THE GALLAGER AND BHATTACHARYYA BOUNDS, ORTHOGONAL SIGNAL AND RANDOM CODING BOUNDS

William A. Pearlman

2005

The Union Bound

Given a set of signals (vectors) $\mathbf{s}_1, \mathbf{s}_2, ..., \mathbf{s}_M$, the Union Bound on the probability of error given the kth was sent is

$$P(\mathcal{E}/\mathbf{s}_k) \leq \sum_{i \neq k} P(\mathcal{E}_{i,k}/\mathbf{s}_k) \tag{1}$$

For orthogonal signals, $|\mathbf{s}_1 - \mathbf{s}_k| = \sqrt{2E_s}, i \neq k$, and

$$P(\mathcal{E}) \leq (M-1)Q(\sqrt{E_s/N_o})$$

For bi-orthogonal signals,

$$|\mathbf{s}_i - \mathbf{s}_k| = \sqrt{2E_s} \text{ for } i \neq k \text{ in a different dimension}$$

and

$$|\mathbf{s}_i - \mathbf{s}_k| = 2\sqrt{E_s} \text{ for the one } i \text{ in the same dimension,}$$

so that

$$P(\mathcal{E}) \leq (M-2)Q\left(\sqrt{\frac{E_s}{N_o}}\right) + Q\left(\frac{2E_s}{N_o}\right)$$

These bounds are increasingly tight as M and E_s/N_o grow larger.

The Battacharyya Bound

We shall now develop a bound on $P(\mathcal{E}_{i,k}/\mathbf{s}_k)$ called the Bhattacharyya bound. The event $\mathcal{E}_{i,k}$ is formally defined as

$$\mathcal{E}_{i,k} = \{\mathbf{r} : p(\mathbf{r}/\mathbf{s}_i) > p(\mathbf{r}/\mathbf{s}_k)\} \quad (i \neq k) \tag{2}$$

for **maximum likelihood decoding**. Consider the indicator function of the above event defined as

$$\phi(\mathbf{r}) = \begin{cases} 1, & \mathbf{r} \in \mathcal{E}_{i,k} \\ 0, & \mathbf{r} \notin \mathcal{E}_{i,k} \end{cases}$$

Therefore, the conditional probability of $\mathcal{E}_{i,k}$ given $\mathbf{s}_k$ is expressed as

$$\begin{aligned} P(\mathcal{E}_{i,k}/\mathbf{s}_k) &= \int_{\mathcal{E}_{i,k}} p(\mathbf{r}/\mathbf{s}_k) d\mathbf{r} \\ &= \int_{\text{all } \mathbf{r}} \phi(\mathbf{r}) p(\mathbf{r}/\mathbf{s}_k) d\mathbf{r} \end{aligned} \tag{3}$$

Since $p(\mathbf{r}/\mathbf{s}_i)/p(\mathbf{r}/\mathbf{s}_k)$ exceeds one for all $\mathbf{r}$ in $\mathcal{E}_{i,k}$, we may overbound $\phi(\mathbf{r})$ by

$$\phi(\mathbf{r}) = 1 \leq \sqrt{\frac{p(\mathbf{r}/\mathbf{s}_i)}{p(\mathbf{r}/\mathbf{s}_k)}} \quad \text{for } \mathbf{r} \in \mathcal{E}_{i,k}.$$

Also, since $\sqrt{p(\mathbf{r}/\mathbf{s}_i)/p(\mathbf{r}/\mathbf{s}_k)}$ is nonnegative for any $\mathbf{r}$, we may also use it as an overbound for $\phi(\mathbf{r})$ for $\mathbf{r}$ elsewhere. Therefore,

$$\phi(\mathbf{r}) \leq \sqrt{\frac{p(\mathbf{r}/\mathbf{s}_i)}{p(\mathbf{r}/\mathbf{s}_k)}}, \quad \text{all } \mathbf{r} \tag{4}$$

Substituting (4) into (3), we obtain an upper bound on $P(\mathcal{E}_{i,k}/\mathbf{s}_k)$ given by

$$P(\mathcal{E}_{i,k}/\mathbf{s}_k) \leq \int_{\text{all } \mathbf{r}} \sqrt{p(\mathbf{r}/\mathbf{s}_i) p(\mathbf{r}/\mathbf{s}_k)} \quad i \neq k \tag{5}$$

and known as the Bhattacharyya bound. Combined with the union bound in (1),

$$P(\mathcal{E}/\mathbf{s}_k) \leq \int_{\mathbf{r}} \sum_{i \neq k} \sqrt{p(\mathbf{r}/\mathbf{s}_i) p(\mathbf{r}/\mathbf{s}_k)} d\mathbf{r} \tag{6}$$

We can calculate the above Bhattacharyya bound for the AWGN channel since

$$p(\mathbf{r}/\mathbf{s}_i) = \frac{1}{(\pi N_o)^{1/2}} \exp -\frac{1}{N_o}|\mathbf{r}-\mathbf{s}_i|^2 \quad i = 1, 2, ..., M$$

Substituting into (5), we obtain after straightforward calculations:

$$P(\mathcal{E}_{i,k}/\mathbf{s}_k) \leq \exp -\frac{1}{4N_o}|\mathbf{s}_i - \mathbf{s}_k|^2 \quad i \neq k$$

The exact expression is $Q\left(\frac{|\mathbf{s}_i-\mathbf{s}_k|}{\sqrt{2N_o}}\right)$ as mentioned previously. From p. 82 of Wozencraft and Jacobs,

$$\left(1-\frac{1}{\alpha^2}\right)\frac{1}{\sqrt{2\pi}\alpha}e^{-\alpha^2/2} < Q(\alpha) < \frac{1}{\sqrt{2\pi}\alpha}e^{-\alpha^2/2}$$

Hence the Bhattacharyya bound is reasonably good, and exponentially tight, for larger $|\mathbf{s}_i - \mathbf{s}_k|/\sqrt{2N_o}$.

In the case of equiprobable and equal energy E_s orthogonal signals, and when combined with the union bound (1), we obtain

$$\begin{aligned} P(\mathcal{E}_{i,k}/\mathbf{s}_k) &\leq \exp -\frac{E_s}{2N_o} \\ P(\mathcal{E}/\mathbf{s}_k) &= P(\mathcal{E}) \leq (M-1)\exp -\frac{E_s}{2N_o} \end{aligned} \tag{7}$$

This bound is useless when $M - 1 > e^{E_s/2N_o}$.

The Gallager Bound

The Gallager bound is, in a sense, a generalization of the union-Bhattacharyya (U-B) bound. Consider the events

$$\mathcal{E}_k = \bigcup_{i\neq k} \mathcal{E}_{i,k} = \left\{\mathbf{r} : \frac{p(\mathbf{r}/\mathbf{s}_i)}{p(\mathbf{r}/\mathbf{s}_k)} > 1 \ \text{ for some } i \neq k\right\}$$

and

$$\tilde{\mathcal{E}}_k = \left\{\mathbf{r} : \sum_{i\neq k}\left[\frac{p(\mathbf{r}/\mathbf{s}_i)}{p(\mathbf{r}/\mathbf{s}_k)}\right]^{\lambda} > 1\right\} \quad \lambda > 0$$

We shall show that

$$\mathcal{E}_k \subset \tilde{\mathcal{E}}_k.$$

If $\mathbf{r}$ is in $\mathcal{E}_k$, then $p(\mathbf{r}/\mathbf{s}_i)/p(\mathbf{r}/\mathbf{s}_k) > 1$ for some $i \neq k$ and for $\lambda > 0, (p(\mathbf{r}/\mathbf{s}_i)/p(\mathbf{r}/\mathbf{s}_k))^\lambda > 1$ for some $i \neq k$. Adding other nonnegative terms doesn't affect the inequality so that

$$\sum_{i \neq k} \left(\frac{p(\mathbf{r}/\mathbf{s}_i)}{p(\mathbf{r}/\mathbf{s}_k)} \right)^\lambda > 1 \quad \text{if } \mathbf{r} \in \mathcal{E}_k.$$

Therefore $\mathbf{r}$ is also in $\tilde{\mathcal{E}}_k$ and $\mathcal{E}_k \subset \tilde{\mathcal{E}}_k$ is proved. Given that $\mathbf{s}_k$ is sent,

$$P(\mathcal{E}_k) = \int_{\mathbf{r} \in \mathcal{E}_k} p(\mathbf{r}/\mathbf{s}_k) d\mathbf{r} \leq \int_{\mathbf{r} \in \tilde{\mathcal{E}}_k} p(\mathbf{r}/\mathbf{s}_k) d\mathbf{r}$$

The previous inequality follows since we are integrating a nonnegative quantity over a bigger set. Given that $\mathbf{s}_k$ is sent $P(\mathcal{E}_k)$ is exactly what we called $P(\mathcal{E}/\mathbf{s}_k)$. Using the indicator function $\tilde{\phi}(\mathbf{r})$ of the set $\tilde{\mathcal{E}}_k$, we see that

$$P(\mathcal{E}/\mathbf{s}_k) \leq \int_{\text{all } \mathbf{r}} \tilde{\phi}(\mathbf{r}) p(\mathbf{r}/\mathbf{s}_k) d\mathbf{r} \tag{8}$$

Also

$$\tilde{\phi}(\mathbf{r}) \leq \left[\sum_{i \neq k} \left(\frac{p(\mathbf{r}/\mathbf{s}_i)}{p(\mathbf{r}/\mathbf{s}_k)} \right)^\lambda \right]^M \tag{9}$$

for all $\mathbf{r}, M \geq 0$, and $\lambda \geq 0$. This fact follows since the term inside the brackets [ ] is at least 1 for all $\mathbf{r} \in \tilde{\mathcal{E}}_k$ and at least zero for $\mathbf{r} \notin \tilde{\mathcal{E}}_k$. Substituting the bound in (9) into (8), we obtain

$$\begin{aligned} P(\mathcal{E}/\mathbf{s}_k) &\leq \int_{\text{all } \mathbf{r}} \left[\sum_{i \neq k} \left(\frac{p(\mathbf{r}/\mathbf{s}_i)}{p(\mathbf{r}/\mathbf{s}_k)} \right)^\lambda \right]^\mu p(\mathbf{r}/\mathbf{s}_k) d\mathbf{r} \qquad (10) \\ &= \int_{\text{all } \mathbf{r}} p(\mathbf{r}/\mathbf{s}_k)^{1-\lambda\mu} \left[\sum_{i \neq k} (p(\mathbf{r}/\mathbf{s}_i))^\lambda \right]^\mu d\mathbf{r} \end{aligned}$$

Since $\mu \geq 0$ and $\lambda \geq 0$, but otherwise arbitrary, we may select $\lambda = 1/(1+\mu)$ to obtain the final Gallager bound:

$$P(\mathcal{E}/\mathbf{s}_k) \leq \int_{\mathbf{r}} (p(\mathbf{r}/\mathbf{s}_k))^{\frac{1}{1+\mu}} \left[\sum_{i \neq k} (p(\mathbf{r}/\mathbf{s}_i))^{\frac{1}{1+\mu}} \right]^\mu d\mathbf{r} \quad \mu \geq 0 \tag{11}$$

We then choose the $\mu \geq 0$ that minimizes the right-hand side of (10) to give the tightest upper bound. Note that $\mu = 1$ is identical to the U-B bound in (6).

Application to Orthogonal Signals in AWGN. Given $\mathbf{s}_k$,

$$\begin{aligned} r_k &= \sqrt{E_s} + n_k \\ r_i &= n_i \quad i \neq k, \text{ i.e., } i = 1, 2, ..., k-1, k+1, ..., M = N \end{aligned}$$

where $n_i \sim \mathcal{N}(0, N_o/2)$, all i.

$$p(\mathbf{r}/\mathbf{s}_k) = \frac{1}{(\pi N_o)^{N/2}} e^{-\frac{1}{N_o}(r_k - \sqrt{E_s})^2} \prod_{i \neq k} e^{-\frac{1}{N_o} r_i^2}$$

and similarly for $p(\mathbf{r}/\mathbf{s}_i)$ for any i. Substituting into (11),

$$\begin{aligned} p(\mathcal{E}/\mathbf{s}_k) \leq & \int_{r_1} \cdots \int_{r_n} \left(\frac{1}{(\pi N_o)^{N/2}} e^{-\frac{1}{N_o}(r_k - \sqrt{E_s})^2} \right)^{\frac{1}{1+\mu}} \left(\prod_{i \neq k} e^{-r_i^2/N_o} \right)^{\frac{1}{1+\mu}} \\ & \times \left(\sum_{i \neq k} \left(\frac{1}{(\pi N_o)^{N/2}} e^{-\frac{1}{N_o}(r_i - \sqrt{E_s})^2} \prod_{j \neq i} e^{-r_j^2/N_o} \right)^{\frac{1}{1+\mu}} \right]^{\mu} dr_1 \cdots dr_N \end{aligned}$$

After some manipulation we obtain with $y_i = r_i / \sqrt{N_o/2}$

$$\begin{aligned} p(\mathcal{E}/\mathbf{s}_k) \leq & e^{-E_s/N_o} \int_{y_1} \cdots \int_{y_N} \left(\prod_{i=1}^{N} \frac{1}{\sqrt{2\pi}} e^{-y_i^2/2} \right) \times \\ & \exp\left[\sqrt{\frac{2E_s}{N_o}} \left(\frac{y_k}{1+\mu} \right) \right] \left(\sum_{i \neq k} \exp\left[\sqrt{\frac{2E_s}{N_o}} \left(\frac{y_i}{1+\mu} \right) \right] \right)^{\mu} dy_1 \cdots dy_N \end{aligned}$$

Note that $\prod_{i=1}^{N} \frac{1}{\sqrt{2\pi}} e^{-y_i^2/2}$ is a joint Gaussian density of the independent random variables $y_1, y_2, \ldots, y_N$. We may express the integral in terms of expectation by:

$$p(\mathcal{E}/\mathbf{s}_k) \leq e^{-E_s/N_o} E[g(y_k)] E\left[\left(\sum_{i \neq k} g(y_i) \right)^{\mu} \right] \tag{12}$$

where $g(z) \equiv \exp\left[\sqrt{\frac{2E_s}{N_o}}\left(\frac{z}{1+\mu}\right)\right]$.

For $0 \leq \mu \leq 1$, the function ξ^μ is a convex $\cap$ function of ξ. By Jensen's inequality, which says that for any convex $\cap$ function $h(\xi)$ of ξ,

$$E[h(\xi)] \leq h(E[\xi])$$

For the function ξ^μ where $\xi = \left(\sum_{i \neq k} g(y_i)\right)$, we have that

$$E\left[\left(\sum_{i\neq k} g(y_i)\right)^\mu\right] \leq \left(E\left[\sum_{i\neq k} g(y_i)\right]\right)^\mu = \left(\sum_{i\neq k} E[g(y_i)]\right)^\mu$$

Because all the y's are identically distributed, we have with substitution into (12),

$$\begin{aligned} p(\mathcal{E}/\mathbf{s}_k) &\leq e^{-E_s/N_o}(M-1)^\mu (E[g(y_1)])^{1+\mu} && (13)\\ E[g(y_1)] &= \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-y_1^2/2} e^{\sqrt{E_s/N_o}\left(\frac{y_1}{1+\mu}\right)} dy_1 && (14)\\ &= \exp\left[\frac{E_s}{N_o}\left(\frac{1}{1+\mu}\right)^2\right] \end{aligned}$$

Finally, we obtain by substitution of (14) into (13),

$$\begin{aligned} P(\mathcal{E}/\mathbf{s}_k) &\leq (M-1)^\mu e^{-E_s/N_o} e^{E_s/N_o\left(\frac{1}{1+\mu}\right)} && (15)\\ &= (M-1)^\mu e^{-(E_s/N_o)(\mu/1+\mu)}, \quad 0 \leq \mu \leq 1 \end{aligned}$$

We can drop the conditioning on $\mathbf{s}_k$ since the RHS is independent of k. Note that $\mu = 1$ indeed gives the U-B bound already derived for orthogonal signals.

Now we minimize the bound for $0 \leq \mu \leq 1$. First, however, we define the source rate in bits per second as

$$R \doteq \frac{1}{T}\log_2 M \text{ bits/second}$$

and overbound $M-1$ by M. With these factors

$$\begin{aligned} P(\mathcal{E}/\mathbf{s}_k) &= P(\mathcal{E}) < 2^{RT\mu} e^{-(E_s/N_o)(\mu/1+\mu)} \\ &= e^{-(RT\ln 2)\mu - (E_s/N_o)(\mu/1+\mu)} \end{aligned}$$

Let $E_s/N_oT = P_s/N_o \equiv C_\infty$ and $R \ln 2 = R'$ nats/sec.

$$P(\mathcal{E}) < \exp -T \left[C_\infty \left(\frac{\mu}{1+\mu} \right) - R'\mu \right]$$

You can check by the nonpositivity of the second derivative that the bracketed term in the exponent is convex $\cap$ for $\mu \geq 0$. Therefore, it has a unique maximum which may be found by setting its first derivative to zero. This maximum minimizes the bound on $P(\mathcal{E})$.

$$\frac{d[\ ]}{d\mu} = C_\infty \left[\frac{1}{1+\mu} - \frac{\mu}{(1+\mu)^2} \right] - R' = 0$$

Solving for μ, $\mu = -1 \pm \sqrt{C_\infty/R'}$. For $\mu \geq 0$, we must take the + sign.

$$\mu = \sqrt{\frac{C_\infty}{R'}} - 1$$

Note that if $C_\infty/R' > 4, \mu > 1$ and if $C_\infty/R < 1, \mu < 0$. The maximum is inside the unit interval if $C_\infty/R' \leq 4$ or $1/4 \leq R'/C_\infty \leq 1$. For $R'/C_\infty < 1/4$, the maximum occurs at $\mu > 1$, which is forbidden for our bound. Since [ ] is convex $\cap$, it increases monotonically with μ when the maximum occurs at $\mu > 1$. Its maximum value within the permitted values is therefore at $\mu = 1$. So for $0 \leq R'/C_\infty < 1/4$, we evaluate [ ] at $\mu = 1$ to obtain $[\ ]_{\mu=1} = 1/2C_\infty - R'$. Substituting $\mu = \sqrt{C_\infty/R'} - 1$ for the range $1/4 \leq R'/C_\infty \leq 1$, we have $[\ ] = (\sqrt{C_\infty} - \sqrt{R'})^2$. So we can express the bound as:

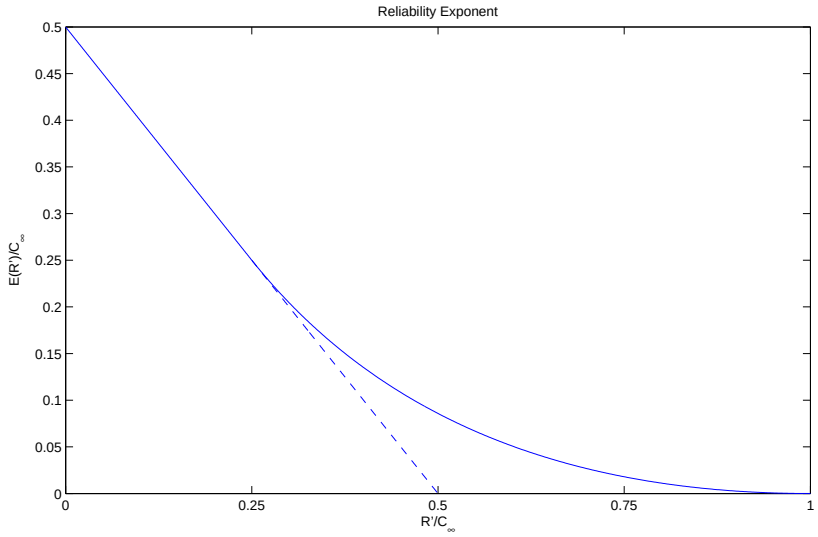
$$P(\mathcal{E}) < e^{-TE(R')} \tag{16}$$

where

$$E(R') = \begin{cases} \frac{1}{2}C_\infty - R', & 0 \leq \frac{R'}{C_\infty} < \frac{1}{4} \\ (\sqrt{C_\infty} - \sqrt{R'})^2, & \frac{1}{4} \leq \frac{R'}{C_\infty} \leq 1 \end{cases}$$

The exponent $E(R')$ is plotted below.

The larger $E(R')$ is for a given rate, the smaller the possible probability of error. $E(R')$ is called the reliability function. Note particularly that $E(R') > 0$ for $R' < C_\infty$. Therefore, for any rate $R' < C_\infty$, the probability of error can be made arbitrarily small for T sufficiently large. The maximum rate $C_\infty = P_s/N_o$ nats/second or $P_s/N_o \ln 2$ bits/second is a factor of 2 larger



than the union bound's maximum rate derived earlier (see figure). The rate C_∞ is actually the true upper limit for arbitrarily low probability of error. The subscript of infinity pertains to the lack of constraint on bandwidth for orthogonal signals (or codewords). The bandwidth W must exceed one-half the number of dimensions per second 0, i.e.,

$$W \geq \frac{N}{2T} = \frac{1}{2}D$$

and $N = M = 2^{RT}$. As $T \to \infty$, the bandwidth W grows exponentially toward infinity by $W \geq \frac{1}{2T}2^{RT}$.

The Random Coding Bound

For orthogonal codewords, N signals means N dimensions and leads to unconstrained bandwidth. For a hypercube of N dimensions, there are 2^N vertices and hence 2^N possible signal points or what we shall call codewords. (The collection of signal points is called a code.) If you fill the vertices, then the number of signals is

$$M = 2^N = 2^{RT} \text{ and } N = RT$$

Here the rate R in bits/sec equals D, the number of dimensions per second. Since we can make $D = \frac{N}{T}$ grow linearly with bandwidth by $D \approx 2W$, W grows linearly with N for fixed T or we fix W when we fix the rate R as T grows large. Unfortunately, when $R = D$, the available vertices are filled and $P(\mathcal{E}) \to 1$ as $T \to \infty$. The reason is that the nearest neighbor distance remains fixed and the number of nearest neighbors equals $N = RT$ which grows linearly with T. One possible remedy is to let R be strictly less than D ($R < D$) by filling only a fraction of the available vertices. Then the fraction

$$\frac{2^{RT}}{2^{DT}} = 2^{-(D-R)T}$$

goes to zero as T grows larger. So, the nearest neighbors are, on the average, not growing with T. The same argument holds if we allow more than $Q = 2$ values in each dimension. If each dimension allows the same Q values, then there are Q^N possible vertices to fill. The number of available bits per dimension is now $\log_2 Q$ instead of just 1. We shall concentrate on codeword vectors

$$\mathbf{s}_j = (s_{ij}, s_{2j}, ..., s_{Nj}) \quad j = 1, 2, ..., M = 2^{RT}$$

where the components s_{ij} can take any one of Q possible values (levels) $\{a_1, a_2, \ldots, a_Q\}$.

When one tries to calculate a probability of error for any single distribution of $M = 2^{RT}$ codewords using among Q^N vertices, it is virtually impossible. Shannon found an ingenious circumvention of this dilemma. One can consider the ensemble of all possible distributions (codes) and calculate the average probability of error. Then there exists at least one code whose error of probability equals the average. This artifice, called **random coding**, will be our strategy in deriving an upper bound on the average of the error probability over an ensemble of possible codes selected in a particular way.

Consider a collection of communication systems which are identical except for the code or signal set $\{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_M\}$. Since each codeword $\mathbf{s}_j$ has N components of Q possible values, there are Q^N possible choices for each $\mathbf{s}_j, j = 1, 2, \ldots, M$. Hence there are $(Q^N)^M$ possible signal sets or codes. Of course, some of them are patently absurd, such as those consisting of M identical codewords. We shall include them in our possibilities, nevertheless. So we have Q^{NM} communication systems which are identical except that each has a different code. We shall calculate the average probability of error

for these Q^{NM} systems. Let P_ℓ equal the probability of error associated with the ℓth code, $\ell = 1, 2, \ldots, Q^{NM}$, i.e., $P_\ell = P(\mathcal{E}/\{\mathbf{s}_j\}_\ell)$. If each code (or system) is equally likely, the average error probability for all Q^{NM} codes is

$$\overline{P(\mathcal{E})} = \frac{1}{Q^{NM}} \sum_{\ell=1}^{Q^{NM}} P_\ell \tag{17}$$

The ℓth code $\{\mathbf{s}_j\}_\ell$ will henceforth be denoted by C_ℓ, so that $P_\ell = P(\mathcal{E}/C_\ell)$. If the codes are not equally likely, we can express $\overline{P(\mathcal{E})}$ in terms of the code probabilities $P(C_\ell) = P(\{\mathbf{s}_j\}_\ell)$ as

$$\overline{P(\mathcal{E})} = \sum_{\ell=1}^{Q^{NM}} P(\mathcal{E}/C_\ell) P(C_\ell)$$

Now let us assume that in all our systems the kth message m_k which uniquely corresponds to $\mathbf{s}_k$ is sent. The probability of error given the codeword $\mathbf{s}_k$ of the ℓth code C_ℓ is denoted $P(\mathcal{E}/C_\ell, \mathbf{s}_k)$. The average error probability given that the $\mathbf{s}_k$ codeword is sent for every system is

$$\overline{P(\mathcal{E}/\mathbf{s}_k)} = \sum_{\ell=1}^{Q^{NM}} P(\mathcal{E}/C_\ell, \mathbf{s}_k) P(C_\ell) \tag{18}$$

We assume maximum likelihood decoding in every receiver. Therefore, we can apply the Gallager bound in (11) to $P(\mathcal{E}/C_\ell, \mathbf{s}_k)$.

$$P(\mathcal{E}/\mathbf{s}_{k,\ell}) < \int_{\mathbf{r}} (p/\mathbf{r}/\mathbf{s}_{k,\ell}))^{\frac{1}{1+\mu}} \left[\sum_{i \neq k} p(\mathbf{r}/\mathbf{s}_{i,\ell})^{\frac{1}{1+\mu}} \right]^{\mu}, \quad \mu \geq 0.$$

where we have used $\mathbf{s}_{k,\ell}$ to denote the kth codeword of the ℓth code C_ℓ. Substituting into (18),

$$\overline{P(\mathcal{E}/\mathbf{s}_k)} < \sum_{\ell=1}^{NM} P(C_\ell) \int_{\mathbf{r}} p(\mathbf{r}/\mathbf{s}_{k,\ell})^{\frac{1}{1+\mu}} \left[\sum_{i \neq k} p(\mathbf{r}/\mathbf{s}_{i,\ell})^{\frac{1}{1+\mu}} \right]^{\mu} d\mathbf{r} \quad \mu \geq 0 \tag{19}$$

The code C_ℓ is the collection of M codewords $\{\mathbf{s}_{1,\ell}, \mathbf{s}_{2,\ell}, \mathbf{s}_{3,\ell}, ..., \mathbf{s}_{\mu,\ell}\}$. We select the codewords of every code independently and at random from the ensemble of all possible codewords. Therefore,

$$P(C_\ell) = P(\{\mathbf{s}_{1,\ell}, \mathbf{s}_{2,\ell}, ..., \mathbf{s}_{M,\ell}\}) = P(\mathbf{s}_{1,\ell}) P(\mathbf{s}_{2,\ell}) ... P(\mathbf{s}_{M,\ell})$$

and for every ℓ, $\mathbf{s}_{j,\ell}$, $j = 1, 2, ..., M$ ranges over the set of all possible Q^N N-tuple code vectors. If they are equiprobable,

$$P(\mathbf{s}_{j,\ell}) = \frac{1}{Q^N} \quad \text{for all } j \text{ and } \ell$$

and $P(C_\ell) = 1/Q^{NM}$, consistent with our expression in (17). We are assuming for now that the codes and codewords are equally probable, but we are carrying out the development in general, because we shall later relax that rather arbitrary constraint.

In the summation over all possible codes in (19), we mean the sum over all possible codewords $\mathbf{s}_1, \mathbf{s}_2$, etc. So we can drop the ℓ subscript notation and replace the sum over ℓ by the sum over all possible 1st, 2nd, etc. codewords. So $\overline{P(\mathcal{E}/\mathbf{s}_k)}$ becomes through the independent and random codeword selections,

$$\begin{aligned}
\overline{P(\mathcal{E}/\mathbf{s}_k)} &< \sum_{\mathbf{s}_1}\sum_{\mathbf{s}_2}\cdots\sum_{\mathbf{s}_M} P(\mathbf{s}_1)P(\mathbf{s}_2)\cdots P(\mathbf{s}_M)\int_{\mathbf{r}} p(\mathbf{r}/\mathbf{s}_k)^{\frac{1}{1+\mu}}\left[\sum_{i\neq k} p(\mathbf{r}/\mathbf{s}_i)^{\frac{1}{1+\mu}}\right]^{\mu} d\mathbf{r} \\
&= \int_{\mathbf{r}} \sum_{\mathbf{s}_k} P(\mathbf{s}_k)p(\mathbf{r}/\mathbf{s}_k)^{\frac{1}{1+\mu}} \prod\left(\sum_{\mathbf{s}_1} P(\mathbf{s}_i)\right)\left[\sum_{i\neq k} p(\mathbf{r}/\mathbf{s}_i)^{\frac{1}{1+\mu}}\right] d\mathbf{r} \qquad (20)
\end{aligned}$$

for $\mu \geq 0$. For $0 \leq \mu \leq 1$, ξ^μ is a convex $\cap$ function of ξ. We again apply Jensen's inequality to $[\ ]^\mu$ in (20) above:

$$\begin{aligned}
\sum_{\mathbf{s}_1}\cdots\sum_{\mathbf{s}_M} P(\mathbf{s}_1)\left[\sum_{i\neq k} p(\mathbf{r}/\mathbf{s}_i)^{\frac{1}{1+\mu}}\right]^{\mu} &= E\left[\sum_{i\neq k} p(\mathbf{r}/\mathbf{s}_i)^{\frac{1}{1+\mu}}\right]^{\mu} \\
&\leq \left[E\sum_{i\neq k} p(\mathbf{r}/\mathbf{s}_i)^{\frac{1}{1+\mu}}\right]^{\mu} \\
&= \left(\sum_{i\neq k}\sum_{\mathbf{s}_i} p(\mathbf{s}_i)p(\mathbf{r}/\mathbf{s}_i)^{\frac{1}{1+\mu}}\right)^{\mu} \qquad (21)
\end{aligned}$$

The $\mathbf{s}_i$'s range over the set of all Q^N vectors and are identically distributed. The expectations $\sum_{\mathbf{s}_i} P(\mathbf{s}_i)p(\mathbf{r}/\mathbf{s}_i)^{1/1+\mu}$ for all i (including k) take the same value. We can express the bound in (20) using (21) as:

$$\overline{P(\mathcal{E}/\mathbf{s}_k)} < (M-1)^{\mu} \int_{\mathbf{r}} \left(\sum_{\mathbf{s}} P(\mathbf{s}) p(\mathbf{r}/\mathbf{s})^{\frac{1}{1+\mu}} \right)^{\frac{1}{1+\mu}} d\rho, \quad 0 \leq \mu \leq 1 \qquad (22)$$

Noting that the bound is independent of $\mathbf{s}_k$, $\overline{P(\mathcal{E}/\mathbf{s}_k)} = \overline{P(\mathcal{E})}$ and the final result is

$$\overline{P(\mathcal{E})} < (M-1)^{\mu} \int_{\mathbf{r}} \left(\sum_{\mathbf{s}} P(\mathbf{s}) p(\mathbf{r}/\mathbf{s})^{\frac{1}{1+\mu}} \right)^{1+\mu} d\mathbf{r}, \quad 0 \leq \mu \leq 1 \qquad (23)$$

where $\mathbf{s}$ denotes a general vector codeword.

The result for $\overline{P(\mathcal{E})}$ in (23) is quite general. It holds for general channels with memory, discrete or continuous. If the outputs $\mathbf{r}$ are discrete, then the integration is replaced with a summation and the conditional density $p(\mathbf{r}/\mathbf{s})$ is replaced by a conditional probability mass function $P(\mathbf{r}/\mathbf{s})$.

We shall now apply (23) to the case of a memoryless channel. A channel is memoryless if a single output symbol depends only on the current input symbol and no other past or future symbols. Mathematically the definition is

$$p(\mathbf{r}/\mathbf{s}) = p(r_1/s_1)p(r_2/s_2)\cdots p(r_N/s_N)$$

We also assume now that the input codeword $\mathbf{s}$ consists of components which have been selected independently and at random from the levels $\{a_1, a_2, ..., a_Q\}$ so that

$$\begin{aligned} P(\mathbf{s}) &= P(s_1)P(s_2)...P(s_N), \\ & \qquad s_i \in \{a_1, a_2, \ldots, a_Q\}, \quad \imath = 1, 2, \ldots, N \end{aligned}$$

when all the levels are equally probable, $P(s_i) = 1/Q$ and $P(\mathbf{s}) = 1/Q^N$, consistent with previous developments. Using the assumptions of a memoryless channel and independently selected codeword components in (23), we obtain

$$\overline{P(\mathcal{E})} < (M-1)^{\mu} \int_{r_1} \cdots \int_{r_N} \left(\sum_{s_1} \cdots \sum_{s_N} \prod_{i=1}^{N} P(s_i) p(r_i/s_i) \right)^{\frac{1}{1+\mu}} dr_1 ... dr_N$$

$$= (M-1)^{\mu} \int_{r_1} ... \int_{r_N} \left(\prod_{i=1}^{N} \sum_{s_i} P(s_i) p(r_i/s_i)^{\frac{1}{1+\mu}} \right)^{1+\mu} dr_1 ... dr_N \quad (24)$$

$$= (M-1)^{\mu} \left(\int_{\rho} \left(\sum_{s} P(s) p(r/s)^{\frac{1}{1+\mu}} \right)^{1+\mu} dr \right)^{N}, \quad 0 \leq \mu \leq 1.$$

The last step in (24) follows from the identical distributions of the codeword components and the identical ranges of the components of the output vector $\mathbf{r} = (r_1, ..., r_N)$.

We now relax the requirement of equiprobable levels and let $P(s)$ be arbitrary. What we are trying to do is overbound the probability of error of the best code by the average over the ensemble. Clearly, the probability of error of the best code is always overbounded by the average regardless of the probability of occurrences of the codes in the code ensemble. In mathematical terms,

$$\min_{\ell} P(\mathcal{E}/C_\ell) \leq \sum_{\ell} P(C_\ell) P(\mathcal{E}/C_\ell) = \overline{P(\mathcal{E})}$$

We have selected our code by first selecting the components of every codeword independently and at random from the set of levels. Secondly each codeword is chosen independently in turn in the same way. Ultimately, the probability of a code depends on the level probabilities $P(s)$. If we make $P(s)$ arbitrary we make $P(C_\ell)$ arbitrary. What we wish to do is choose $P(s)$ to minimize the bound.

Let us now put rate into the picture. We overbound $M-1$ by $M = e^{R_N N}$, where R_N is the rate in nats per dimensions, i.e.,

$$R_N = \frac{1}{N} \ln M \text{ nats/dimension}$$

With these substitutions, (24) may be expressed as:

$$\overline{P(\mathcal{E})} < e^{-N[E_o(\mu, \mathbf{P}) - \mu R_N]}, \quad 0 \leq \mu \leq 1 \quad (25)$$

where $E_o(\mu, \mathbf{P})$ is defined to be

$$E_o(\mu, \mathbf{P}) = -\ln \int_{r} \left(\sum_{s} P(s) p(r/s)^{\frac{1}{1+\mu}} \right)^{1+\mu} dr$$

and $\mathbf{P}$ is the vectors of probabilities $(P(a_1), P(a_2), ..., P(a_Q))$.

We can obtain the tightest bound by maximizing the bracketed term in the exponent over $0 \leq \mu \leq 1$ and the level probabilities $P(s)$ denoted by $\mathbf{P}$. The tightest bound is

$$\begin{aligned} \overline{P(\mathcal{E})} &< e^{NE(R_N)} \\ E(R_N) &= \max_{0\leq\mu\leq 1} \max_{\mathbf{P}} [E_o(\mu, \mathbf{P}) - \mu R_N] \end{aligned} \tag{26}$$

If we can show that $E_o(\mu, \mathbf{P}) - \mu R_N$ is positive for some μ and $\mathbf{P}$, then $\overline{P(\mathcal{E})} \to 0$ as $N \to \infty$. If the average error probability over all codes goes to zero with N increasing, then there is at least one code attaining the average error probability.

In general it is quite difficult to carry out the double maximization indicated above. Instead, let us choose values for μ and, perhaps, $\mathbf{P}$ and demonstrate that $E_o(\mu, \mathbf{P}) - \mu R_N$ is positive for a certain range of rates R_N. The first case we examine is a two-level alphabet with equiprobable levels, i.e., the hypercube with equiprobable components in each dimension. Arbitrarily set $\mu = 1$. Recall that $\mu = 1$ gives the Union-Bhattacharyya bound.

N-Dimensional Hypercube: $Q = 2, P(a_1) = P(a_2) = \frac{1}{2}, a_1 = a_2 = \sqrt{E_N}$

AWGN Channel: $p(\rho/s) = \frac{1}{\sqrt{\pi N_o}} e^{-\frac{1}{N_o}(\rho - s)^2}$

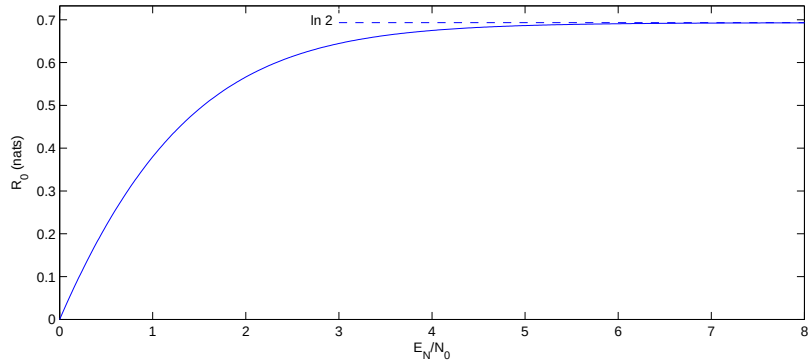
$\mu = 1$ and E_N is the energy/dimension

Evaluating $E_o(\mu, \mathbf{P})$ in (25),

$$\begin{aligned} E_o\left(1, \left\{\frac{1}{2}, \frac{1}{2}\right\}\right) &= -\ln \int_{-\infty}^{\infty} \left(\frac{1}{2} \left(\frac{1}{\sqrt{\pi N_o}} \right)^{\frac{1}{2}} e^{-\frac{1}{2N_o}(r - \sqrt{E_n})^2} + \frac{1}{2} \left(\frac{1}{\sqrt{\pi N_o}} \right)^{\frac{1}{2}} e^{-\frac{1}{2N_o}(r + \sqrt{E_N})^2} \right) dr \\ &= -\ln \frac{1}{4\sqrt{\pi N_o}} \int_{-\infty}^{\infty} \left(e^{-\frac{1}{N_o}(r - \sqrt{E_N})^2} + e^{-\frac{1}{N_o}(r + \sqrt{E_N})^2} + 2e^{-\frac{E_N}{N_o}} e^{-\frac{r^2}{N_o}} \right) dr \\ &= -\ln \frac{1}{4} \left(1 + 1 + 2e^{-\frac{E_N}{N_o}} \right) \\ &= \ln \frac{2}{1 + e^{-\frac{E_N}{N_o}}} \equiv R_o \text{ nats/dimension} \end{aligned}$$

For $\mu = 1$,

$$\overline{P(\mathcal{E})} < e^{-N(R_o - R_N)}, \quad R_o = \ln \frac{2}{1 + e^{-\frac{E_N}{N_o}}}$$



If $R_N < R_o$, $\overline{P(\mathcal{E})} \to 0$, as $N \to \infty$. The most R_o can be is $\ln 2$ nats or 1 bit per dimension for large E_N/N_o. That maximum rate represents the filling of the available vertices of the hypercube with codewords. In that case we have already seen that $P(\mathcal{E}) \to 1$ as $N \to \infty$. So the random code filling only a fraction of the vertices does produce at least one code with arbitrarily low $P(\mathcal{E})$ for sufficiently large N. We must have a rate R_N less than R_o which depends on E_N/N_o.

One expects that we should be able to signal at higher rates than 1 bit/dimension for large E_N/N_o if we allow multi-level codeword components. Then the vertices are saturated at $\log_2 Q$ bits/dimension. We expect then to be able to signal at close to $\log_2 Q$ bits/dimension at large E_N/N_o Q-level codeword components. We now derive the $\overline{P(\mathcal{E})}$ bound for this case.

N-dimensions, Q-level components, $\mu = 1$

AWGN channel: $p(r/s) = \frac{1}{\sqrt{\pi N_o}} e^{-\frac{1}{N_o}(r-s)^2}$

$s \in \{a_1, a_2, ..., a_Q\}$

Evaluating $E_o(1, \mathbf{P})$ in (25):

$$\begin{aligned} R_o &\equiv E_o(1, \mathbf{P}) \\ &= \ln \int_r \left(\sum_{i=1}^{Q} P(a_i) p(r/a_i)^{\frac{1}{2}} \right)^2 dr \\ &= -\ln \int_\rho \left(\sum_{i=1}^{Q} P(a_i) \frac{1}{(\pi N_o)^{\frac{1}{4}}} e^{-\frac{1}{2N_o}(r-a_i)^2} \right) dr \end{aligned}$$

$$= -\ln \int_\rho \sum_{i=1}^{Q} \sum_{i=j}^{Q} \frac{1}{(\pi N_o)^{\frac{1}{2}}} P(a_i)P(a_j) e^{-\frac{1}{2N_o}[(r-a_i)^2+(r-a_j)^2]} dr$$

$$R_o = -\ln \sum_{i=1}^{Q} \sum_{j=1}^{Q} P(a_i)P(a_j) e^{-\frac{1}{4N_o}(a_i-a_j)^2}$$

and

$$\overline{P(\mathcal{E})} < e^{-N(R_o-R_N)}$$

Wozencraft and Jacobs have calculated R_o versus E_N/N_o for equally spaced levels with the level probabilities $P(a_i)$ all equal and also optimized. Both sets of curves for different Q show the anticipated saturation at $\log_2 Q$. For a given E_N/N_o one can choose a value of Q that yields the largest R_o. Indeed one can certainly signal at rates $R_N < R_o$, where R_o for a given E_N/N_o can be maximized by choosing a large enough alphabet size Q. Again, for $R_N < R_o$, there exists a code with arbitrarily low $P(\mathcal{E})$ for N sufficiently large. The probability of choosing such a code by our random selection process is high, as we now show. Let $\overline{P(\mathcal{E})} < \delta$ and $P(k\delta)$ be the probability of choosing a code C such that $P(\mathcal{E}/C) \geq k\delta$. Then

$$P(k\delta) = \sum_{C_i P(\mathcal{E}/C) \geq k\delta} P(C) \leq \sum_{\text{all } C} \frac{P(\mathcal{E}/C)}{k\delta} P(C) = \frac{1}{k\delta}\overline{P(\mathcal{E})} < \frac{\delta}{k\delta} = \frac{1}{k}$$

The probability of choosing a code with error probability greater than k times the upper bound on the average is less than $1/k$.

Receiver Quantization

When the receiver must meet the task of computing $\mathbf{r} \cdot \mathbf{s}_i$ for all $i = 1, 2, ..., M$ so as to make a decision, an inordinate amount of storage and computation is required. The order of complexity is $NM = N2^{R_N N} = N2^{RT}$. The components of the received vector $\mathbf{r}$ are continuous ($r_o = \int_0^T r(t)\phi_j(t)dt$, $j = 1, 2, ..., N$) and it is always desirable to use a digital computer. For digital computations, a quantization is required on the components of $\mathbf{r}$. But we are interested in special purpose digital computers called decoders which can be simply implemented and operate on coarsely quantized components of $\mathbf{r}$. We first investigate the degradation imposed by the quantization of $\mathbf{r}$.

We assume that each component of $\mathbf{r}$ is quantized independently by the same quantization rule. That is,

$$r_j \to r'_j \quad j = 1, 2, ..., N$$

and each r_j^1 is a member of the discrete set of symbols $\{b_1, b_2, ..., b_Q\}$. The mapping from r_j to r'_j is given by the rule: if

$$x_{k-1} < r_j \leq x_k, \quad r_j^1 = b_k \quad k = 1, 2, ..., Q$$

$$x_o = -\infty, x_Q = +\infty$$

Probabilities may be assigned to the quantizer symbols by

$$P[r'_j = b_k] = P[x_{k-1} < r_j \leq x_k]$$

As $r_j = s_{ij} + n_j$, $j = 1, 2, ..., N$ for a given signal vector $\mathbf{s}_i = (s_i, s_{i2}, ..., s_{iN})$, the channel specifies the conditional probability density $p(r_j/s_{ij})$. Assume the components of the signal vector are one of A possible values, $a_1, a_2, ..., a_A$. We can calculate from known quantities the probability of a transition from a signal value a_ℓ to a quantizer output symbol b_h by

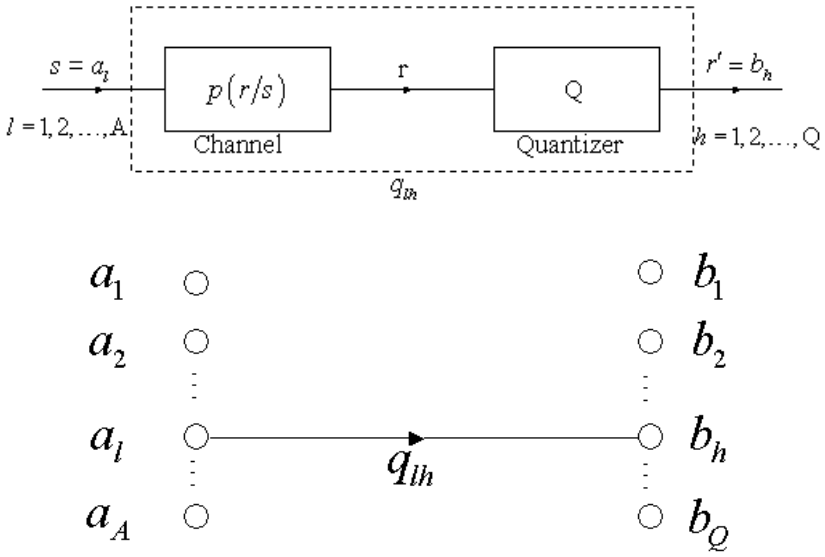
$$\begin{aligned} P(r'_j = b_h/s_{ij} = a_\ell) &= P(x_{n-1} < r_j \leq x_h/s_{ij} = a_\ell) \\ &= \int_{x_{h-1}}^{x_n} p(r_j/s_{ij} = a_\ell) dr_j, \\ &\quad j = 1, 2, \ldots, N; \ell = 1, 2, \ldots, A; h = 1, 2, \ldots, Q \end{aligned}$$

For example, the AWGN channel gives

$$p(r_j/s_{ij} = a_\ell) = \frac{1}{\sqrt{\pi N_o}} \exp -(r_j - a_\ell)^2$$

These transition probabilities

$$\begin{aligned} q_{\ell h} &\equiv P(r'_j = b_h/s_{ij} = a_\ell), \\ &\quad h = 1, 2, ..., Q, \quad \ell = 1, 2, ..., A \end{aligned} \tag{27}$$



define a new channel with discrete input and output, whereas the unquantized outputs gave a discrete input and continuous output

Because each component of **r** is operated on independently and identically by the quantization and is independent given the signal input (the original continuous channel is memoryless), the same set of transition probabilities $\{q_{\ell h}\}$ pertain to each component and the components r'_j are conditionally independent. The new channel for the transition from the signal vector $\mathbf{s}_i$ to the discrete output vector **r'** is memoryless, i.e.,

$$P(\mathbf{r'}/\mathbf{s}_i) = \prod_{j=1}^{N} P(r'_j/s_{ij})$$

We have here a situation where the random coding bound for memoryless channels is applicable. From (25) on page 15

$$\begin{aligned} \overline{P(\mathcal{E})} &< e^{-N[E_o(\mu,\mathbf{P})-\mu R_N]}, \quad 0 \le \mu \le 1 \\ E_o(\mu,\mathbf{P}) &= -\ln \textstyle\int_\rho \left[\sum_s P(s)(p(\rho/s))^{\frac{1}{1+\mu}}\right] d\rho \end{aligned}$$

Although stated explicitly for continuous output values ρ, we noted previously that the expressions are valid for discrete outputs when the integral

is replaced by a sum and the conditional probability density by a conditional probability mass function. So we express $E_o(\mu, \mathbf{P})$ alternatively as

$$E_o(\mu, \mathbf{P}) = -\ln \sum_{\rho} \left[\sum_{s} P(s)(P(\rho/s))^{\frac{1}{1+\mu}} \right]^{1+\mu}$$

Since s takes values $a_1, a_2, ..., a_A$ and ρ the symbols $b_1, b_2, ..., b_Q$, and $P(\rho/s) = P(\rho = b_h/s = a_\ell) = q_{\ell h}$, the above gives

$$E_o(\mu, \mathbf{P}) = -\ln \sum_{h=1}^{Q} \left[\sum_{\ell=1}^{A} P(a_\ell) q_{\ell h}^{\frac{1}{1+\mu}} \right]^{1+\mu} \tag{28}$$

Evaluating for $\mu = 1$ defines the rate R'_o (denoted by R_Q in some textbooks

$$R'_o = E_o(\mu = 1, \mathbf{P}) = -\ln \sum_{h=1}^{Q} \left[\sum_{\ell=1}^{A} P(a_\ell) \sqrt{q_{\ell n}} \right]^2 \tag{29}$$

as obtained in the textbook. For $\mu = 1$, the ensemble average probability of error is

$$\overline{P(\mathcal{E})} < e^{-N(R'_o - R_N)} \tag{30}$$

This result holds for all discrete input, discrete output memoryless channels as well as the specific case here of an independently quantized output of a memoryless channel.