Estimates of Error Rates for Codes on Burst-Noise Channels

By E. O. ELLIOTT

(Manuscript received April 8, 1963)

The error structure on communication channels used for data transmission may be so complex as to preclude the feasibility of accurately predicting the performance of given codes when employed on these channels. Use of an approximate error rate as an estimate of performance allows the complex statistics of errors to be reduced to a manageable table of parameters and used in an economical evaluation of large collections of error detecting codes. Exemplary evaluations of error detecting codes on the switched telephone network are included in this paper.

On channels which may be represented by Gilbert's model of a burst-noise channel, the probabilities of error or of retransmission may be calculated without approximations for both error correcting and error detecting codes.

I. INTRODUCTION

The structure in bursts of noise on real communication channels is usually very difficult to describe. As a consequence, no general procedure exists for predicting the performance of error detecting or error correcting codes, and no basic set of parameters exists for describing the channel. Gilbert[1] has shown that a simple Markov model with three parameters provides a close approximation to certain telephone circuits used for the transmission of binary data. When such an approximation is possible, the error rates for codes may be easily calculated from these channel parameters and properties of the code. (See Section V.)

To provide a means for estimating error rates for binary block codes in more general circumstances, a table of probabilities $P(m,n)$ may be employed. $P(m,n)$ is the probability that m bit errors occur in a transmitted block of n bits. It was speculated and later corroborated (as we will show) that equivalent error detecting codes would have rather comparable error rates when employed on the same channel. (Two codes are equivalent if one may be obtained from the other by a permutation of bit positions.) Thus the average error rate for all codes equivalent to a given code may be used as an estimate of the true error rate. This average probability of an undetected error in a single transmission of a word is given by

$$\bar{P}_u = \sum_{m=1}^{n} \frac{w(m)}{\binom{n}{m}} P(m, n)$$

where code word usage is assumed uniform, $w(m)$ is the average number of code words at distance m from a typical code word, and n is the block length of the code.

No definitive statement regarding the accuracy of this estimate can be made at this point. A limited investigation, however, suggests that it will ordinarily be a reasonable estimate.

As an example of the use of this method, a collection of 29 interesting error detecting codes is evaluated, using the recorded error data of the field testing program conducted by the data transmission evaluation task force of the Bell System.[2] The Bose-Chaudhuri (31, 21) code is included in this collection and is analyzed in considerable detail to illustrate the full potentials and limitations inherent in the method.

In the interest of simplicity, the discussion to follow will be limited to binary block codes with particular interest in error detection. The methods employed, however, are not limited to these particular applications, and are open to obvious generalizations.

II. PRELIMINARY DEFINITIONS AND OBSERVATIONS

A binary block code C, hereinafter referred to as a "code," is a collection of binary words of 0's and 1's of length n. N will be used to denote the total number of words in C. The distance $\delta(x,y)$ between two binary words x and y of length n is the number of bit positions in which x and y differ. The weight $| x |$ of x is the distance $\delta(\theta,x)$ between x and the all-zero word θ. The number of ordered pairs of code words x, y such that $\delta(x,y) = m$ is denoted by $W(m)$, and $w(m) = W(m)/N$.

The communication channel is described by a collection of conditional probabilities of the form $P(x \rightarrow y)$, which give the probability that the word y will be received when x is transmitted. A channel is called *metric* whenever $P(x \rightarrow y)$ is a function only of $\delta(x,y)$: i.e., $P(x \rightarrow y) = F(m,n)$, where $m = \delta(x,y)$ and n is the block length. A channel is called *symmetric* whenever $P(x \rightarrow y)$ is a function only of $z = y - x \pmod 2$.

It should be noted that a metric channel is symmetric and that a symmetric memoryless channel is metric. The Gilbert burst-noise channel[1] is an example of a symmetric channel which, because of its memory (i.e., interdependence of error probabilities of neighboring bits), is not metric.

When a code is used for error detection, it will be assumed that error correction is accomplished by retransmissions of any received words which are detected to be in error. The specific manner in which the receiver signals to the transmitter for a retransmission will not be considered. It will be assumed, however, that this backward signaling is error-free, that each retransmission consists of a single word, and that repeated retransmissions of a word are possible. Since very little information is required for the backward signaling for retransmissions, it is not too unrealistic to assume that it is error-free. Most retransmission systems will, however, probably involve delays in retransmissions, and the retransmitted data may consist of a block of several words. Because of the burst nature of noise on many channels, the effect of these retransmission delays is improvement of the channel, and we can then expect codes to perform better than our model indicates.

Thus, for an error detecting code, an (undetected) error occurs if a received word is a code word different from the transmitted word. If x is the transmitted word, then the probabilities of an undetected error, of a word retransmission, and of acceptance of a correct word are, respectively

$$\textstyle\sum_{y(\neq x)\varepsilon C} P(x \to y) \qquad \sum_{y \not\varepsilon C} P(x \to y) \qquad \text{and} \qquad P(x \to x).$$

Now, if we assume that the words of the code are used with equal frequencies, then the averages of the above probabilities are, respectively

$$P_u = \frac{1}{N} \textstyle\sum_{x \varepsilon C} \sum_{y(\neq x)\varepsilon C} P(x \to y) \tag{1}$$

$$P_r = \frac{1}{N} \textstyle\sum_{x \varepsilon C} \sum_{y \not\varepsilon C} P(x \to y) \tag{2}$$

and

$$P_0 = \frac{1}{N} \textstyle\sum_{x \varepsilon C} P(x \to x). \tag{3}$$

These probabilities are of some interest in themselves, but for symmetric communication channels the probability P_E that a word is received in error after possible retransmissions is given by

$$P_E = \frac{P_u}{1 - P_r}. \tag{4}$$

This result follows from the definitional equation

$$P_E = \text{Prob (undetected error} \mid \text{received word is accepted)}$$

the definition of conditional probability, and the observations that an undetected error implies acceptance of the received word and that the probability of a received word being accepted is $1 - P_r$.

Suppose the channel is metric, so that $P(x \to y) = F(m,n)$ where $m = \delta(x,y)$ and n is the length of x and y. Then, from (1), (3) and (2)

$$P_u = \sum_{m=1}^{n} w(m)F(m,n), \tag{5}$$

$$P_0 = F(0,n),$$

and

$$P_r = 1 - (P_0 + P_u). \tag{6}$$

It is evident from (5) that on a metric channel equivalent codes have identical values of P_u, since w is invariant under a permutation of the bit positions in a code.

III. $\bar{P}_u$ ON SYMMETRIC CHANNELS

Let $\bar{P}_u$ denote the average value of P_u over all bit-position permutations of the code. If $P(m,n)$ is the total probability of m errors in a block of length n, i.e.

$$P(m,n) = \textstyle\sum_{|y|=m} P(\theta \to y) \tag{7}$$

then

$$\bar{P}_u = \sum_{m=1}^{n} w(m) \frac{P(m,\, n)}{\binom{n}{m}}. \tag{8}$$

This result may be seen as follows: consider a particular code C and channel X. Corresponding to each permutation π of the n bit positions is a permutation of C which we will call πC. Now, using (1)

$$\begin{aligned} \bar{P}_u &= \frac{1}{n!} \textstyle\sum_{\pi} \frac{1}{N} \sum_{x \varepsilon \pi C} \sum_{y (\neq x) \varepsilon \pi C} P(x \to y) \\ &= \frac{1}{N} \textstyle\sum_{x \varepsilon C} \sum_{y (\neq x) \varepsilon C} \frac{1}{n!} \sum_{\pi} P(\pi x \to \pi y). \end{aligned} \tag{9}$$

For a symmetric channel there is a function f such that $P(x \to y) =$

$f(z)$ where $z = y - x \pmod 2$. Then, if z contains m ones

$$\frac{1}{n!} \sum\nolimits_{\pi} P(\pi x \to \pi y) = \frac{1}{n!} \sum\nolimits_{\pi} f(\pi z).$$

Now any n-place binary sequence having exactly m ones is left invariant by $m!(n\text{-}m)!$ permutations of its digits. The sum just written is therefore equal to

$$\frac{m!(n-m)!}{n!} \sum f(u) = \frac{P(m, n)}{\binom{n}{m}}$$

where the sum is over all distinct n-place binary sequences u having exactly m ones. Equation (8) follows by inserting this result in (9).

Now that $\bar{P}_u$ has been obtained, it is an easy matter to obtain $\bar{P}_r$, the average probability of a retransmission for all permutations of the code. Since $P_0 = P(0,n)$ and $P_0 + P_r + P_u = 1$, it follows that

$$\bar{P}_r = 1 - \bar{P}_u - P(0,n).$$

Our $\bar{P}_u$ estimate is exactly equal to P_u whenever the code in question is invariant under all permutations of bit positions. Thus, accurate results are obtained on symmetric channels for single parity check codes, constant weight codes, etc.

It is of interest to note that in the case of group codes of given block length and redundancy, $w(m)$ has an unevenly weighted average value which may be used to estimate $\bar{P}_u$ in terms of the code's minimum distance D. Consider group codes of block length n and dimension k. For such group codes there are 2^{kc} ways of assigning the k information positions to the check positions of the $c = n - k$ check bits, but for such assignments the resulting codes are not necessarily distinct. Of these, however, it is known (Ref. 3, p. 54) that in $2^{(k-1)c}$ cases a given binary word z will belong to the resulting code, provided the information portion of z does not contain only 0's. Now, there are $\left[\binom{n}{m} - \binom{c}{m}\right]$ binary words of weight m having nonzero information parts whenever $0 < m \leqq c$, and there are $\binom{n}{m}$ such words whenever $c < m \leqq n$. As a consequence, the "average" number $\bar{w}(m)$ of code words of weight m is

$$\bar{w}(m) = \frac{1}{2^{kc}} \left[\binom{n}{m} - \binom{c}{m}\right] 2^{(k-1)c} \qquad \text{when } 0 < m \leqq c$$

and

$$\bar{w}(m) = \frac{1}{2^{kc}} \binom{n}{m} 2^{(k-1)c} \qquad \text{when } c < m \leqq n$$

wherein the average is over the multiplicity of group codes of the specified block length and dimension which result from these assignments of information bit positions to check bit positions.

Let

$$\bar{C}(m) = \bar{w}(m) \bigg/ \binom{n}{m}$$

then

$$\bar{C}(m) = 2^{-c} \left\{ 1 - \frac{\binom{c}{m}}{\binom{n}{m}} \right\} \qquad \text{when } 0 < m \leqq c$$

and

$$\bar{C}(m) = 2^{-c} \qquad \text{when } c < m \leqq n.$$

This result may be of use as follows. Suppose we have knowledge only of the minimum distance D of a given group code that we wish to evaluate on some channel. Let us make the bold assumption that the big difference between the given code and the "average" of all codes is the fact that the given code contains no words of weight $1, \cdots, D - 1$. Then (8) yields

$$\bar{P}_u \approx \sum_{m=D}^{n} \bar{C}(m) P(m,n). \tag{10}$$

When the dimension of a code is large, it may be unfeasible to ascertain $w(m)$ because of the immense amount of computation required. It is in such cases that (10) may prove to be a useful approximation.

IV. $\bar{P}_u$ ON ASYMMETRIC CHANNELS

We propose the following reasonably general model of an asymmetric channel. Two channel states are hypothecated: a "good" state in which no errors occur, and a "bad" state in which $0 \rightarrow 1$ errors occur with probability p_0 and $1 \rightarrow 0$ errors occur with probability p_1. The manner in which good and bad states occur will not be specified beyond knowledge of the total probability $S(s,n)$ of being in the bad state for some s bits of the n bits of a block. Particular arrangements of these s bad bits need not be equiprobable.

Let $q_0 = 1 - p_0$ and $q_1 = 1 - p_1$, and make the following definitions when x and y are binary words of length n:

$A(x,y)$ = the number of bit positions where x is 0 and y is 1,
$A'(x,y)$ = the number of bit positions where both x and y are 0,
$B(x,y)$ = the number of bit positions where x is 1 and y is 0,
$B'(x,y)$ = the number of bit positions where both x and y are 1.

Let the state sequence of the channel be described by a binary word v, in which each digit is G or B according as the state of the channel at that digit's position is good or bad. Now define

$A^*(x,y,v)$ = the number of bit positions in which x and y are 0 and v is B, and

$B^*(x,y,v)$ = the number of bit positions in which x and y are 1 and v is B.

The error probabilities for this channel, conditional on the state sequence v, may now be given as follows:

$$P(x \to y \mid v) = \left| \begin{array}{ll} 0 \text{ if at some bit position } v \text{ is } G \text{ and} & \\ \quad x \text{ and } y \text{ are different} & (11) \\ p_0^{a} q_0^{a^*} p_1^{b} q_1^{b^*} \text{ otherwise} & (12) \end{array} \right.$$

where the values of the previously defined functions are

$$a = A(x,y) \qquad a' = A'(x,y)$$
$$B = B(x,y) \qquad b' = B'(x,y)$$

and

$$a^* = A^*(x,y,v),$$
$$b^* = B^*(x,y,v).$$

Define

$$\bar{P}(x \to y \mid v) = \frac{1}{n!} \sum\nolimits_{\pi} P(\pi x \to \pi y \mid v) \tag{13}$$

wherein π is the arbitrary permutation of bit positions that we have used before. Notice that by (11), (12) and (13)

$$\bar{P}(x \to y \mid v) = \bar{P}(x \to y \mid \pi v) \tag{14}$$

and therefore that $\bar{P}(x \to y \mid v)$ depends only on how many B's are in v and not on their positions in v. Suppose v contains s B's. We can now say, using (13) and writing $\bar{P}_s(x \to y)$ for $\bar{P}(x \to y \mid v)$, that

$$\bar{P}_s(x \to y) = \frac{1}{n!} \sum\nolimits_{\pi} P(x \to y \mid \pi v) \tag{15}$$

and from (11) we know $P(x \rightarrow y \mid \pi v) = 0$ whenever πv has G's in positions where x and y differ.

We will use (12) in evaluating (15) by first finding the number of permutations π for which $P(x \rightarrow y \mid \pi v)$ has a fixed value. Suppose a^* and b^* are such numbers that $a^* + b^* = s - (a + b)$, with $0 \leqq a^* \leqq a'$ and $0 \leqq b^* \leqq b'$. Then there are $\binom{a'}{a' - a^*} = \binom{a'}{a^*}$ arrangements of $a' - a^*$ G's among the a' bit positions where x and y are 0, and there are $\binom{b'}{b' - b^*} = \binom{b'}{b^*}$ arrangements of $b' - b^*$ G's among the b' bit positions where x and y are 1. Hence there are a total of $\binom{a'}{a^*}\binom{b'}{b^*}$ arrangements of the $n - s$ G's among the $a' + b'$ bit positions where x and y are the same. For each such arrangement there are $s!(n - s)!$ permutations π under which the arrangement is invariant. Consequently, the total number of permutations π for which $P(x \rightarrow y \mid \pi v) = p_0^a q_0^{a^*} p_1^b q_1^{b^*}$ is given by $s!(n - s)! \binom{a'}{a^*}\binom{b'}{b^*}$. Hence, they contribute

$$\frac{n!\binom{a'}{a^*}\binom{b'}{b^*}}{\binom{n}{s}} p_0^a q_0^{a^*} p_1^b q_1^{b^*}$$

to the sum in (15). We conclude then that

$$\bar{P}_s(x \rightarrow y) = \sum_{a^*=\max(0,\, t-b')}^{\min(a',\, t)} \frac{\binom{a'}{a^*}\binom{b'}{t - a^*}}{\binom{n}{s}} p_0^a p_1^b q_0^{a^*} q_1^{t-a^*} \qquad (16)$$

where $t = s - (a + b)$.

If we set $r = |x|$, then $\bar{P}_s(x \rightarrow y)$ may be expressed in terms of b, a, r and s as

$$H(b, a, r, s)$$

$$= \left(\frac{p_0}{q_1}\right)^a \left(\frac{p_1}{q_1}\right)^b q_1^s \sum_{a^*=\max(0,\, s-(a+r))}^{\min(n-(a+r),\, s-(a+b))} \left(\frac{q_0}{q_1}\right)^{a^*} \frac{\binom{n - (a + r)}{a^*}\binom{r - b}{s - (a + b + a^*)}}{\binom{n}{s}}$$

which is just another form of (16). This asymmetric channel may now be compactly described by a function J which gives the probability, averaged over all permutations π of the bit positions, of making b 1 → 0 errors and a 0 → 1 errors in a transmitted word of weight r

$$J(b,a,r) = \sum_{s=a+b}^{n} H(b,a,r,s)S(s,n).$$

For a code C, let us define $I_C(b,a,r)$ to be $1/N$ times the number of ordered code-word pairs (x,y) for which $A(x,y) = a$, $B(x,y) = b$, and $|x| = r$. Then finally the asymmetric analogue of (8) for the average probability $\bar{P}_u$ of an undetected error may be written as

$$\bar{P}_u = \sum_{(b,\ a,\ r):b \leqq r \leqq n, a \leqq n-r} I_C(b, a, r)\ J(b, a, r). \tag{17}$$

V. ERROR PROBABILITIES ON GILBERT BURST-NOISE CHANNELS

Gilbert's model[1] of a burst-noise channel is a binary symmetric channel (with memory) determined by an elementary Markov chain. As in the preceding model for an asymmetric channel, a good (G) and bad (B) state are assumed of the channel. No errors occur in the G state, but in the B state, the probability of a bit error is $(1 - h)$. With the transmission of each bit, the channel has opportunity to change states. The transitions $G \rightarrow B$ and $B \rightarrow G$ have probabilities P and p, respectively, while the transitions $G \rightarrow G$ and $B \rightarrow B$ have probabilities $Q = 1 - P$ and $q = 1 - p$. When Q and q are large, the states G and B tend to persist, simulating features of a burst-noise channel. Gilbert (Ref. 1, p. 1262) has shown how this model approximates the burst noise on two of the calls from the field testing program of the data transmission evaluation task force of the Bell System.

Using conditional probabilities determined by the parameters P,p,h, it is a simple matter to calculate the probability that a transmitted word x be received as y on a Gilbert channel. This probability depends on the modulo 2 difference $z = y - x$ of y and x.

Suppose a is the number of 0's in z which precede the first 1 in z, c is the number of 0's following the last 1, and b_i $(i = 1,\cdots, |z| - 1)$ are the number of 0's between consecutive 1's in z. Then, if $z \neq \theta$

$$P(x \rightarrow y) = P(z) = w(a)\left\{\textstyle\prod_{i=1}^{|z|-1} v(b_i)\right\}u(c) \tag{18}$$

where w, v and u are functions such that $w(k) = P(0^k1)$, $v(k) = P(0^k1 \mid 1)$, and $u(k) = P(0^k \mid 1)$ $(k = 0, 1, \cdots)$. Here 0^k denotes k consecutive zeros. Also, if $z = \theta$ then

$$P(x \rightarrow x) = P(\theta) = 1 - \sum_{i=0}^{n-1} w(i). \tag{19}$$

Using generating functions, Gilbert has shown that u, v and w satisfy the following recurrence equations

$$\begin{aligned} u(0) &= 1,\ u(1) = p + hq; \\ u(k) &= (Q + hq)u(k-1) - h(Q-p)u(k-2), \qquad k = 2, 3, \cdots \qquad (20) \\ v(k) &= u(k) - u(k+1), \qquad k = 0, 1, \cdots \\ w(k) &= p_B(1-h)u(k). \end{aligned}$$

Equation (18) results from the obvious composition of the conditional probabilities in the v and u terms. Equation (19) results from the fact that the event not 0^n is the union of the events 1, 01, $0^2 1$, $\cdots$, $0^{n-1}1$. Since these events are disjoint,

$$P(0^n) = 1 - P(\text{not } 0^n) = 1 - \sum_{i=0}^{n-1} P(0^i 1).$$

In the interest of completeness, we shall sketch a proof that u, v and w satisfy the recurrence equation (20).

To see that

$$v(k-1) = u(k-1) - u(k), \qquad k = 1, 2, \cdots$$

note that the event 10^{k-1} is the union of $10^{k-1}1$ and 10^k and that the latter two events are disjoint. Hence

$$\text{Prob }(0^{k-1} \mid 1) = \text{Prob }(0^{k-1}1 \mid 1) + \text{Prob }(0^k \mid 1)$$

and therefore

$$u(k-1) = v(k-1) + u(k).$$

We define $u(0) = 1$. That $u(1) = p + qh$ is obvious. To establish that $u(k+1) = (Q + hq)u(k) - h(Q-p)u(k-1), \quad k = 1, 2, \cdots$ we shall need to introduce

$$u_G(k) = \text{Prob }(0^{k-1}G \mid 1) \quad \text{and} \quad u_B(k) = \text{Prob }(0^{k-1}0_B \mid 1)$$

wherein 0_B denotes a zero in the bad state. Clearly

$$u(k) = u_G(k) + u_B(k)$$

and

$$u_B(k) = \frac{h}{1-h} v(k-1).$$

Now, considering transitions, we see that

$$
\begin{aligned}
u(k+1) &= (Q+Ph)u_G(k) + (p+qh)u_B(k) \\
&= (Q+Ph)\{u(k) - u_B(k)\} + (p+qh)u_B(k) \\
&= (Q+Ph)u(k) - (Q+Ph-p-qh)u_B(k) \\
&= (Q+Ph)u(k) - (Q-p)(1-h)u_B(k) \\
&= (Q+Ph)u(k) - (Q-p)h\{u(k-1) - u(k)\}.
\end{aligned}
$$

Finally, it is evident that if z' is obtained from z by inverting the order of the bits, then $P(z') = P(z)$. This results from the fact that the forward and backward state transition probabilities are identical. As a consequence,

$$
\begin{aligned}
w(k) = \text{Prob }(0^k1) &= \text{Prob }(10^k) \\
&= p_B(1-h)\text{ Prob }(0^k \mid 1) = p_B(1-h)u(k)
\end{aligned}
$$

and the proof is complete.

The performance of error detecting codes on Gilbert channels can now be calculated using (18)–(20) in (1)–(4). For an error correcting group code using coset decoding,[4] the probability of incorrect decoding is given by

$$P_e = 1 - \sum_{i=1}^{s} P(\alpha_i)$$

where the α_i are the coset leaders for the code. These coset leaders would presumably be chosen so as to minimize P_e and therefore may not necessarily be the minimal weight elements of cosets.

It is interesting to note that if a Gilbert channel with parameters (P,p,h) is sampled at every kth bit, then the string of bits obtained has the same structure as the bits on a Gilbert channel with parameters (P',p',h) where

$$P' = \frac{P}{P+p}\{1-(Q-p)^k\}$$

and

$$p' = \frac{p}{P+p}\{1-(Q-p)^k\}.$$

The proof of this assertion is given in Ref. 5, p. 385. This result is useful for analysis when time division multiplex encoding is employed.

VI. $P(m,n)$ FOR GENERALIZED GILBERT CHANNELS

The probabilities $P(m,n)$ for a Gilbert burst-noise channel are readily computed by recursive methods. However, it is just as easy to obtain $P(m,n)$ for a slightly more general symmetric channel. In the Gilbert model, an error bit can occur only when the channel is in the bad state. In the model proposed here, an error bit can occur in either the good or the bad state but with different probabilities. Transitions between the good and bad states are the same as in the Gilbert model.

Let k denote the probability of correct reception of a bit when the channel is in the good state, and let $h' = 1 - h$ and $k' = 1 - k$.

Let $G(m,n) =$ Prob (m errors in a block of length $n \mid$ the channel is in the good state at the first bit) and $B(m,n) =$ Prob (m errors in a block of length $n \mid$ the channel is in the bad state at the first bit). Then

$$P(m,n) = \frac{p}{P+p} G(m,n) + \frac{P}{P+p} B(m,n)$$

and $G(m,n)$ and $B(m,n)$ may be found recursively from

$$\begin{aligned} G(m,n) &= G(m,n-1)Qk + B(m,n-1)Pk + G(m-1,n-1)Qk' \\ &\quad + B(m-1,n-1)Pk', \\ B(m,n) &= B(m,n-1)qh + G(m,n-1)ph + B(m-1,n-1)qh' \\ &\quad + G(m-1,n-1)ph', \\ &\quad G(0,1) = k \qquad\qquad B(0,1) = h, \\ &\quad G(1,1) = k' \quad \text{and} \quad B(1,1) = h'. \end{aligned}$$

We must also assign the values $G(m,n) = B(m,n) = 0$ when $m < 0$ or $m > n$.

VII. THE BOSE-CHAUDHURI (31, 21) CODE ON THE TELEPHONE NETWORK

As an illustration of the use of the $\bar{P}_u$ estimate for P_u, the performance of a Bose-Chaudhuri (31, 21) code (Ref. 3, p. 166) on the switched telephone network is analyzed. As a source of error statistics for the channels of the telephone network, the records of the field testing program described by Alexander, Gryb and Nast[2] are employed. These give in sequence the numbers of correct bits and error bits for 1010 calls of 10 and 30 minutes' duration over a variety of facilities in the switched telephone network. A detailed summary of the number of

Table I — Number of Calls

Type of Call	1200 bps		600 bps 10 min.
	30 min.	10 min.	
Long haul	181	34	229
Short haul	102	20	151
Exchange	108	28	157

calls of each type made at 600-bps and 1200-bps transmission rates with the FM digital subset appears in Table I.*

For each call in this program, the probability $P(m,31)$ that m bit-errors occur in a block of length 31 for $m = 0, 1, \cdots, 31$ has been determined. In doing this, each call is divided into consecutive blocks 31 bits long starting at the ith bit in the call ($i = 1, \cdots, 31$) and the number $N_i(m)$ of blocks containing m bit-errors is noted. This corresponds to viewing each call as, in some sense, 31 different calls, depending on the phase with which we enter the call (i.e., which of the first 31 bits we take as first in governing the subdivision). We thus obtain, for each $i = 1, \cdots, 31$, a probability $P_i(m,31) = N_i(m)/N$ that a block in the subdivision contains m bit-errors. (N is the total number of blocks in the subdivision.) We now average over the possible entry phases and take the probability $P(m,31)$ that m errors occur in a block of length 31 to be $(1/31) \sum_{i=1}^{31} P_i(m,31)$.

Examination of the $P(m,31)$ values obtained reveals some interesting facts. For example, on some calls the probability of having numerous errors in a block greatly exceeds the probability of having only a few errors. For many calls, however, $P(m,31)$ is maximum at $m = 1$, decreases with increasing m, and is often zero for m greater than 2 or 3. On still others, $P(m,31)$ is maximum at $m = 1$, decreases for the next few values of m, and then increases to some smaller relative maximum around $m = 15$ to 17 before its final descent to zero. To illustrate this variability among calls, we present in Table II the $P(m,31)$ values for four calls. In Table II, the P_1 entry under the call's number is the over-all bit-error rate for the call.

Properties of the burst nature of errors on calls like No. 1167 are responsible for $P(m,31)$ having its maximum value midway in the range $m = 1, \cdots, 31$. On such calls there are long bursts of errors. When the burst length is shorter, $P(m,31)$ may more closely resemble that for call No. 1641. These effects can be noted also in Table III,

* Consult Refs. 2 and 6 for a description of call types and for further details regarding the field testing program.

TABLE II — SAMPLE $P(m,31)$ VALUES

Call Type	LH/600/10	SH/1200/30	EX/600/10	LH/1200/30
Call No.	1167	1641	2058	2250
P_1	22.50×10^{-4}	2.70×10^{-4}	0.22×10^{-4}	0.03×10^{-4}
$m = 0$	0.99587	0.99276	0.99972	0.99995
1	0.14×10^{-4}	63.20×10^{-4}	1.83×10^{-4}	0.18×10^{-4}
2	0.22	8.32	0.08	0.16
3	0.14	0.69	0.06	0.12
4	0.20	0.06	0.08	0.0
5	0.14	0.05	0.11	
6	0.25	0.02	0.64	
7	0.14	0.0	0.0	
8	0.14			
9	0.50			
10	0.92			
11	1.00			
12	0.75			
13	1.20			
14	3.18			
15	4.29			
16	4.46			
17	4.88			
18	3.84			
19	4.12			
20	3.51			
21	2.54			
22	2.17			
23	1.78			
24	0.78			
$\geqq 25$	0.0			

which gives the average $P(m,n)$ values for all calls of the field test program.

The quantities $w(m) = 0, 1, \cdots, 31$ for the Bose-Chaudhuri (31, 21) code are presented in the Table IV. Since each check bit of this code applies to an odd number of information bits, $w(m)$ is symmetric: i.e., $w(m) = w(31 - m)$, and therefore $w(m)$ is tabulated only for $m = 0, \cdots, 15$.

Using the above $w(m)$ values and the $P(m,31)$ tables in (8) gives a $\bar{P}_u$ estimate for the undetected error rate on each call.

The smoothed cumulative distributions of the percentage of calls over particular facilities having an estimated undetected error rate not exceeding specified values are shown in Figs. 1 and 2 for the two transmission rates used. We have excluded the 10-minute calls at 1200 bps from this summary of the data because of the small size of the sample.

The approximate retransmission probabilities were generally less than 0.1 per cent. On some 7 per cent of the calls, the rate was between 0.1 and 1 per cent. On only three calls did it exceed one per cent.

It is impossible to obtain exact values of P_u for this code on the tele-

TABLE III — AVERAGE $P(m,n)$ VALUES FOR ALL CALLS OF THE FIELD TEST PROGRAM

m	$n = 8$	$n = 15$	$n = 17$	$n = 21$	$n = 23$	$n = 31$*
1	1.24×10^{-4}	2.07×10^{-4}	2.31×10^{-4}	2.77×10^{-4}	3.00×10^{-4}	3.90×10^{-4}
2	2.28×10^{-5}	3.66×10^{-5}	4.06×10^{-5}	4.82×10^{-5}	5.19×10^{-5}	6.72×10^{-5}
3	9.31×10^{-6}	1.27×10^{-5}	1.40×10^{-5}	1.63×10^{-5}	1.75×10^{-5}	2.18×10^{-5}
4	5.15×10^{-6}	6.98×10^{-6}	7.40×10^{-6}	8.62×10^{-6}	9.20×10^{-6}	1.14×10^{-5}
5	3.62×10^{-6}	4.69×10^{-6}	4.75×10^{-6}	5.50×10^{-6}	5.98×10^{-6}	7.30×10^{-6}
6	2.41×10^{-6}	3.59×10^{-6}	3.54×10^{-6}	3.61×10^{-6}	3.82×10^{-6}	4.81×10^{-6}
7	8.25×10^{-7}	2.66×10^{-6}	2.98×10^{-6}	2.58×10^{-6}	2.78×10^{-6}	3.54×10^{-6}
8	1.03×10^{-7}	2.29×10^{-6}	2.37×10^{-6}	2.13×10^{-6}	2.06×10^{-6}	2.63×10^{-6}
9		1.92×10^{-6}	2.04×10^{-6}	2.23×10^{-6}	1.69×10^{-6}	2.11×10^{-6}
10		1.74×10^{-6}	1.83×10^{-6}	2.17×10^{-6}	1.89×10^{-6}	1.65×10^{-6}
11		1.17×10^{-6}	1.68×10^{-6}	1.86×10^{-6}	2.12×10^{-6}	1.31×10^{-6}
12		4.51×10^{-7}	1.30×10^{-6}	1.81×10^{-6}	1.98×10^{-6}	1.16×10^{-6}
13		8.78×10^{-8}	4.73×10^{-7}	1.72×10^{-6}	1.88×10^{-6}	1.03×10^{-6}
14		1.23×10^{-8}	1.19×10^{-7}	1.02×10^{-6}	1.57×10^{-6}	1.15×10^{-6}
15		9.47×10^{-10}	2.83×10^{-8}	6.03×10^{-7}	1.07×10^{-6}	1.33×10^{-6}
16			2.83×10^{-9}	2.28×10^{-7}	5.13×10^{-7}	2.10×10^{-6}
17				7.67×10^{-8}	2.81×10^{-7}	2.31×10^{-6}
18				1.13×10^{-8}	1.04×10^{-7}	1.31×10^{-6}
19				$2.83 \times 10^{-}$	2.17×10^{-8}	8.25×10^{-7}
20					2.83×10^{-9}	5.13×10^{-7}
21						3.26×10^{-7}
22						2.07×10^{-7}
23						1.32×10^{-7}
24						5.10×10^{-8}
25						4.72×10^{-9}

* $P(m,31) = 0$ for $m = 26, \cdots, 31$.

Table IV—$w(m)$ for the Bose-Chaudhuri (31, 21) Code

m	$w(m)$
0	1
1	0
2	0
3	0
4	0
5	186
6	806
7	2635
8	7905
9	18910
10	41602
11	85560
12	142600
13	195300
14	251100
15	301971

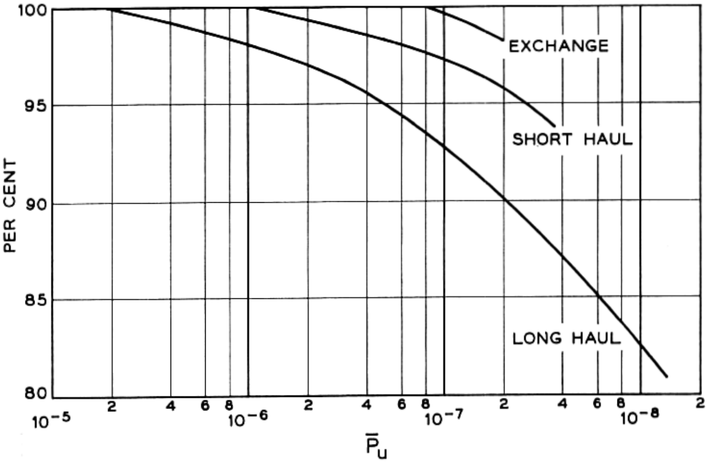

Fig. 1 — Percentage of 10-minute calls at 600 bps with undetected error probabilities not exceeding $\bar{P}_u$.

phone network, since it was not measured during the actual field test program. The records of that program do not allow accurate calculation of it for a variety of reasons.[6] We can, however, think of the recorded bit-error data from the field test program as representing the additive noise of a class of hypothetical channels, and then ask the question, "How well does $\bar{P}_u$ estimate P_u for these hypothetical channels?" To do this, a computer program was written to reconstruct the sequences

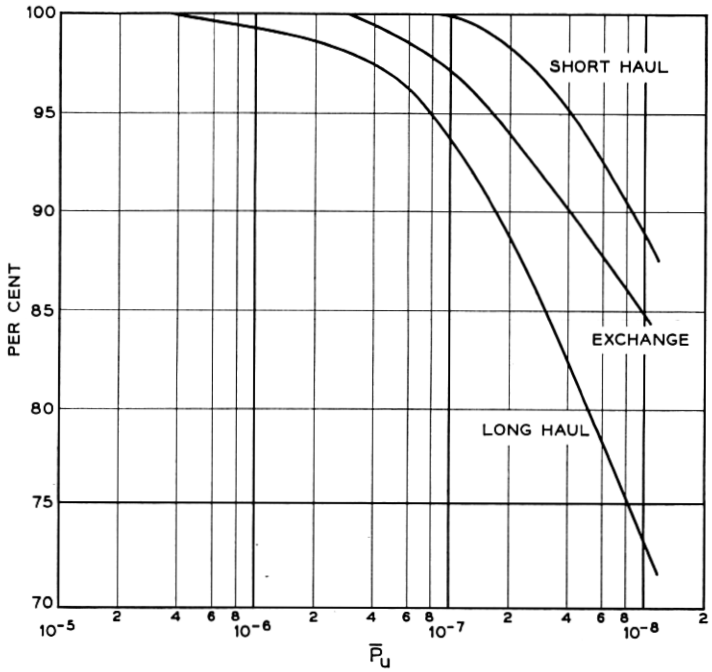

Fig. 2 — Percentage of 30-minute calls at 1200 bps with undetected error probabilities not exceeding $\bar{P}_u$.

of 1's and 0's from the sequential numbers of correct bits and error bits of the task force records. The resulting sequences are then divided into blocks of length 31, and each block is tested to determine if it is the zero word, a code word, or a noncode word. Again each call is treated as 31 calls, according to which of the first 31 bits is chosen first in determining the subdivision into blocks, and the average undetected and detected error rates are calculated.

Of the 1010 test calls in the program, only 10 contained undetected errors. The total number of word-errors was 37 out of a total of 1.06×10^9 words. This corresponds to an over-all undetected word-error rate of 3.5×10^{-8}.

To compare the estimates of $\bar{P}_u$ with the values of P_u obtained from the simulation, we note first that $P_u = 0$ for 1000 calls, whereas $\bar{P}_u$ on these calls varied over a considerable range. On the 10 calls with undetected word-errors the ratios of $P_u/\bar{P}_u$ ranged from 0.83 to 24.8, with an average value of 7.4. On 7 out of the 10 calls, $P_u/\bar{P}_u$ was less than 10. The average value of $\bar{P}_u$ over all calls was 2.8×10^{-8}, which is indeed a good approximation to the over-all error rate noted above for the simulation.

The foregoing example suggests that order-of-magnitude accuracy may be obtained using the $\bar{P}_u$ estimate for P_u in ordinary circumstances. To investigate the question of accuracy further, 35 different codes with block lengths less than 25 bits were analyzed on a variety of Gilbert channels. The exact P_u values and $\bar{P}_u$ estimates were compared and found generally to agree within an order of magnitude except in some extreme cases. In these extreme cases, both $\bar{P}_u$ and P_u are practically zero, yet their ratio is large.

It should be noted that, whereas no definitive statement about the accuracy of $\bar{P}_u$ is presently possible, there are practical advantages associated with its use. First, the analysis of the code and channel are separated so that, once the channel has been analyzed for a given block length, many codes of that block length may be evaluated and compared. Secondly, the amount of computation required is significantly less than that required using various simulation techniques. There is one notable limitation imposed on its use. When the code is very large, the amount of computation required to obtain $w(m)$ may be prohibitive. In such cases the approximation offered by (10) may be useful.

VIII. A SAMPLE SURVEY OF CODES

Table V

To further illustrate the sort of code evaluation programs that the $\bar{P}_u$ estimate may be employed in, a collection of 29 codes of various block lengths and redundancy were evaluated using the $P(m,n)$ data from the field tests as summarized in Table III. The codes are all cyclic codes with exception of the constant-weight 4-out-of-8 code, and they have, for their given block length and redundancy, the largest minimum distance attainable with cyclic codes. They are designated in Table V by the number pair (n,k), where n is block-length and k is the dimension of the code. In most cases, when there are two codes with the same (n,k) but with different $w(m)$ values, both codes are included in the evaluation. The difference between the evaluation of these codes and the previous evaluation of the Bose-Chaudhuri (31, 21) code is that here the average undetected error-rate over all calls is calculated instead of an individual rate for each call. The distribution of call types in the field test program is not ideal for taking such an average as a figure of merit, yet the average does provide a convenient single number for each code, and, moreover, a considerable delineation of requirements

TABLE V — UNDETECTED ERROR-RATE ESTIMATES FOR A SAMPLE COLLECTION OF CODES

$n = 8$		$n = 15$		$n = 17$		$n = 21$		$n = 23$		$n = 31$	
k	$\bar{P}_u$	k	$\bar{P}_u$	k	$\bar{P}_u$	k	$\bar{P}_u$	k	$\bar{P}_u$	k	$\bar{P}_u$
*	1.7×10^{-5}	11	2.6×10^{-6}	9	9.4×10^{-8}	15	6.4×10^{-7}	12	1.0×10^{-8}	21	2.8×10^{-8}
7	3.1×10^{-5}	10	1.0×10^{-6}	8	4.1×10^{-8}	12	4.9×10^{-7}	11	4.6×10^{-9}	21	3.0×10^{-8}
4	1.1×10^{-6}	7	8.4×10^{-8}			11	2.5×10^{-8}			20	1.2×10^{-8}
		6	3.7×10^{-8}			9	4.2×10^{-9}			20	1.1×10^{-8}
		6	3.5×10^{-8}			5	2.0×10^{-10}			16	8.2×10^{-10}
		5	1.2×10^{-8}							15	3.9×10^{-10}
		4	5.3×10^{-9}							15	3.5×10^{-10}
		2	1.7×10^{-9}							11	1.4×10^{-11}
										10	7.4×10^{-12}

* The 4-out-of-8 code.

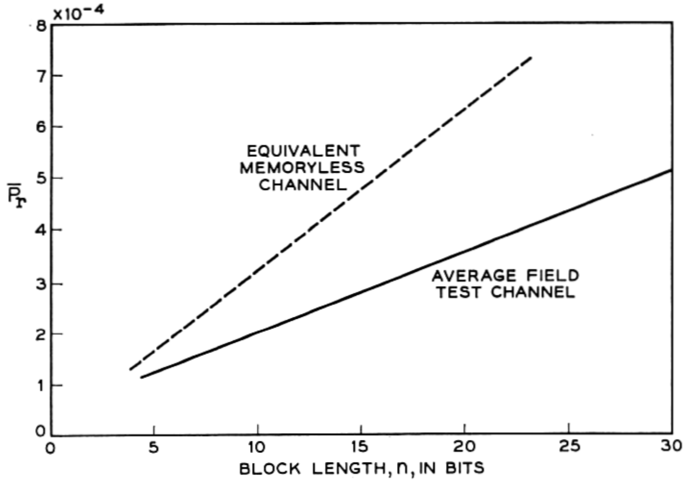

Fig. 3 — Probability of retransmission $\bar{P}_r$ versus block length n.

would be necessary to devise an improved set of weighting factors. There is the further consideration that, when ranked according to error rates, the relative positions of codes would remain almost unchanged by such a refinement.

The probability $\bar{P}_r$ of retransmission is given as a function of code block length in Fig. 3. The slight differences in $\bar{P}_r$ between different codes of the same block length are too small to be noted at three-decimal accuracy. Also plotted in Fig. 3 are the retransmission rates for a memoryless binary symmetric channel having the same average probability $P_1 = 3.2 \times 10^{-5}$ of a bit being in error. This second curve is above the first, since errors are more broadly scattered on the memoryless channel and consequently cause more retransmissions.

IX. CONCLUSIONS

In the search for suitable codes for a given data transmission service, the problem of predicting or evaluating performance is encountered. Several mathematical models of communication channels exist for which the calculation of error rates may be easily performed using parameters associated with the channel. Of such models, we note particularly that Gilbert's burst-noise channel is to be included, and we have outlined the appropriate methods for these calculations. Not all channels, however, admit to a representation by such reasonable models. At this point, models could be abandoned completely and recourse could be taken to actual field testing of a complete system or to the simulation of a complete system using data obtained in field testing. Short of such complete abandonment of models is the method of approximation of code performance factors which has been presented here. Useful mostly for error detecting codes, the method separates the analysis of performance into two parts. The channel is characterized by the probabilities of various numbers of bit errors occurring in a block of given length. A code is characterized by the average number of code words at specified distances from other code words. A simple combination of these two types of quantities gives a useful and economical indication of code performance applicable to general binary block codes and to asymmetric channels with memory. The numbers resulting from such analysis are probably more valuable for a relative indication of performance than they are for an absolute indication. In this connection, it is well to note that when error rates are very low, small differences are operationally of little significance.

As an exemplary application of this method, a collection of 29 codes was evaluated for use on the switched telephone network as error-detecting codes, in conjunction with retransmission as a means of error-correction. The codes in this collection present a wide range in reliability and indicate that it would not be difficult to select appropriate codes for specific data transmission services by suitably enlarging the class of codes examined.

X. ACKNOWLEDGMENTS

The author would like to acknowledge his indebtedness to W. R. Cowell and Robert Morris for their assistance in this undertaking and to Eric Wolman for his support and advice.

REFERENCES

1. Gilbert, E. N., Capacity of a Burst-Noise Channel, B.S.T.J. **39**, September, 1960, p. 1253.
2. Alexander, A. A., Gryb, R. M. and Nast, D. W., Capabilities of the Telephone Network for Data Transmission, B.S.T.J., **39**, May, 1960, p. 431.
3. Peterson, W. W., *Error-Correcting Codes*, John Wiley and Sons, New York, 1961.
4. Slepian, D., A Class of Binary Signaling Alphabets, B.S.T.J., **35**, January, 1956, p. 103.
5. Feller, W., *An Introduction to Probability Theory and its Applications*, Vol. I, second edition, John Wiley and Sons, New York, 1959.
6. Morris, R., Further Analysis of Errors Reported in Capabilities of the Telephone Network for Data Transmission, B.S.T.J., **41**, July, 1962, p. 1399.