The Limits of Minimum Distance Decoding

R. J. McEliece
Communications Systems Research Section

We point out that decoding algorithms which are based on the minimum distance of a block code cannot be used to achieve channel capacity. This degradation is compared with the similar degradation caused by sequential decoding.

I. Introduction

It is well-known that block coding-decoding schemes suffer several disadvantages relative to convolution coding-sequential decoding schemes. The main disadvantages are: (1) the nonexistence of a known sequence of good block codes with relatively simple decoding algorithms, and (2) the inability of good binary block-decoding algorithms to perform well when hard decisions are not used (the famous 2-dB loss on the white gaussian channel).

On the other hand, sequential decoding has a disappointing flaw: it cannot be practically used to achieve reliable communication at all rates below capacity, as R_{comp} limits performance. I wish to point out in this note that a large class of block-decoding schemes suffer from a similar handicap. The class of decoding algorithms I will consider I call *minimum distance* (MD) algorithms. An MD algorithm is one which is based on the minimum distance d of the code; i.e., it corrects up to $(d-1)/2$ errors, but no more. We shall see that on a binary symmetric channel with transition probability p, if $p > 0.075^+$, that $R_{\text{comp}}(p)$ exceeds $R_{\text{MD}}(p)$, the largest rate at which reliable communication can be achieved by an MD algorithm. For binary antipodal signalling over a white gaussian channel, with binary detector quantization, the situation is more complicated for MD algorithm: there exists a dimensionless rate $R = 0.5377^+$ at which the minimum E_b/N_0 required for reliable communication is minimum, 2.547^+. In order to surpass this with sequential decoding—again with binary quantization—one must use convolutional codes of rates < 0.3196.

II. An Unproved Assumption

Now before giving the details of this calculation, let us admit that these results depend upon an unproved hypothesis. That hypothesis is that for a fixed rate R, the largest possible value for the minimum distance of a block code of length n is asymptotically equal to $n \cdot H_2^{-1}(1-R)$, where H_2 is the binary entropy function. We really only

know that the best minimum distance is at least this good. However, this hypothesis is widely believed to be true; and if it should turn out to be false, the results of this note can easily be modified and will not be qualitatively changed.

III. The Details

The details of the calculation are quite easy. For the BSC[1] with error probability p, capacity is $1 - H_2(p)$, and R_{comp} is

$$1 - \log_2(1 + 2\sqrt{p(1-p)})$$

By our above assumption, for large n an MD algorithm will correct $\frac{1}{2}n \cdot H_2^{-1}(1-R)$ errors, and so by the law of large numbers if $p < \frac{1}{2}H_2^{-1}(1-R)$ reliable communication can be achieved. Thus we define $R_{\text{MD}}(p) = 1 - H_2(2p)$; this is the supremum of the set of rates at which MD algorithms will succeed in driving the error probabilities to zero. Figure 1 is a plot of $R_{\text{comp}}(p)/\text{Cap}(p)$ and $R_{\text{MD}}(p)/\text{Cap}(p)$ for $0 \leq p \leq 0.25$. For $p \geq 0.25$ $R_{\text{MD}} = 0$, while

$$\frac{R_{\text{comp}}(p)}{\text{Cap}(p)} \downarrow \frac{1}{2}$$

As stated above, the two curves cross at $p = 0.075355^+$.

For the white gaussian channel, with binary antipodal signalling and binary detector quantization, the calculations are only slightly more difficult. If the energy of one binary symbol is E_S, then the probability of detector error is

$$p = Q\sqrt{\frac{2E_S}{N_0}}$$

where

$$Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty \exp\left(-\frac{t^2}{2}\right)dt$$

[1]BSC = binary symmetric channel.

and $\frac{1}{2}N_0$ is the spectral density of the noise process. Instead of dealing with capacities, we wish to know the smallest E_b/N_0 for which the probability of error can be made arbitrarily small. With block (or convolutional) codes of rate R the energy available per channel symbol is $E_S = E_b \cdot R$. Thus with maximum likelihood decoding, reliable communication can be achieved if $R \leq 1 - H_2(p)$; thus the minimum E_b/N_0 is

$$\left(\frac{E_b}{N_0}\right)_{\text{min}} = \frac{1}{2R}\left(Q^{-1}[H_2^{-1}(1-R)]\right)^2 \qquad \text{(capacity)}$$

For R_{comp} the equation is

$$R \leq 1 - \log_2(1 + 2\sqrt{p(1-p)})$$

i.e.,

$$\left(\frac{E_b}{N_0}\right)_{\text{min}} = \frac{1}{2R}\left(Q^{-1}\left[\frac{1 - 2^{1-R}(2^R - 1)^{1/2}}{2}\right]\right)^2 \qquad (R_{\text{comp}})$$

Finally, for MD decoding, we need

$$p = Q\left(\left[\frac{2E_bR}{N_0}\right]^{1/2}\right) \leq \frac{1}{2}H_2^{-1}(1-R);$$

$$\left(\frac{E_b}{N_0}\right)_{\text{min}} = \frac{1}{2R}\left(Q^{-1}\left[\frac{1}{2}H_2^{-1}(1-R)\right]\right)^2 \qquad (R_{\text{MD}})$$

These values are plotted in Fig. 2. Note that both the R_{comp} and the Cap curves are monotone decreasing with R, reflecting the gains which accrue with increasing bandwidth occupancy. However, the MD curve has its minimum at $R = 0.537724^+$ for which $E_b/N_0 = 2.547^+$. In order to surpass this with R_{comp}, we see that $R \leq 0.3196^+$ is required. It is interesting to compare Fig. 2 with Fig. 6.49 in Wozencraft and Jacobs (Ref. 1, p. 442) where similar behavior was observed in the performance of BCH codes versus convolutional codes.

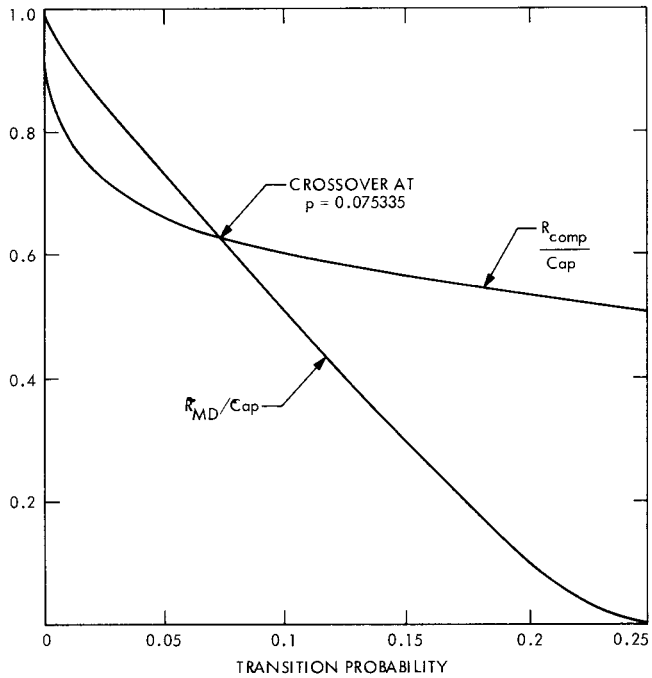

Fig. 1. Comparison of R_{comp} and R_{MD} on a binary symmetric channel

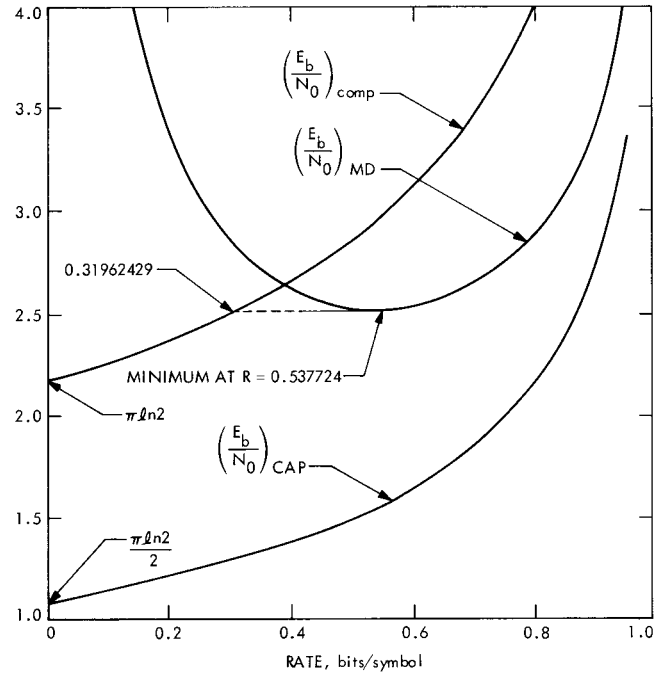

Fig. 2. Comparison of behavior of maximum likelihood sequential, and minimum distance decoding on white gaussian channel with hard limiting

Reference

1. Wozencraft, J., and Jacobs, I., *Principles of Communication Engineering*, John Wiley & Sons, New York, 1965.