag{91d}$$

$[\bar{f}^r]^{1/r} \leq \bar{f}$, $r \leq 1$; see under (76) in the text;

$$= \sum_{\mathbf{y}} \overline{P_m^{1-s}} \, (\overline{\sum_{m'} P_{m'}^{s/\rho}})^\rho \tag{91e}$$

average of sum equals sum of averages;

$$< \exp \rho NR \sum_{\mathbf{y}} \overline{P_m^{1-s}} \, \overline{(P_{m'}^{s/\rho})^\rho} \tag{91f}$$

exp $NR - 1$ identical terms.

If we now recall the useful rule for interchanging sum aud product signs,

$$\sum_{\mathbf{y}} \prod_{i=1}^{N} f(y_i) = \prod_{i=1}^{N} \sum_{y_i} f(y_i), \tag{92}$$

we see that (91f) breaks down into an average of a product of N identically distributed random variables, which is the product of the averages, and which can be written out as

$$\overline{g_m(-s)} < \exp \rho NR[\sum_j (\sum_k p_k p_{jk}^{1-s})(\sum_{k'} p_{k'} p_{jk'}^{s/\rho})^{\rho}]^N, \tag{91g}$$

or

$$\overline{g_m(-s)} < \exp\{-N[E_0(s, \rho, \mathbf{p}) - \rho R]\}, \quad 0 \le s \le \rho \le 1, \tag{91h}$$

where $E_0(s, \rho, \mathbf{p})$ is defined as in (24). Since this bound is independent of m, it also applies to the quantity $M^{-1} \sum_m \overline{g_m(-s)}$, and since it applies to the average, there must be at least one code in the ensemble for which it applies to the quantity $M^{-1} \sum_m g_m(-s)$. For this code, by substitution in (88), we obtain simultaneously

$$\Pr(E_1) < \exp\{-N[E_0(s, \rho, \mathbf{p}) - \rho R - sT]\},$$

$$\Pr(E_2) < \exp\{-N[E_0(s, \rho, \mathbf{p}) - \rho R + (1 - s)T]\}, \quad 0 \le s \le \rho \le 1. \tag{93}$$

For fixed R and T, the bounds differ by T for any s, ρ, and $\mathbf{p}$, so that they are both maximized by the same values of these parameters, as stated in (24) and (26).

Gallager's expurgation technique improves this bound at low rates. Define

$$q(\mathbf{x}_m, \mathbf{x}_{m'}, s) = \sum_{\mathbf{y}} P_m^{1-s} P_{m'}^{s}, \tag{94}$$

then from (87)

$$g_m(-s) = \sum_{m' \neq m} q(\mathbf{x}_m, \mathbf{x}_{m'}, s). \tag{95}$$

If we choose a code from a random ensemble as before, the probability that $g_m(-s)$ will equal or exceed some number B is

$$\Pr[g_m(-s) \ge B] = \overline{\phi_{\text{code}}(s)}, \tag{96}$$

where

$$\phi_{\text{code}}(s) = \begin{cases} 1, & g_m(-s) \ge B, \\ 0, & g_m(-s) < B. \end{cases} \tag{97}$$

We upper bound $\phi_{\text{code}}(s)$ by

$$\phi_{\text{code}}(s) \le \sum_{m' \neq m} \frac{q(\mathbf{x}_m, \mathbf{x}_{m'}, s)^{1/\rho}}{B^{1/\rho}}, \quad \rho \ge 1. \tag{98}$$

Equation (98) is obvious for $\phi_{\text{code}}(s) = 0$; for $\rho = 1$ and $\phi_{\text{code}}(s) = 1$, (98) follows from (95) and (97); increasing ρ increases all terms in the sum less than 1, and if any term is greater than 1, (98) is true anyway. Thus

$$\Pr[g_m(-s) \ge B] \le B^{-1/\rho} \sum_{m' \neq m} \overline{(\sum_{\mathbf{y}} P_m^{1-s} P_{m'}^{s})^{1/\rho}}, \quad \rho \ge 1 \tag{99a}$$

substituting (94) and (98) into (96);

$$< B^{-1/\rho} \exp NR \overline{(\sum_{\mathbf{y}} P_m^{1-s} P_{m'}^{s})}^{1/\rho} \tag{99b}$$

exp NR − 1 equal terms;

$$= B^{-1/\rho} \exp NR[\sum_k \sum_{k'} p_k p_{k'} (\sum_j p_{jk}^{1-s} p_{jk'}^{s})^{1/\rho}]^N \tag{99c}$$

using (92), and writing out the indicated average, a product of N identical averages. With $E_x(s, \rho, \mathbf{p})$ defined as in (25), we have

$$\Pr[g_m(-s) \ge B] < B^{-1/\rho} \exp\left\{-\frac{N}{\rho}[E_x(s, \rho, \mathbf{p}) - \rho R]\right\}, \quad 0 \le s \le 1, \quad \rho \ge 1. \tag{100}$$

Let us then choose B to be

$$B_0 = 2^{\rho} \exp\{-N[E_x(s, \rho, \mathbf{p}) - \rho R]\}, \tag{101}$$

then

$$\Pr[g_m(-s) \ge B_0] < \tfrac{1}{2}. \tag{102}$$

If we then expurgate all code words $\mathbf{x}_m$ for which $g_m(-s) \ge B_0$, the average number of code words remaining in a code will be greater than $M' = M/2$, from (102), so there must be at least one code with M' code words and thus rate R', where

$$R' > \frac{1}{N} \ln M' = R - \frac{\ln 2}{N}. \tag{103}$$

For every word in this code

$$g_m(-s) < B_0 = \exp\left\{-N\left[E_x(s, \rho, \mathbf{p}) - \rho R - \frac{\rho \ln 2}{N}\right]\right\}, \tag{104}$$

using (101). Substituting back in (88), we find that we can achieve simultaneously

$$\Pr(E_1) < \exp\{-N[E_x(s, \rho, \mathbf{p}) - \rho R - sT - o(1)]\}$$

$$\Pr(E_2) < \exp\{-N[E_x(s, \rho, \mathbf{p}) - \rho R + (1 - s)T - o(1)]\}, \quad 0 \le s \le 1, \quad \rho \ge 1, \tag{105}$$

where $o(1)$ is a function which goes to zero as N goes to infinity. Again the bounds are jointly optimized by a single set of s, ρ, and $\mathbf{p}$, giving the bounds of (25) and (26). The $o(1)$ is ignored in the text as inconsequential.

Proof of Theorem 3 (Construction from Sphere-Packing Exponent): An alternative statement of Theorem 2 comes from solving for T in (24) and (26); then we can say that there exists a code of length N and rate R nats and a decoding scheme such that

$$\Pr(E_1) < \exp(-NE_1),$$
$$\Pr(E_2) < \exp[-NE_2(R, E_1)], \tag{106}$$
$$E_2(R, E_1) = \max_{0\le s\le\rho\le 1,\mathbf{p}} \frac{1}{s}E_0(s, \rho, \mathbf{p}) - \frac{\rho}{s}R - \frac{1-s}{s}E_1,$$

where $E_0(s, \rho, \mathbf{p})$ is as in (24). It is now convenient to perform the change of variables

$$\rho_1 = \frac{\rho - s}{s}$$
$$\rho_2 = \frac{s}{1-s} \tag{107}$$

and to restrict ourselves to some particular value of $\mathbf{p}$; then

$$E_2(R, E_1) \ge \max_{\rho_1\ge 0, 0\le\rho_2\le 1/\rho_1} \frac{1+\rho_2}{\rho_2}E_0(\rho_1, \rho_2, \mathbf{p}) - (1+\rho_1)R - \frac{1}{\rho_2}E_1, \tag{108}$$
$$E_0(\rho_1, \rho_2, \mathbf{p}) = -\ln \sum_j \Big(\sum_k p_k p_{jk}^{1/(1+\rho_2)}\Big) \Big(\sum_{k'} p_{k'} p_{jk'}^{1/(1+\rho_1)}\Big)^{\rho_2(1+\rho_1)/(1+\rho_2)},$$

where equality holds when we use the optimum $\mathbf{p}$. Now take some rate R' which satisfies $R(1/\rho_1, \mathbf{p}) \le R' \le R(0, \mathbf{p})$, and let

$$E_1 = E_{sp}(R', \mathbf{p}) = \max_{0\le\rho\le 1/\rho_1} E_0(\rho, \mathbf{p}) - \rho R', \tag{109}$$

where the definition of the fixed-rate sphere-packing exponent is that of (30). From the convexity of $E_{sp}(R', \mathbf{p})$,[3] we have the inverse relationship

$$R' = \max_{0\le\rho\le 1/\rho_1} \frac{E_0(\rho, \mathbf{p}) - E_1}{\rho}. \tag{110}$$

Now we bound $E_0(\rho_1, \rho_2, \mathbf{p})$ by Hölder's inequality:[12]

$$E_0(\rho_1, \rho_2, \mathbf{p}) \ge -\ln\Big[\sum_j \Big(\sum_k p_k p_{jk}^{1/(1+\rho_2)}\Big)^{1+\rho_2}\Big]^{1/(1+\rho_2)} \cdot\Big[\sum_j \Big(\sum_k p_k p_{jk}^{1/(1+\rho_1)}\Big)^{1+\rho_1}\Big]^{\rho_2/(1+\rho_2)}$$
$$= \frac{1}{1+\rho_2}E_0(\rho_2, \mathbf{p}) + \frac{\rho_2}{1+\rho_2}E_0(\rho_1, \mathbf{p}), \tag{111}$$

where $E_0(\rho, \mathbf{p})$ is defined by (18); equality holds if

$$q_j(x) = \sum_k p_k p_{jk}^{\frac{1}{1+\rho}} \tag{112}$$

is independent of j. Now substitution of (111) into (108) yields

$$E_2(R, E_1) \ge \max_{\rho_1\ge 0, 0\le\rho_2\le 1/\rho_1} E_0(\rho_1, \mathbf{p}) - (1+\rho_1)R + \frac{E_0(\rho_2, \mathbf{p}) - E_1}{\rho_2}. \tag{113}$$

The maximizations can be carried out separately, and with the use of (109) and (110) become

$$E_2(R, E_1) \ge E_{sp}(R, \mathbf{p}) - R + R'. \tag{114}$$

This and (109) combine to give the statement of Theorem 3. Theorem 3(a), for totally symmetric channels, follows from tracing the cases of equality.

Acknowledgment

The author is indebted to R. G. Gallager for his intellectual leadership and invaluable criticism.

References

[1] C. E. Shannon and W. Weaver, *The Mathematical Theory of Communication*. Urbana, Ill.: University of Illinois Press, 1949.
[2] R. M. Fano, *Transmission of Information*. Cambridge, Mass.: M.I.T. Press, 1961.
[3] R. G. Gallager, "A simple derivation of the coding theorem and some applications," *IEEE Trans. Information Theory*, vol. IT-11, pp. 3–18, January 1965.
[4] C. E. Shannon, R. G. Gallager, and E. Berlekamp, "Lower bounds to error probability for coding on discrete memoryless channels," *Information Control*, vol. 10, pp. 65–103, 1967.
[5] C. E. Shannon, "The zero-error capacity of a noisy channel," *IRE Trans. Information Theory*, vol. IT-2, pp. 8–19, September 1956.
[6] G. D. Forney, *Concatenated Codes*. Cambridge, Mass.: M.I.T. Press, 1966.
[7] G. D. Forney, "On decoding BCH codes," *IEEE Trans. Information Theory*, vol. IT-11, pp. 549–558, October 1965.
[8] G. D. Forney, "Generalized minimum distance decoding," *IEEE Trans. Information Theory*, vol. IT-12, pp. 125–132, April 1966.
[9] J. E. Savage, "Sequential decoding—the computation problem," *Bell Sys. Tech. J.*, vol. 45, pp. 149–177, 1966.
[10] B. Reiffen, "A note on very noisy channels," *Information Control*, vol. 6, p. 126, 1963.
[11] P. M. Ebert, "Error bounds for parallel communication channels," M.I.T. Research Laboratory of Electronics, Cambridge, Mass., Tech. Rept. 448, 1966, Appendix C.
[12] G. H. Hardy, J. E. Littlewood, and G. Polya, *Inequalities*. Cambridge, England: Cambridge University Press, 1959.
[13] W. B. Davenport, Jr., and W. L. Root, *Random Signals and Noise*. New York: McGraw-Hill, 1958, pp. 322–324.