THE OPTIMAL CODE RATE VS. A PARTIAL BAND JAMMER

R. J. McEliece and W. E. Stark

Coordinated Science Laboratory
University of Illinois
Urbana, IL 61801 USA

ABSTRACT

We take an abstract view of the problem of coding vs. a jammer on a binary symmetric channel, and conclude that either: coding can completely neutralize the jammer, i.e. render him no worse than uniform background noise; or: the best code rate is exactly r = .3790. Here "best" is with respect to channel capacity as a figure of merit. If the channel cutoff rate is used instead, the best rate is .247. We also give some extensions to M-ary channels, $M \geq 2$.

THE JAMMED BINARY SYMMETRIC CHANNEL

Consider a binary symmetric channel for which the crossover probability ε depends on a parameter x, a nonnegative real number, called the "signal-to-noise ratio." We assume that $\log \varepsilon$ is a convex $\cap$, decreasing function of $\log x$, so that a log-log plot of ε vs. x has the general shape usually encountered in practice (Figure 1).

We further assume that the signal-to-noise ratio is defined as the ratio of the signal power, assumed constant, to the average noise power, which is entirely due to a hostile jammer. The jammer may subject the n-th channel transmission to an "instantaneous" signal-to-noise ratio X_n, subject only to the constraint that the average noise power does not exceed a given constant. If the transmitter adopts a scrambling strategy as a countermeasure, then it is reasonable to model the sequence $\{X_n\}$ as a sequence of independent, identically distributed random variables.

Under these circumstances, the channel available to the transmitter is just a binary symmetric channel whose crossover probability is the expectation $\bar{\varepsilon} = E(\varepsilon(X))$, where X has the common distribution of the X_n's. What the jammer wants to do is to choose X so as to maximize this crossover probability subject to his or her average power constraint. In symbols, the optimization problem is:

$$\text{maximize:} \quad E(\varepsilon(X)) \tag{1}$$

$$\text{subject to:} \quad E(X^{-1}) = x^{-1} \quad . \tag{2}$$

(The constraint (2) reflects the fact that the signal-to-noise ratio x is proportional to the inverse of the jammer's average power.)

It follows, from a simple convex analysis which we omit, that the optimizing X is concentrated at only two values, X = 0, and $X = x' > 0$. If we denote the probability that $X = x'$ by ρ, then by (2) we have $x' = \rho x$, and so the optimizing distribution is in fact determined by the following simpler program:

$$\text{maximize:} \quad \rho\, \varepsilon(\rho x) \tag{3}$$

$$\text{subject to:} \quad 0 \leq \rho \leq 1 \quad . \tag{4}$$

It is quite easy to see that the solution to this problem depends on the unique positive solution x_0 to the equation

$$x_0 \varepsilon'(x_0) + \varepsilon(x_0) = 0 \quad . \tag{5}$$

The maximum possible crossover probability ε that the jammer can present to the transmitter is then given by

$$\varepsilon^*(x) = \begin{cases} \varepsilon(x) & \text{if } x \leq x_0 \text{ (here } \rho = 1) \\ \dfrac{x_0\, \varepsilon(x_0)}{x} & \text{if } x \geq x_0 \text{ (here } \rho = \dfrac{x_0}{x}) \end{cases} \quad . \tag{6}$$

Thus whatever the original dependence of ε on x, in the presence of this kind of jamming, ε is simply an inverse linear function of x, for sufficiently large signal-to-noise ratios. This relationship is easy to describe on a log-log graph: the original curve is replaced by its tangent of slope -1, for $x \geq x_0$ (Figure 1). This transformation to an inverse-linear relationship has been noted before, perhaps first by Viterbi [4].

Let us now consider how coding can be used to combat the jammer. The capacity of a BSC with crossover probability ε is given by

$$C = 1 - H_2(\varepsilon), \tag{7}$$

where $H_2(\varepsilon) = -\varepsilon \log_2 \varepsilon - (1 - \varepsilon)\log_2(1 - \varepsilon)$ is the binary entropy function. In the presence of the optimal jamming given by (6), this means that reliable coded communication is possible, provided that the code rate r satisfies

$$r < 1 - H_2(\varepsilon^*(x)) \quad . \tag{8}$$

Since x denotes the per letter signal-to-noise ratio, and r measures information bits per letter,

CH 1734-3/82-0001/$00.75

it follows that the minimum needed bit signal-to-noise ratio, which we denote by E_b/N_0, must satisfy

$$E_b/N_0 > \frac{x}{1 - H_2(\varepsilon^*(x))} \quad . \tag{9}$$

If we are in the range $x \geq x_0$, the simple relationship in (6) allows us to write, in place of (9),

$$E_b/N_0 > \frac{x_0\varepsilon(x_0)}{\varepsilon^*(1 - H_2(\varepsilon^*))} \quad . \tag{10}$$

We find numerically that the denominator in (10) is maximized at $\varepsilon^* = \varepsilon_0 = 0.1545$, corresponding to $C(\varepsilon^*) = .3790$ bits per letter. From (6), we see that the corresponding value of x is $x_0\varepsilon(x_0)/\varepsilon_0$; if this number is $\geq x_0$, i.e., if $\varepsilon_0 \leq \varepsilon(x_0)$, we reach the surprising conclusion that the transmitter's optimal code rate is exactly $r_0 = 0.3790$. On the other hand, if $\varepsilon_0 \geq \varepsilon(x_0)$, the optimal code rate will be less than r_0, but the optimizing value of ρ, the jammer's "duty factor", will be $\rho^* = 1$. A duty factor $\rho^* = 1$, in turn, corresponds to a constant signal-to-noise ratio, and this means that the best the jammer can do is to present a uniform channel to the transmitter. In summary:

$\varepsilon(x_0) \geq .1545$: optimal code rate, $r_0 = 0.3790$
optimal jamming factor $\rho^* = .1545/\varepsilon(x_0)$. (11)

$\varepsilon(x_0) < .1545$: optimal code rate < 0.3790
optimal jamming factor $\rho^* = 1$. (12)

That both of the alternatives can actually occur is illustrated by the following examples.

Example 1: (Binary FSK modulation). Here we have [5]

$$\varepsilon = \tfrac{1}{2} e^{-x/2} \quad . \tag{13}$$

An easy calculation with (5) gives $x_0 = 2$, $\varepsilon(x_0) = \tfrac{1}{2} e^{-1} = .1839$. Hence the first alternative (11) holds, the optimal code rate is 0.3790, and the jammer's optimal duty factor is $\rho^* = .1545/.1839 = 0.840$. In Figure 2, we show graphically the relationship between r, the code rate, and the minimum required E_b/N_0, for "uniform jamming", with $\rho = 1$, and jamming with ρ chosen optimally.

Example 2: (Binary PSK modulation). Here we have [5]

$$\varepsilon = Q(\sqrt{2x}) \quad , \tag{14}$$

where Q denotes the tail of a standard normal distribution,

$$Q(t) = \frac{1}{\sqrt{2\pi}} \int_t^\infty e^{-u^2/2}\, du \quad . \tag{15}$$

Another easy calculation with (5) gives $x_0 = 0.709$ [1], $\varepsilon(x_0) = 0.138$. Here the second alternative (12) holds, the optimal code rate turns out to be 0, and the jammer's optimal duty factor is $\rho^* = 1$. in Figure 3, these facts and others are displayed graphically.

SOME EXTENSIONS

The analysis in the previous section can be repeated using the channel cutoff rate $R_0 = 1 - \log_2(1+2\sqrt{\varepsilon(1-\varepsilon)})$ in place of channel capacity. Without going into the numerical details, let us simply state that if this is done, the optimizing code rate turns out to be 0.247, rather than .379. We can also extend these results to M-ary symmetric channels, for $M \geq 2$. We present the results of the straightforward calculations in the following tables.

Table 1. (M-ary Symmertric Channel, Capacity)

M	ε	r
2	.1545	.3790
4	.0833	.3964
8	.0445	.4103
16	.0235	.4216
32	.0123	.4308
64	.00637	.4383

Table 2. (M-ary Symmetric Channel, R_0)

M	ε	r
2	.136	.247
4	.073	.239
8	.039	.226
16	.020	.218
32	.011	.191
64	.0054	.185

In each table entry, "ε" denotes the channel crossover probability which optimizes (from the transmitter's viewpoint) the channel's performance, and "r" denotes the optimal code rate, measured in M-ary units. Thus, for example in Table 1, the M = 16 entry implies that the code r = .4216 is optimal, in the following sense. There is a certain positive real number a, such that if one uses codes of rate .4216, and the available "information byte" signal-to-noise ratio exceeds a, the induced channel will have capacity greater than .4216, so that if the coding is sufficiently elaborate, an arbitrary small decoded error probability is possible. However, for any rate other than .4216, the minimum needed byte signal-to-noise ratio exceeds a. Similarly the entries in Table 2 give the optimal rate, if one wishes to have the channel cutoff parameter exceed the code rate.

It is possible to show that, as $M \to \infty$, the optimal rate vs. capacity approaches 1/2, whereas the optimal rate vs. the cutoff rate approaches 0. We have observed this phenomenon before [2], and believe C, not R_0 is a better guideline for actual coded systems. We hope to say more about this interesting problem in a later paper.

Another possible extension of the results concerns jamming in the presence of side information, available to the receiver, In our discussion so far, we have assumed implicitly that the transmitter had only statistical knowledge of the crossover probability ε_n which governed the n-th channel transmission. If, however, the transmitter knows ε_n exactly, then, as we have shown elsewhere, [2], the resulting channel capacity is just the average of the capacities of the "instantaneous channels". Thus, when side information is available, we can proceed as follows.

Suppose we have an M-input channel where capacity C depends on the signal-to-noise ratio x, and that $C = C(x)$ is measured in M-ary units. If C(x) is an increasing, convex function of x, and approaches 1 as $x \to \infty$, then if side information is present, channel capacity vs. an optimal jammer is given by [3]

$$C^*(x) = \begin{cases} C(x) & \text{, for } x \le x_0 \text{ (here } \rho = 1) \\ 1 - \dfrac{A_0}{x} & \text{, for } x \ge x_0 \text{ (here } \rho = \dfrac{x_0}{x}) \end{cases} \tag{16}$$

where now x_0 is the solution to the equation

$$x_0 C'(x_0) + C(x_0) = 1, \quad A_0 = x_0(1 - C(x_0)). \tag{17}$$

As before, we now argue that since reliable communication is possible if $r < C^*(x)$, in the interval $x \ge x_0$, the minimum needed byte signal-to-noise ratio is given by

$$E_b/N_0 > \frac{x}{1 - \dfrac{A_0}{x}} = \frac{A_0}{r(1-r)} \tag{18}$$

The minimum of this expression occurs at $r = 1/2$. This leads us to the conclusion that with side information present, the optimal code rate is 1/2, independent of the receiver structure, provided that $C(x_0) \le 1/2$.

Once again, we can repeat these arguments for the cutoff rate instead of capacity. Elsewhere [2] we have shown that it is the Bhattachayra parameter D rather than R_0 which behaves linearly in this situation. The relationship between R_0 and D is

$$R_0 = 1 - \log_M(1+(M-1)D). \tag{19}$$

If $D = D(x)$ is a decreasing, convex ∪ function of x, then in the presence of optimal jamming, we have

$$D^*(x) = \begin{cases} D(x), & x \le x_0 \ (\rho = 1) \\ \dfrac{A_0}{x}, & x \ge x_0 \ \ \rho = \dfrac{x_0}{x}, \end{cases} \tag{20}$$

where x_0 is the solution to

$$x_0 D'(x_0) + D(x_0) = 0, \quad A_0 = x_0 D(x_0). \tag{21}$$

Reasoning just as before, we see that provided $x \ge x_0$,

$$E_b/N_0 > \frac{A_0}{D^*(1 - \log_M(1+(M-1)D^*)} . \tag{22}$$

By minimizing the denominator in (22), we obtain the following table of R_0-optimal code rates:

Table 3. (R_0-Optimal Code Rates, Side Information Present)

M	r
2	.454
4	.405
8	.355
16	.308
32	.266
64	.231

Of course, the code rates listed in Tables 1-3, and the single rate r=.5 for (capacity, side information present) are valid only if the corresponding jammer duty factors are less than one. We have investigated this proviso and find it to be true for M-ary FSK signalling, for all $M \ge 2$. Thus for example, for M-ary FSK, with unquantized, i.e., "soft decision" output, we find the following:

Table 4. (Various Data for M-ary FSK, Unquantized Output, Side Information Present)

M	Opt. Code Rate	(E_b/N_0),dB	Optimal ρ
2	.50	7.82	.99
4	.50	5.33	.98
8	.50	4.11	.95
16	.50	3.41	.92
32	.50	2.97	.87

As one illustration of the validity of Table 3, we cite Figure 7 in Viterbi's article [4], where one can see that the minimum needed E_b/N_0, where R_0 is the figure of merit, and 8-ary FSK as used, is about .35, as predicted by Table 3.

References

1. D. R. Martin and P. L. McAdam, "Convolutional codes with optimal jamming," International Conference on Communications (1980) Conference Record, pp. 4.3.1-4.3.7.

2. R. J. McEliece and W. E. Stark, "Channels with Block Interference," submitted to IEEE Transactions on Information Theory, November 1981.

3. W. E. Stark and R. J. McEliece, "Capacity and coding in the presence of fading and jamming," National Telecommunications Conference Record, Dec. 1981, pp. B7.4.1-B7.4.5.

4. A. J. Viterbi, "Spread-spectrum communication - myths and realities," IEEE Communications Magazine, vol. 17 (1979), pp. 11-18.

5. J. M. Wozencraft and I. M. Jacobs, Principles of Communications Engineering. New York: Wiley, 1965.

ACKNOWLEDGEMENT

This research was supported by the Joint Services Electronics Program under Contract N00014-79-C-0424.

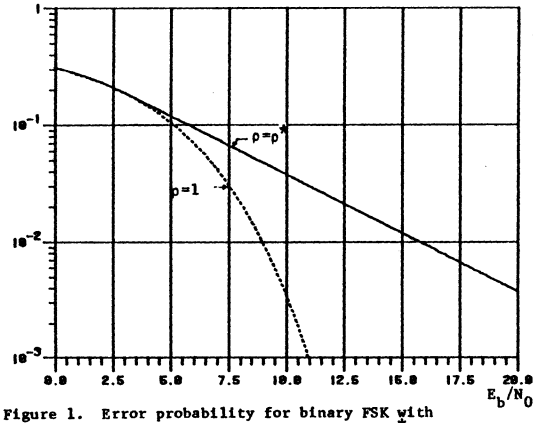

Figure 1. Error probability for binary FSK with uniform ($\rho=1$) and worst case ($\rho=\rho^*$) jamming.

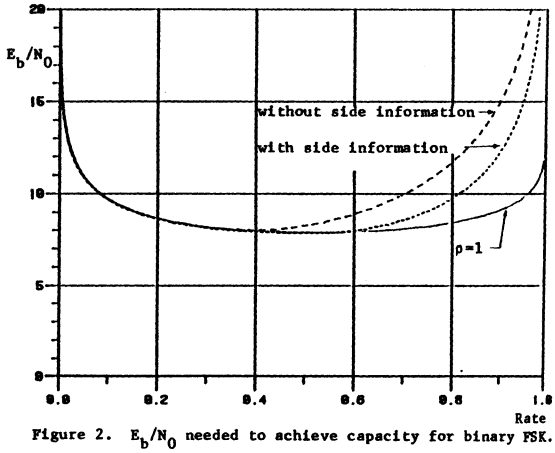

Figure 2. E_b/N_0 needed to achieve capacity for binary FSK.

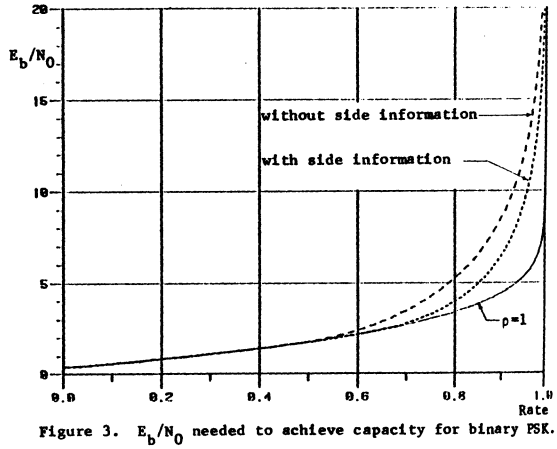

Figure 3. E_b/N_0 needed to achieve capacity for binary PSK.