Coding with Deletions + Insertions

Sequential Decoding for Binary Channel with Noise and Synchronization Errors

by R.G. Gallager

Lincoln Lab Group Report 2502
Sept. 61

UNCLASSIFIED

SEQUENTIAL DECODING FOR BINARY CHANNELS WITH NOISE AND SYNCHRONIZATION ERRORS

ABSTRACT

R. G. GALLAGER

LINCOLN LAB GROUP REPORT 2502
SEPT 61

Consider a channel for which the input is a sequence of binary digits and for which the output is the same sequence with each digit independently modified in the following way: with probability P_e, the digit is changed; with probability P_d, the digit is deleted from the sequence; and with probability P_i, the digit is replaced by two randomly chosen digits. The channel output gives no indication which digits were deleted or inserted.

It is shown that convolutional coding and sequential decoding can be applied, with minor modifications, to this channel and bounds are derived on computation and error probability analogous to the bounds for the Binary Symmetric Channel. More precisely, a computational cut-off rate, R_{comp}, is defined as

$$R_{comp} = 1 - 2 \log_2 [\sqrt{P_e} + \sqrt{P_d} + \sqrt{P_i} + \sqrt{1 - P_e - P_d - P_i}].$$

For code rates less than R_{comp} bits per digit, the average decoding computation in the incorrect subset grows more slowly than linearly with the coding constraint length, and the probability of decoding error decreases exponentially with constraint length. For $P_d = P_i = 0$, the above expression for R_{comp} reduces to that derived by Wozencraft and Reiffen for the Binary Symmetric Channel.

Introduction:

Coding theory in the past has dealt almost exclusively with the problem of correcting errors on noisy memoryless channels. There are now in existence a number of coding schemes that can be implemented with reasonable efficiency to provide virtually error-free communication on channels that fit the memoryless model. However, these schemes fail whenever a timing error is made, i.e., when the receiver interprets one position in a sequence as another.

In most digital communication systems, periodic synchronization pulses are transmitted to avoid timing errors, but these signals often require as much as half the total transmitted power. Such systems are not only inefficient, but also complicated by the synchronization circuitry. Furthermore, these systems still suffer occasional synchronization errors which can easily be the principal source of failure if coding is used for error correction.

In this paper it is shown that convolutional coding and sequential decoding can be modified to correct both noise errors and timing errors. The modification increases the decoding complexity somewhat, but it is quite possible that the over-all system complexity is reduced due to the elimination of synchronization signals. Unfortunately, some departure from physical reality is required to obtain an analytically simple model, but models closer to physical reality can be handled by the same techniques.

Channel Model

We assume a channel for which the input and output are sequences of binary digits. Each input digit is treated by the channel in one of four ways. First, with probability P_e the output digit is the opposite digit from the input. Second, with probability P_d the digit is deleted, but the receiver has no indication which digits are deleted. Third, with probability P_i the channel will insert two digits in place of the input digit, both random and independent of the input digit. Fourth, with probability $P_c = 1 - P_e - P_d - P_i$, the transmitted digit will pass through the channel unaltered. Finally, we assume that the channel treats each input digit with statistical independence. This assumption of independence is not good physically since, when the timing between transmitter and receiver is sufficiently bad to delete or insert a whole digit, it is also bad enough to cause many errors in the vicinity of that digit. If the correlation between these errors dies out after a few digits, the results should not be greatly altered.

It is unknown whether this model fits any real channels closely enough to be useful. On the other hand, these results clearly indicate that coding can be efficiently used on channels when noise disturbs the signal horizontally along the time axis as well as vertically along the amplitude axis. The difficulty is that we have quantized the time scale so grossly that a shift of one unit will take many bauds. In practice, sequential decoding could be used to track much smaller time variations, although the mathematical analysis would become much more difficult. This would essentially involve using coding to track the phase of the signal and would insure a certain amount of independence between additive noise errors and phase errors.

<u>Summary of Results:</u>

We will assume that binary information at the channel input is fed into a convolutional coder as described by Wozencraft and Reiffen.[1] The output of this device is then added, modulo two, to a pseudo-random sequence of 0's and 1's to obtain the coded input to the channel. Roughly, this random sequence is necessary to provide desirable distance characteristics between one coded sequence and shifted versions of other coded sequences. After this coded input is passed through the type of channel described in the previous section, a sequential decoder is used in much the same way as described in Reference 1. The principal differences are that the decoder tests for possible deletions and insertions and that it incorporates the pseudo-random sequences used by the coder into its generation of test coded sequences. The decoder is described in more detail in the next section. Using a typical convolutional code with this decoding scheme on the type of channel described above, we can prove the following results.

For transmission rates smaller than a computational cut-off rate, $R_{comp} = 1 - 2 \log_2 [\sqrt{P_e} + \sqrt{P_d} + \sqrt{P_i} + \sqrt{P_c}]$, the average amount of computation per digit required to reject the incorrect subset of the code structure grows more slowly than linearly with the constraint length of the code. It is interesting to observe that if $P_d = 0$ and $P_i = 0$, this equation for R_{comp} reduces to that derived in (1) for the Binary Symmetric Channel.

For transmission rates smaller than a lower bound to the channel capacity, $R \leq 1 + P_e \log_2 P_e + P_d \log_2 P_d + P_i \log_2 P_i + P_c \log_2 P_c$, the probability of error decreases exponentially with the constraint length and this exponent approaches that for the Binary Symmetric Channel as P_d and P_i approach 0.

Numerical Example

To provide an idea of the numbers involved in this work, assume a channel for which $P_e = 0.01$, $P_d = P_i = 0.0016$ and $P_e = 0.9868$. Also assume a transmission rate of 1/4 bit per digit and a constraint length of 500 digits. R_{comp} for this channel is then 0.534 bit per digit, and the bound on computation derived in Equation 33 gives an average computation on the incorrect subset of 6000 computations per digit. This is not very encouraging, but if one applies the bound in Reference 1 to a binary symmetric channel with the same rate and the same R_{comp}, one gets 690 computations per digit. Experimental data on the Binary Symmetric Channel indicates that the actual average computation is smaller by a factor of over 100. Thus, in practice, we might expect about 60 computations per digit on the channel with timing errors. Furthermore, the bounds derived here are considerably looser than those in Wozencraft and Reiffen,[1] so that 20 computations per digit might be a more realistic figure.

Let us compare these figures with a system in which synchronization signals are used to avoid sync errors and coding is used to correct errors. If half the power is used for synchronization, then we must use a transmission rate of 1/2 bit per digit in the code instead of 1/4. Applying the bound in Reference 1 to such a code, we get 3400 computations per digit, or perhaps in actual practice 34 computations per digit. Even after taking into account the more involved unit of computation for channels with timing errors, it is seen that roughly the same amount of computation is required in both cases. The probabilities of decoding error in the two cases are completely negligible (about 10^{-30} without synchronization and about 10^{-25} with synchronization), but synchronization errors may cause trouble in the system with synchronization signals.

These figures are sufficiently promising to indicate that the correction of timing errors by sequential decoding is a possibility that should at least be considered in a system using sequential decoding for error correction. To answer the question of specific application, however, some experimental simulation of such a system will undoubtedly be required.

Decoding Strategy

It will be assumed in what follows that the reader is reasonably familiar with the theory of sequential decoding as described by Wozencraft and Reiffen.[1] Assume, as in Reference 1, that the decoder has decoded the transmitted message correctly up to a certain point and is attempting to decode the next digit in the sequence. Assume further that the decoder knows which digit (or deletion) in the received sequence corresponds to the last digit decoded. This assumption will be discussed later.

Consider the set of possible transmitted sequences consistent with the already decoded digits as a tree structure branching out from the last decoded digit. The decoder now starts at the last decoded digit and traces out the various branches of the tree. At each length, n, the decoder compares the sequence it has generated with the received sequence. Whenever the transmission of this generated sequence appears too unlikely, in a sense to be defined later, the computer rejects the sequence, back tracks, and starts tracing out another sequence. The amount of computation does not become prohibitive in this procedure because whenever a sequence is rejected, all the code sequences that branch out from that set of initial digits are rejected. The principal difference between decoding for channels with sync errors and for simple Binary Symmetric Channels lies in the determination of when a sequence is too unlikely. Ideally, we would like to compute the probability of receiving the actual received sequence conditional on the transmission of the hypothesized transmitted sequence. However, this is computationally unattractive since many different combinations of deletions, insertions, and errors can transform a given sequence into the same received sequence. On the other hand, it is easy to calculate the probability of obtaining particular configurations of errors, deletions and insertions; and it turns out that it is easy to calculate the maximum of this probability over all configurations that transform a given transmitted sequence into a given received sequence. The decoder compares this maximum probability against a criterion at each length, n, and rejects the sequence when it falls below the criterion. All of the results here are based on this criterion and it is unknown how much better the probability of decoding error would be if maximum likelihood decoding were used instead.

Actually, instead of calculating the probability of the most probable configuration, we will calculate the negative of the logarithm of this quantity. For a configuration of E errors, D deletions, I insertions, and C correct digits, define

$$H_{n,m} = -E \ln P_e - D \ln P_d - I \ln P_i - C \ln P_c \qquad (1)$$

where $n = E + D + I + C$ is the number of considered transmitted digits and $m = n + I - D$ is the number of considered received digits. Note that m depends on I and D as well as n and can range from 0 to 2n. Suppose, for a given transmitted sequence and a given received sequence, that we know the minimum value of $H_{n-1,m}$, denoted MIN $(H_{n-1,m})$ for a particular n and for all m, $0 \leq m \leq 2n - 2$. Then MIN $(H_{n,m})$ will be the smallest of the following three quantities:

$$\text{MIN}\,(H_{n-1,m}) - \ln P_d \qquad (2\text{-a})$$

$$\text{MIN}\,(H_{n-1,m-2}) - \ln P_i \qquad (2\text{-b})$$

$$\text{MIN}\,(H_{n-1,m-1}) - \begin{Bmatrix} \ln P_c \\ \ln P_e \end{Bmatrix} \qquad (2\text{-c})$$

where $\ln P_c$ is to be used if the m th received digit is the same as the n th transmitted digit, and $\ln P_e$ is to be used otherwise.

This rule is verified by noting that Equation 2-a is the minimum of $H_{n,m}$ for all configurations ending with a deletion. Likewise, Equation 2-b is the minimum of $H_{n,m}$ for all configurations ending with an insertion, and 2-c is the minimum of $H_{n,m}$ for all configurations ending with either a correct transmission or an error. Note that we must not assume a final error if the n th transmitted digit is the same as the m th received digit, and we must not assume a final correct transmission otherwise. Then 2-a, 2-b, and 2-c exhaust all possibilities and MIN $(H_{n,m})$ is the smallest of the three.

Thus the decoder at each length n will use Equation 2 to compute MIN $(H_{n,m})$ for each m; compare this with the criterion and store MIN $(H_{n,m})$ for each m that satisfies the criterion. For convenience we will define this combination of 3 addition , a 4-way comparison, and a store as one computation. Note that MIN $(H_{n,m})$ need only be computed for those n, m, such that not all of the quantities MIN $(H_{n,m})$, MIN $(H_{n-1,m-1})$ and MIN $(H_{n-1,m-2})$ have been rejected.

In the sections that follow, we will find bounds on the number of different MIN $(H_{n,m})$ that have to be computed as a function of n and use this to bound the average computation on the entire incorrect subset. Finally, these same bounds will be used to bound the probability of decoding error with such a scheme.

Bound on Computation

It is obvious that the number of computations that must be performed to reject a sequence in the incorrect subset depends very strongly on the criterion for rejection of MIN $(H_{n,m})$. The smaller this criterion, the faster the sequences in the incorrect subset will be rejected, and the smaller the overall amount of computation will be. Unfortunately, a small criterion also increases the probability of rejecting the correct sequence.

To avoid this difficulty, we define an ordered set of criteria $H_j(n)$ each defined for each n less than the constraint length, n_t, such that

$$H_o(n) < H_1(n) < H_2(n) < \ldots \text{ for all } n < n_t.$$

In decoding a digit, the decoder starts at the 0 th criterion and if both subsets are rejected on this criterion, the decoder moves to the first criterion and so forth until some sequence is accepted out to length n_t. At this point the first digit of that sequence is decoded and the decoder moves on to the next branch point of the tree to decode the next digit. Let $\overline{N}$ be the average number of computations necessary on the incorrect subset before decoding a digit, and let $\overline{N}_j$ be the average number of computations to reject the jth criterion in the incorrect subset. Then,

$$\overline{N} = \overline{N}_o + \sum_{j=1}^{j_{max}} \overline{N}_j \Pr[\text{both subsets rejected on } j-1 \text{ criterion}].$$

The probability of rejecting the transmitted sequence is an upper bound to that of rejecting both subsets so that

$$\overline{N} \leq \overline{N}_o + \sum_{j=1}^{j_{max}} \overline{N}_j \Pr[\text{rejecting transmitted sequence on } j-1 \text{ criterion}]. \quad (3)$$

First a bound will be found for the probability of rejecting the transmitted sequence in terms of the criteria. Then this bound will be used to set the criteria in terms of a desired probability of rejection. Finally, in terms of these criteria, $\overline{N}_j$ will be bounded by averaging over the ensemble of all convolution codes.

Let $H_t(n)$ be the value of $H_{n,m}$ for the set of errors, deletions, and insertions that actually occur in transmission. $H_t(n)$ is then the sum of n identically distributed independent random variables. This random variable is $-\ln P_e$ with probability P_e, $-\ln P_d$ with probability P_d, $-\ln P_i$ with probability P_i, and $-\ln P_c$ with probability P_c. The Chernov bound [2] then states that for $s > 0$,

$$\Pr\left[H_t(n) \geq H_j(n)\right] \leq \exp -n\left[s\mu'(s) - \mu(s)\right] \tag{4}$$

when $\mu(s)$ is the semi-invariant generating function of the above random variable,

$$\mu(s) = \ln\left[P_e e^{-s \ln P_e} + P_d e^{-s \ln P_d} + P_i e^{-s \ln P_i} + P_c e^{-s \ln P_c}\right]$$

$$= \left[P_e^{1-s} + P_d^{1-s} + P_i^{1-s} + P_c^{1-s}\right] \tag{5}$$

and where

$$\mu'(s) = \frac{d\mu(s)}{ds} = \frac{1}{n} H_j(n) \tag{6}$$

Equations 4, 5, and 6 relate $H_j(n)$ and $\Pr\left[H_t(n) \geq H_j(n)\right]$ parametrically through s. It can be shown [2] that for $s > 0$, both $\mu'(s)$ and $s\mu'(s) - \mu(s)$ are increasing with s, and thus increasing with each other. Furthermore, $\mu'(0) = \frac{1}{n}\overline{H_t(n)}$ and $\mu'(\infty) = -\ln(P_{min})$ where P_{min} is the smallest of the 4 probabilities (see Figure 1).

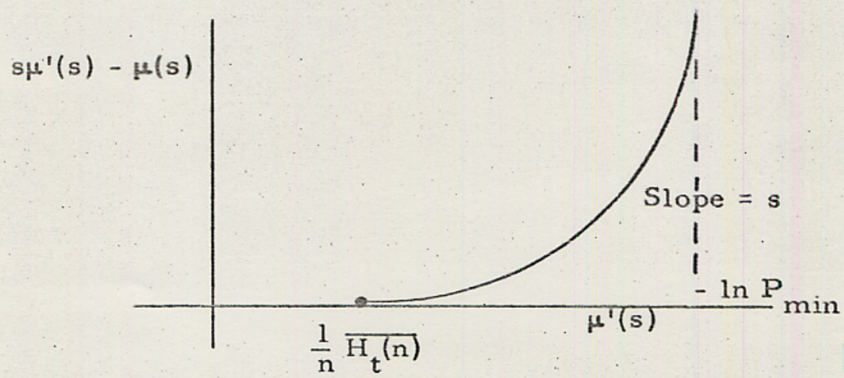

Figure 1

We now specify $H_j(n)$ so that the probability of rejecting the correct sequence at length n is less than some number independent of n, say e^{-K_j}. We do this by relating K_j and $H_j(n)$ parametrically by

$$H_j(n) = n\mu'(s) \tag{7}$$

$$K_j = n[s\mu'(s) - \mu(s)]. \tag{8}$$

If the decoder decodes on the basis of n_t transmitted digits, then there are at most n_t opportunities to reject the transmitted sequence, and the probability of rejecting the transmitted sequence is at most

$$n_t e^{-K_j} \tag{9}$$

Next, in terms of these $H_j(n)$, we must find a bound for $\overline{N}_j$, the average number of computations required to reject the j^{th} criterion in the incorrect subset. $\overline{N}_j$ is therefore the sum of the average number of computations, $\overline{N_j(n)}$, necessary at each length n to go to n + 1.

$$\overline{N}_j = \sum_{n=1}^{n_t} \overline{N_j(n)} \tag{10}$$

We now find two bounds for $\overline{N_j(n)}$, one valid for large n and the other for small n.

In order to bound $\overline{N_j(n)}$ for large n, consider the ensemble in which each digit of the convolution generator and each digit of the added random sequence are independent equiprobable binary digits. It can be shown that over this ensemble each sequence of length n_T in the incorrect subset is statistically independent of the received sequence. Using this it is shown in the Appendix, Equation A-25, that the expected number of values of m, for which a given sequence in the incorrect subset will have $MIN[H_{n,m}] \leq H_j(n)$ is bounded by,

$$E[H_{inc} \leq H_j(n)] \leq 4 \exp -n \left[\ln 2 + (s-1)\mu'(s) - \mu(s)\right] \tag{11}$$

valid for $0 \leq s \leq 1$, where $\mu(s)$ is defined in Equation 5, and

$$H_j(n) = n\mu'(s) \tag{12}$$

Equation 11 is proved in the Appendix for a wide class of conditions which include the cases of practical interest. Only the coefficient must be modified in other cases.

Equation 11 is inconvenient due to the implicit dependence of s on n, but using Equation 8, 11 becomes;

$$E[H_{inc} \leq H_j(n)] \leq 4 \exp \left\{K_j - n\left[\ln 2 + (2s-1)\mu'(s) - 2\mu(s)\right]\right\} \tag{13}$$

By differentiating the coefficient of -n in Equation 13 with respect to s, a minimum is found at $s = 1/2$. Thus,

$$E[H_{inc} \leq H_j(n)] \leq 4 \exp \left\{K_j - n\left[\ln 2 - 2\mu(1/2)\right]\right\} \tag{14}$$

The quantity $\ln 2 - 2\mu(1/2)$ is an upper bound to the rates in nats per digit for which we will prove that the average computation on the incorrect subset grows more slowly than linearly with constraint length. Define:

$$R_{comp} = \ln 2 - 2\mu(1/2) = \ln 2 - 2 \ln\left[\sqrt{P_e} + \sqrt{P_d} + \sqrt{P_i} + \sqrt{P_c}\right] \tag{15}$$

where the last expression comes from Equation 5. This expression is the same as R_{comp} by Wozencraft and Reiffen [1] except for the appearance of $\sqrt{P_d}$ and $\sqrt{P_i}$ and the use of nats instead of bits. Substituting Equation 15 into 14,

$$E[H_{inc} \leq H_j(n)] \leq 4 \exp (K_j - n R_{comp}) \tag{16}$$

For $n < \frac{K_j}{R_{comp}}$, the exponent in Equation 16 becomes positive, so we will find a tighter bound when $n \leq \frac{K_j}{R_{comp}}$. For a very simple bound, we observe that the length of received sequence, m, that must be considered can range only from 0 to 2n, giving

$$E[H_{inc} \leq H_j(n)] \leq 2n + 1 \leq \frac{2K_j}{R_{comp}} + 1 \quad \text{for } n \leq \frac{K_j}{R_{comp}} . \tag{17}$$

For a tighter bound in this range, we observe that $n - D_{max} \leq m \leq n + I_{max}$, where I_{max} and D_{max} are the maximum number of insertions and deletions possible while satisfying the j^{th} criterion at length n. From Equation 1, $-I_{max} \ln P_i \leq H_{m,n} \leq H_j(n) = n\mu'(s)$. $n\mu'(s)$ increases with n and can be evaluated at $n = \frac{K_j}{R_{comp}}$ with the help of Equation 8.

$$I_{max} \leq \frac{K_j \mu'(s_1)}{R_{comp}(-\ln P_i)} \quad \text{for } n \leq \frac{K_j}{R_{comp}} \tag{18}$$

where s_1, from Equation 8, is the solution of

$$R_{comp} = s_1 \mu'(s_1) - \mu(s_1) \tag{19}$$

Similarly

$$D_{max} \leq \frac{K_j \mu'(s_1)}{R_{comp}(-\ln P_d)} \quad \text{for } n \leq \frac{K_j}{R_{comp}} \tag{20}$$

$$E[H_{inc} \leq H_j(n)] \leq 1 + A_3 K_j \quad \text{for } n \leq \frac{K_j}{R_{comp}} \tag{21}$$

where A_3, from Equation 18 and 20,

$$A_3 = \frac{\mu'(s_1)}{R_{comp}} \left(- \frac{1}{\ln P_i} - \frac{1}{\ln P_d} \right) \leq \frac{2}{R_{comp}} \tag{22}$$

It is shown by Wozencraft and Reiffen [1] that the number of different sequences in the incorrect subset at length n + 1 is bounded by Ae^{nR}, where R is the transmission rate of the code in nats per digit, and A is a small constant required by the discrete points where the tree structure branches. From Equations 16 and 21, we get:

$$N_j(n) \leq 4A \exp (K_j - n[R_{comp} - R]) \tag{23}$$

$$N_j(n) \leq A\,(1 + A_3 K_j) \exp nR, \qquad n \leq \frac{K_j}{R_{comp}} \tag{24}$$

From Equations 16, 23, and 24 we get

$$\overline{N}_j \leq \sum_{n=1}^{n_1} A\,(1 + A_3 K_j) \exp nR + \sum_{n_1+1}^{n_t} 4A \exp (K_j - n[R_{comp} - R], \tag{25}$$

$$\text{for any } n_1 \leq \frac{K_j}{R_{comp}}$$

Note that for $R < R_{comp}$ both the sums in Equation 25 are partial geometric series with the terms decreasing away from n_1. We choose n_1 to approximately equalize the first term in each series

$$n_1 \leq \frac{K_j - \ln(1 + A_3 K_j)}{R_{comp}} < n_1 + 1 \tag{26}$$

Substituting Equation 26 into 25, and further bounding by replacing the partial geometric series with infinite series, after some manipulation we get

$$\overline{N}_j \leq A_2\,(1 + A_3 K_j)^{1-B} \exp BK_j \tag{27}$$

where

$$B = \frac{R}{R_{comp}}$$

$$A_2 = A\left(\frac{1}{1 - e^{-R}} + \frac{1}{1 - e^{R - R_{comp}}}\right)$$

The average computation in the incorrect subset can now be evaluated by substituting Equations 27 and 9 into 3.

$$\overline{N} \leq A_2(1 + A_3 K_o)^{1-B} \exp B K_o + n_T \sum_{j=1}^{j_{max}} A_2 (1 + A_3 K_j)^{1-} \tag{28}$$

$$\exp (BK_j - K_{j-1})$$

To further simplify $\overline{N}$, the values of K_j must be specified, and it is unknown how to do this so as to minimize $\overline{N}$ for a given n_T. Even if this could be done, it would be pointless since we are ignoring the computation in the correct subset. We could evaluate the average computation over the good subset by changing the decoding strategy somewhat, but for the Binary Symmetric Channel, the bound achieved in this way is many orders of magnitude higher than the experimentally measured values.

The most sensible procedure is to use the same criteria as used by Wozencraft and Reiffen [1] and compare the resulting answer with their answer. Then, since the bounding procedure here is more crude than their procedure, we can expect the comparison between this channel and the Binary Symmetric Channel to be more favorable experimentally then theoretically.

Following Wozencraft and Reiffen, [1] let

$$K_j = K_o + j\Delta K \tag{29}$$

$$\Delta K = \frac{\ln B}{B - 1} \tag{30}$$

$$K_o = \ln n_T + \Delta K \tag{31}$$

Substituting Equation 29 into 28, after some rearrangment we get

$$\overline{N} \leq A_2 (1 + A_3 K_o)^{1-B} \exp BK_o + n_T A_2 \exp [\Delta K + (B-1) K_o] F \tag{32}$$

where

$$F = \sum_{j=1} \exp\left\{j(B-1)\,\Delta K + (1-B)\ln(1 + A_3K_o + jA_3\Delta K)\right\}$$

$$\leq \sum_{j=1} (1 + A_3K_o)^{1-B} \exp\left\{j(B-1)\,\Delta K\left[1 - \frac{A_3}{1 + A_3K_o}\right]\right\}$$

$$\leq \frac{(1 + A_3K_o)^{1-B} \exp\left\{(B-1)\Delta K\left(1 - \frac{1}{K_o}\right)\right\}}{1 - \exp\left\{(B-1)\,\Delta K\left(1 - \frac{1}{K_o}\right)\right\}} \quad (33)$$

Substituting Equations 33, 30 and 29 into Equation 32 and rearranging terms,

$$\overline{N} \leq \left(1 + \frac{A_3 \ln B}{B-1} + A_3 \ln n_T\right)^{1-B} \frac{A_2 B^{B/1-B} n_T^B}{1 - B^{1-1/\ln n_T}} \quad (34)$$

For comparison purposes, the bound on computation in the incorrect subset for the Binary Symmetric Channel [1] is,

$$\overline{N}_{BSC} \leq \frac{A_2' B^{B/1-B} n_T^B}{1 - B} \quad (35)$$

$$A_2' = A\left(\frac{1}{1-e^{-R}} + \frac{1}{1-e^{R-R_{comp}}}\right) \quad (36)$$

Note that A_2 is at most 4 times larger than A_2', and that the principal difference between the bounds is the initial factor of Equation 34, containing a $[\ln n_T]^{1-B}$ term.

Probability of Decoding Error

A decoding error can be made if for some j some sequence in the incorrect subset satisfies the criterion j while the transmitted sequence has failed criterion j - 1. The probability of this event can be upper bounded by the probability that for some j some sequence in the incorrect subset satisfies the j^{th} criterion at length n_T while the transmitted sequence fails criterion j - 1 at some length. Since the probability of a union of events is bounded by the sum of the individual probabilities,

$$Pr(e) \leq Pr\,[H_{inc} \leq H_o(n_T)] + \sum_{j=1} Pr[H_{inc} \leq H_j(n_T)]\; Ae^{nR}$$

$$Pr\,[\text{transmitted sequence fails } j - 1] \qquad (37)$$

Equation 8 can be used to bound $Pr\,[H_{inc} \leq H_j(n_T)]$ since the probability of 1 or more occurrences of an event is bounded by the expected number of occurrences of the event. For sufficiently large j, however, the bound given by Equation 8 to $Pr[H_{inc} \leq H_j(n_T)]\; Ae^{nR}$ is larger than 1. The probability of error on these high criteria is bounded by the probability that the transmitted sequence fails the first of them. Thus

$$Pr(e) \leq 4A \exp - n[(s_o - 1)\mu'(s_o) - \mu(s_o) + \ln 2 - R]$$

$$+ \sum_{j=1}^{\hat{j}} n_T\, 4A \exp \left\{ -K_{j-1} - n_T[(s_j - 1)\mu'(s_j) - \mu(s_j) + \ln 2 - R] \right\} + n_T\, e^{-K_{\hat{j}}} \qquad (38)$$

where

$$K_j = n_T\,[s_j\mu'(s_j) - \mu(s_j)] \qquad (39)$$

$$(s_{\hat{j}} - 1)\mu'(s_{\hat{j}}) - \mu(s_{\hat{j}}) + \ln 2 - R \geq 0 > (s_{\hat{j}+1} - 1)\,\mu'(s_{\hat{j}+1}) - \mu(s_{\hat{j}+1}) + \ln 2 - R \qquad (40)$$

By multiplying and dividing the first term of Equation 38 by $e^{K_o} = n_T\, e^{\Delta K}$, and introducing Equation 39 into both the first and second terms of Equation 38 we get

$$\Pr(e) \le \sum_{j=0}^{\hat{j}} \left\{ n_T\, 4A\, e^{\Delta K} \exp -n_T \left[(2s_j - 1)\, \mu'(s_j) - 2\mu(s_j) + \ln 2 - R \right] \right\} + n_T\, e^{-K\hat{j}} \tag{41}$$

From Equation 39, as j increases, s_j increases from 0 toward 1. Furthermore, as shown in Equation 14, $(2s_j - 1)\,\mu'(s_j) - 2\mu(s_j) + \ln 2 - R$ reaches its minimum value at $s_j = 1/2$. Thus, if $s_{\hat{j}} > \frac{1}{2}$, the maximum term in the summation in Equation 41 will be at that j for which $s_j \approx \frac{1}{2}$. If $s_{\hat{j}} \le \frac{1}{2}$, the maximum term will be at $\hat{j}$. From Equation 40, s_j decreases with increasing R.

Define,

$$R_{crit} = -\frac{1}{2}\mu'\left(\frac{1}{2}\right) - \mu\left(\frac{1}{2}\right) + \ln 2 \tag{42}$$

For $R \ge R_{crit}$, from Equation 40,

$$(\hat{s}_j - 1)\,\mu'(s_{\hat{j}}) - \mu(s_{\hat{j}}) + \ln 2 \ge R \ge R_{crit}$$

so that $s_{\hat{j}} \le \frac{1}{2}$.

Two bounds are now derived for Pr (e), the first valid for $R \le R_{crit}$ and the second valid for $R \ge R_{crit}$. For sufficiently noisy channels, R_{crit} turns out to be negative, and then the one bound is valid for all R. It can be shown that R_{crit} is always less than R_{comp}, so that the vanishing of R_{crit} is no serious problem. For $R < R_{crit}$,

$$\Pr(e) \le (\hat{j} + 2)\, n_T\, 4A\, e^{\Delta K} \exp \left\{ -n_T \left[R_{comp} - R \right] \right\} \tag{43}$$

Equation 43 is derived from Equation 41 by noting that the $\hat{j} + 1$ terms in the summation and the last term are all bounded by using $s_j = \frac{1}{2}$ in the summation

Furthermore, to bound $\hat{j}$, using Equations 29, 39 and 40,

$$\hat{j}\Delta K < K_{\hat{j}} \leq n_T [R_{comp} - R]$$

$$\Pr(e) \leq 4A [n_T^2 [\frac{R_{comp} - R}{\Delta K}] + 2 n_T] e^{\Delta K}$$

$$\exp -n_T [R_{comp} - R] \quad R < R_{crit} \tag{44}$$

For $R > R_{crit}$, each exponent in Equation 41 is bounded by

$$e^{-K_{\hat{j}}} = \exp -n [s_{\hat{j}} \mu'(s_{\hat{j}}) - \mu(s_{\hat{j}})]$$

where $R \leq (s_{\hat{j}} - 1) \mu'(s_{\hat{j}}) - \mu(s_{\hat{j}}) + \ln 2$. Thus

$$\Pr(e) \leq 4A(\hat{j} + 2) n_T e^{\Delta K} \exp -n_T [s_{\hat{j}} \mu'(s_{\hat{j}}) - \mu(s_{\hat{j}})] \tag{45}$$

for

$$R \leq (s_{\hat{j}} - 1) \mu'(s_{\hat{j}}) + \ln 2 \tag{46}$$

and $R \geq R_{crit}$

Eliminating $\hat{j}$ as before we get

$$\Pr(e) \leq 4A [n_t^2 \frac{s_{\hat{j}} \mu'(s_{\hat{j}}) - \mu(s_{\hat{j}})}{\Delta K} + 2 n_T]$$

$$\exp -n_T [s_{\hat{j}} \mu'(s_{\hat{j}}) - \mu(s_{\hat{j}})] \tag{47}$$

Equations 46 and 47 give a parametric representation of Pr(e) and R in terms of s_j for $R \geq R_{crit}$. As P_d and P_i approach 0, the relation between exponents and rates in these bounds approaches those of Wozencraft and Reiffen.[1]

Unfortunately, these probability of error expressions do not take into account the possibility of the decoder reconstructing the correct transmitted sequence with an incorrect set of deletions, insertions, and errors. This is unimportant except that we started out by assuming that the decoder knew which received symbol corresponded to the last digit decoded. To satisfy this assumption, the decoder must determine whether the digits being decoded correspond to deletions, insertions, errors, or correct transmissions. Clearly this connot be done perfectly since, for instance, if two 0's in a row are transmitted and one of them deleted, there is no way to guess which one was deleted. The computer can easily choose one of the most likely combinations of errors, deletions, and insertions, however. Furthermore, with high probability, the accepted sequence will be the same as the transmitted sequence for many digits. Thus, even if an incorrect decision is made regarding the actual pattern of deletions, insertions, and errors, this incorrect pattern over the initial part of the sequence will be more likely than the actual pattern, and will actually reduce the amount of computation required to decode the next digit.

APPENDIX

The first problem in this Appendix is to find an upper bound to how many different sequences can be achieved by a combination of D deletions, I insertions, and E errors on a given n length sequence. A very simple upper bound is the multinomial coefficient $\binom{n}{D,\, I,\, E}$, but this is a poor bound since many different combinations of deletions, insertions, and errors give rise to the same sequence. A better bound is complicated by the fact that the number of sequences that can be achieved depends on the sequence one starts with. For example, deleting D digits from n consecutive 0's can only give rise to one sequence, namely, N - D 0's. As a result, we consider the average number of sequences that can be achieved over the ensemble of equiprobable n length sequences.

Theorem 1

The average number of different sequences that can be formed by deleting D digits from an n-length sequence and then inserting on I digits is bounded by

$$\overline{N}(n, D, I) \le 2^{I-D} \sum_{J=0}^{D} \sum_{L=0}^{I} 2^{L+J} \binom{n-1-L-J}{D-J,\ I-L} \qquad \text{(A-1)}$$

for $D + I < n$, $D \geq 0$, $I \geq 0$

$$\overline{N}(n, D, I) = 2^{2I} \text{ for } D + I = n,\ D \geq 0,\ I \geq 0 \qquad \text{(A-2)}$$

Proof of Equation A-2 in Theorem

Recall that an insertion was defined as the replacement of a digit with any combination of 2 digits. Thus, when $D + I = n$, each of the I digits remaining after deletions is replaced by an arbitrary pair of digits so that every sequence of length 2I can be formed, proving Equation A-2. To prove Equation A-1, we first need a lemma.

Lemma:

$\overline{N}(n, D, I)$ satisfies the recursion inequality, (A-3)

$$\overline{N}(n, D, I) \leq \overline{N}(n-1, D, I) + \frac{1}{2}\overline{N}(n-1, D-1, I) + 2\overline{N}(n-1, D, I-1) \text{ for}$$

$n > D + I$, $D \geq 0$, and $I \geq 0$. By convention, set $\overline{N}(n, D, I) = 0$ for $D < 0$, or $I < 0$.

Proof of Lemma

First the lemma will be proved for $D > 0$, $I > 0$. Consider listing all binary sequences of length n-1, and beside each sequence list first all sequences formed from that sequence by D deletions and I insertions, then all sequences formed by D-1 deletions and I insertions, then sequences formed by D deletions and I-1 insertions. We call these list A, list B, and list C. Now place a 0 in front of all the length n-1 sequences, a 0 in front of all members of list A, and write each member of list C four times, inserting in turn 00, 01, 10, and 11 in front of each. We call these modified lists OA, B, and IC. For any n length sequence starting with 0, these lists contain all sequences of D deletions and I insertions since the first list contains all sequences formed without changing the first digit; the second contains all sequences deleting the first digit; and the third, all sequences with an insertio on the first digit. Now we show by construction that every sequence in B and IC that starts with a 0 is already contained in OA.

Pick an arbitrary sequence in B starting with 0, and a combination of D deletions and I insertions for forming it from the n length sequence. The first digit is a deletion, and let us suppose that there are K insertions $K \geq 0$ occurring before the first unchanged digit. These first 2K + 1 digits in the sequence in B can also be formed from the n length sequence by deleting the first digit previously undeleted, not deleting the first digit of the n length sequence, and modifying the inserted digits for the K insertions to correspond to digits 2 to 2K + 1 in the sequence in B rather than 1 to 2K. The digits in B from 2K + 2 on can be formed as before, giving us a formation of the sequence with D deletions, I insertions, and the first digit unchanged. Thus, this sequence is in list OA. The same argument applies to a sequence in IC starting with 0.

Next observe that 0's and 1's are symmetrical over the insertion and deletion operations so that on the average (over the n - 1 length sequences), half the sequences in list B start with 0 and do not require counting. Furthermore, two times the number of sequences in list C have 10 or 11 inserted in front of them in list IC and must be counted. But since $\overline{N}(n-1, D, I)$ is the average number of sequences in list A, $\overline{N}(n-1, D-1, I)$ is the average number of sequences in list B, and $\overline{N}(n-1, D, I-1)$ is the average number in list C, we have the statement of the lemma for n length sequences starting with 0. By symmetry (or repetition of the argument), the lemma is also true for n length sequences starting with 1, thus completing the proof of the lemma for $D > 0$, $I > 0$.

Finally, if $D = 0$, the proof the lemma can be repeated omitting list B, and if $I = 0$, the proof can be repeated omitting list C. One term in Equation A-3 drops out for each of these cases due to the convention $\overline{N}(n, D, I) = 0$ for $D < 0$ or $I < 0$.

<u>Proof of Equation A-1 in Theorem:</u>

Consider the recursion relationship

$$M(n, D, I) = M(n-1, D, I) + \frac{1}{2} M(n-1, D, I-1) + 2M(n-1, D, I-1) \qquad (A-4)$$

for $n > D + I$, $D \geq 0$, $I \geq 0$, subject to the boundary conditions $M(n, D, I) = 2^{2I}$

for

$$n = D + I, \quad D \geq 0, \; I \geq 0, \text{ and } M(n, D, I) = 0 \text{ for } D < 0, \; I < 0 \tag{A-5}$$

Using the lemma, which has the same boundary conditions, it can be seen that

$$\overline{N}(n, D, I) \leq M(n, D, I) \tag{A-6}$$

We now find a generating function for M(n, D, I) and expand it to get Equation A-1. Define

$$A(\eta, \delta, \psi) = \sum_{n=1}^{\infty} \sum_{D=0}^{n-1} \sum_{I=0}^{n-D-1} M(n, D, I)\, \eta^n \delta^D \psi^I \tag{A-7}$$

Substituting Equation A-4 into Equation A-7 we get

$$A(\eta, \delta, \psi) = \sum_{n=1}^{\infty} \sum_{D=0}^{n-1} \sum_{I=0}^{n-D-1} \eta M(n-1, D, I,)\, \eta^{n-1} \delta^D \psi^I$$

$$+ \sum_{n=1}^{\infty} \sum_{D=0}^{n-1} \sum_{I=0}^{n-D-1} \frac{1}{2} \eta \delta M(n-1, D-1, I)\, \eta^{n-1} \delta^{D-1} \psi^I$$

$$+ \sum_{n=1}^{\infty} \sum_{D=0}^{n-1} \sum_{I=0}^{n-D-1} 2\eta \psi M(n-1, D, I-1)\, \eta^{n-1} \delta^D \psi^{I-1} \tag{A-8}$$

$$= \eta A(\eta, \delta, \psi) + \eta \sum_{k=0}^{\infty} \sum_{I=0}^{k} M(k, k-I, I)\, \eta^k \delta^{k-I} \psi^I$$

$$+ \frac{1}{2} \eta \delta \; A(\eta, \delta, \psi) + 2\eta\psi \, A(\eta, \delta, \psi) \tag{A-9}$$

The second term in Equation A-9 results from the first term in Equation A-8. When k is substituted for n-1 in the first term, all terms in $A(\eta, \delta, \psi)$ appear along with terms in which k = D + I. Rearranging Equation A-9, and using Equation A-5, we get

$$A(\eta, \delta, \psi) = \frac{\eta \sum_{k=0}^{\infty} \sum_{I=0}^{k} 2^{2I} \eta^{k} \delta^{k-I} \psi^{I}}{1 - \eta - \frac{1}{2}\eta\delta - 2\eta\psi} \qquad \text{(A-10)}$$

Expanding the denominator of Equation A-10 in a power series

$$A(\eta, \delta, \psi) = \left[\eta \sum_{k=0}^{\infty} \sum_{I=0}^{k} 2^{2I} \eta^{k} \delta^{k-I} \psi^{I}\right] \left[\sum_{i=0}^{\infty} \eta^{i} \left(1 + \frac{1}{2}\delta + 2\psi\right)^{i}\right]$$

Substituting h for I and expanding the last term

$$A(\eta, \delta, \psi) = \left[\eta \sum_{k=0}^{\infty} \sum_{h=0}^{k} 2^{2h} \eta^{k} \delta^{k-h} \psi^{h}\right] \left[\sum_{i=0}^{\infty} \sum_{j=0}^{i} \sum_{\ell=0}^{i-j} \eta^{i} \delta^{j} \psi^{\ell} \; 2^{\ell - j} \binom{i}{j, \ell}\right] \qquad \text{(A-11)}$$

Finally after making the substitutions of the dummy variables:

$n = 1 + k + i$

$I = h + \ell$

$D = k - h + j$

$J = k - h$

$L = h$

we get

$$A(\eta, \delta, \psi) = \sum_{n=1}^{\infty} \sum_{D=0}^{n-1} \sum_{I=0}^{n-1-D} \eta^{n} \delta^{D} \psi^{I} \quad 2^{I-D} \sum_{J=0}^{D} \sum_{L=0}^{I} 2^{L+J} \binom{n-1-L-J}{D-J,\ I-L} \qquad \text{(A-12)}$$

This substitution is quite tedious due to the many interchanges of summations required, with the associated change of limits, and is not repeated here. Term-by-term association of Equation A-12 and Equation A-7 and the use of Equation A-6 give Equation A-1, thus proving the theorem.

Theorem 2

Let X be a random binary sequence of length n and Y be an independent random binary sequence of length 2n. Then the expected number of values of m, for which X can be converted into the first m digits of Y by a set of deletions, insertions, and errors such that $H_{n,m} \leq H_j(n)$ is bounded by

$$E[H_{inc} \leq H_j(n)] \leq \frac{\exp - n[\ln 2 + (s-1)\mu'(s) - \mu(s)]}{[1-2P_d^{1-s} e^{-\mu(s)}][1-2P_i^{1-s} e^{-\mu(s)}]} \qquad \text{(A-13)}$$

where $H_{n,m}$ is defined in Equation 1, $\mu(s)$ in Equation 5, $0 \leq s \leq 1$, and

$$H_j(n) = n\mu'(s). \qquad \text{(A-14)}$$

Note that this bound is in parametric form and is similar to Equation 4.

Proof

Define $\overline{N}(n, D, I, E)$ as the average number of different sequences that can be formed by D deletions, I insertions, and E errors on a randomly chosen n length sequence. Theorem 1 bounded the number of sequences that could be formed by D deletions and I insertions, and for each of them there are $\binom{n-D-I}{E}$ combinations of errors. Thus,

$$\overline{N}(n, D, I, E) \leq 2^{I-D} \sum_{L=0}^{I} \sum_{J=0}^{D} 2^{L+J} \binom{n-I-L-J}{I-L,\, D-J} \binom{n-D-I}{E}$$

$$\leq 2^{I-D} \sum_{J=0}^{D} \sum_{L=0}^{I} 2^{L+J} \binom{n-L-J}{I-L,\ D-J,\ E}$$

The expected number of these to be converted into the first $m = n - D + I$ digits of Y is

$$2^{-m}\,\overline{N}(n, D, I, E) \leq 2^{-n} \sum_{J=0}^{D} \sum_{L=0}^{I} 2^{L+J} \binom{n-L-J}{D-J,\ I-L,\ E} \qquad \text{(A-15)}$$

We can now bound $E[H_{inc} \leq H_j(n)]$ by summing the right side of Equation A-15 over all values of D, I, and E satisfying $H_{inc} \leq H_j(n)$. This will be done by a technique similar to the Chernov bound. First, define the generating function

$$G_n(t) = \sum_{D, I, E} 2^{-m}\,\overline{N}(n, D, I, E)\, e^{tH_{n,m}} \qquad \text{(A-16)}$$

$$\geq \sum_{D, I, E \ni H_{n,m} \leq H_j(n)} 2^{-m}\,\overline{N}(n, D, I, E)\, e^{tH_{n,m}} \qquad \text{(A-17)}$$

where the second summation is just over the D, I, E satisfying $H_{n,m} \leq H_j(n)$. For t negative, $e^{tH_{n,m}} \geq e^{tH_j(n)}$ for every term in Equation A-17. Thus,

$$G_n(t) \geq e^{tH_j(n)}\, E[H_{m,n} \leq H_j(n)] \qquad \text{(A-18)}$$

Combining Equation A-15, A-16, and A-18, we get

$$E[H_{n,m} \leq H_j(n)] \leq e^{-tH_j(n)}\, 2^{-n} \left\{ \sum_{D, I, E} \sum_{J=0}^{D} \sum_{L=0}^{I} 2^{L+J} \binom{n-L-J}{D-J,\ I-L,\ E} e^{tH_{n,m}} \right\} \qquad \text{(A-19)}$$

In order to get a convenient expression for the sum in Equation A-19, consider the multinomial expansion of $e^{n\mu(s)}$, with $\mu(s)$ given in Equation 5.

$$e^{n\mu(s)} = [P_e^{1-s} + P_d^{1-s} + P_i^{1-s} + P_c^{1-s}]^n$$

$$= \sum_{D=0}^{n} \sum_{I=0}^{n-D} \sum_{E=0}^{n-D-I} \binom{n}{D,\ I,\ E} \exp\left\{(1-s)\right.$$

$$\left.[E \ln P_e + D \ln P_d + I \ln P_i + (n-E-D-I) \ln P_c]\right\}$$

$$= \sum_{D=0}^{n} \sum_{I=0}^{n-D} \sum_{E=0}^{n-D-I} \binom{n}{D,\ I,\ E} \exp - (1-s)\, H_{n,m} \qquad \text{(A-20)}$$

Notice that if we set $t = -(1-s)$, Equation A-20 is the term in Equation A-19 with $J = 0$, $L = 0$. In the same way,

$$2^{J+L} P_d^{(1-s)J} P_i^{(1-s)L} \quad e^{(n-J-L)\mu(s)} = \sum_{D=J}^{n-L} \sum_{I=L}^{n-D} \sum_{E=0}^{n-D-I}$$

$$2^{J+L} \binom{n-J-L}{D-J,\ I-L,\ E} \exp -(1-s)\, H_{n,m} \qquad \text{(A-21)}$$

Summing the right side of Equation A-21 over $0 \leq J \leq n$ and $0 \leq L \leq n - J$ and interchanging the summations, we get the quantity within the brackets in Equation A-19 for $t = -(1-s)$. We upper bound this by the left side of Equation A-21 summed over all $J \geq 0$ and $L \geq 0$ to give a double geometric series. Thus, Equation A-19 becomes

$$E[H_{n,m} \leq H_j(n)] \leq \frac{e^{(1-s)\, H_j(n)}\, 2^{-n}\, e^{n\mu(s)}}{[1 - 2P_d^{1-s}\, e^{-\mu(s)}]\, [1 - 2P_i^{1-s}\, e^{-\mu(s)}]}$$

$$\text{for } s \leq 1 \qquad \text{(A-22)}$$

The restriction $s \leq 1$ is required by the restriction $t \gtreqless 0$ in Equation A-19. Furthermore, $s \leq 1$ insures that the geometric series represented by the denominator of Equation A-22 converge for $P_d < P_c$; $P_i < P_c$. Since Equation A-22 is valid for any $s \leq 1$, we can choose s to satisfy Equation A-14. As $n \to \infty$, this s becomes arbitrarily close to the s^* minimizing the bound. Finally, substituting Equation A-14 into A-22, we have the statement of the theorem, Equation A-13. Q, E. D.

The denominator of Equation A-13 is still in a somewhat inconvenient form, but it can be demonstrated directly that if

$$-\ln P_d \geq -P_d \ln P_d - P_i \ln P_i - P_e \ln P_e - P_c \ln P_c = \overline{H(p)} \tag{A-23}$$

then

$$\frac{1}{1-2P_d^{1-s} e^{-\mu(s)}} \leq 2 \quad \text{for } s \leq 1$$

Likewise, if

$$-\ln P_i \geq \overline{H(p)} \tag{A-24}$$

then

$$\frac{1}{1-2P_i^{1-s} e^{-\mu(s)}} \leq 2 \quad \text{for } s \leq 1$$

Consequently, subject to Equations A-23 and A-24, which are satisfied in any practical case, we have

$$E[H_{n,m} \leq H_j(n)] \leq 4 \exp -n\,[\ln 2 + (s-1)\,\mu'(s) - \mu(s)]$$

$$\text{for } 0 \leq s \leq 1 \tag{A-25}$$

REFERENCES

1. J.M. Wozencraft and B. Reiffen, Sequential Decoding, M.I.T. Technology Press and Wiley, New York, 1961.
2. R.M. Fano, Transmission of Information, M.I.T. Technology Press and Wiley, New York 1961.