THE BELL SYSTEM TECHNICAL JOURNAL
Vol. 58, No. 9, November 1979
Printed in U.S.A.

Some Theoretical Observations on Spread-Spectrum Communications

By J. E. MAZO

(Manuscript received May 25, 1979)

We consider a simple direct-sequence model of spread-spectrum communications over a bandwidth W using signals of duration T. In addition to the dimension $n = 2WT$ of signal space, the other parameters of interest are the number $(u + 1)$ of simultaneous users of the system, the error rate $Pe(u)$, and the number M of subscribers, or potential users. We investigate the relationships between these parameters, and, in particular, study the validity of the usual Gaussian approximation often used to compute $Pe(u)$. Basically, we conclude that, if M is larger than $n^2/2$, then the Gaussian approximation is not a guaranteed error rate for $(u + 1)$ users, but rather an average over all possible $(u + 1)$ users. If M is somewhat less than this number (the exact value is not known), codes can be assigned so that a uniform performance at least as good as $Pe(u)$ can be obtained, where, again, $Pe(u)$ is calculated from the Gaussian approximation. Uniform performance guarantees are given for any value of M, but they (for M large) permit fewer simultaneous users that the Gaussian approximation predicts. These bounds explicitly use the maximum cross-correlation between the signals of the different subscribers. This quantity played no role in the Gaussian approximation.

I. INTRODUCTION

In general, spread-spectrum communications refers to a class of modulation methods by which the information-bearing signal is transmitted via a modulated signal having much greater bandwidth. Two common methods are used to accomplish the spreading. In one method, direct-sequence modulation, the information signal is multiplied by a rapidly varying waveform. This waveform, which the receiver is required to know, may be thought of as having a pseudo-random character. For practical reasons, it has finite duration and is repeated in time. We refer to any particular suitable waveform, or a collection of such, as a code. The other method for spectrum spreading is frequency hopping. In this case, the available transmission band is divided into a large number of disjoint frequency intervals, and the information is conveyed by hopping from one such frequency to another. The information may be transmitted by phase-shift-keying each frequency or by using a particular set of frequencies for a particular symbol, etc. Again the code for frequency hopping must be known to the receiver.

The initial motivation for introducing such a scheme appears to be in its military use as an anti-jamming device. The jammer, not knowing the transmitter's code for spectrum spreading, must thus blanket all codes. Most of the jammer's power is wasted in codes that are orthogonal to the one in actual use.

An additional application of more commercial interest was introduced by Costas.[1] His idea was to use spread spectrum as a way to make a large bandwidth, W, available as a communication resource to many potential users without preassigning frequency divided channels (FDM) (and thus overlimiting the number of potential users) and without having a dynamic assignment of FDM (thus incurring the need and cost of external control). In modern work, this is usually accomplished, or imagined to be accomplished, by assigning "almost orthogonal" codes, or code vectors, to different users as a means to limit the mutual interference between users.

Very recently, attention has been drawn to spread spectrum as a possible modulation method for cellular mobile radio systems.[2] Our interest was drawn to this area by Henry's subsequent criticism[3] of the analysis of Cooper and Nettleton.[2] While the particular question in this controversy appears to have been resolved (in Henry's favor), our own survey of the situation has brought out some deeper questions relating to assumptions made in the analysis by Cooper, Nettleton, and Henry, and often made elsewhere. Specifically, lip service is often paid to making the codes approximately orthogonal. Yet when the performance analysis is finally made for these digital systems, one typical user is considered and all other users which are simultaneously using the channel are treated as interfering Gaussian noise having uniform power spectrum over the band of interest. Nowhere does any measure of the approximate orthogonality of the signals of different users enter the performance estimates. Our objective, then, is to examine what validity can be given to performance curves calculated using the Gaussian approximation and what relation, if any, this approximation has to the idea of approximate orthogonality of different users' signals.

To gain some insight into these questions, we examine a simple direct-sequence system designed to transmit binary data and give upper bounds or the error rate $\mathrm{Pe}(u)$ that a user will experience when there are u other users on the channel. Assuming that the bounds yield a good description, we can reach some easily stated conclusions.

Let there be M subscribers or potential users of the system and let there be $(u + 1)$ simultaneous users, $u + 1 \leq M$. Also denote the calculated error rate by $\text{Pe}(u)$. Then, by a random coding argument, we conclude for $M = u + 1$ that there is a code such that the $(u + 1)$ users each have error rate $\text{Pe}(u)$, where $\text{Pe}(u)$ is calculated via the Gaussian approximation. This, however, does not take into account the possibility that the $u + 1$ users may be selected from $M > u + 1$ subscribers. The random coding argument also suggests that, in fact, no limit need be placed on M if $\text{Pe}(u)$ is estimated from the Gaussian approximation. However, the interpretation given to $\text{Pe}(u)$ immediately changes. It is no longer an error rate for each of $(u + 1)$ users, but is an *average* error rate where the average is taken over all ways $(u + 1)$ users are selected from the subscriber population.

Next, the question of a *guaranteed* error rate for any $(u + 1)$ users is taken up. That is, we present a performance bound valid for each of the $(u + 1)$ users which is independent of how the $(u + 1)$ users are selected from the population of size M. The results show that if, in our n-dimensional signal space, we are packing so many unit energy signal vectors (corresponding to different subscribers) that the cross-correlations (cosines between vectors) are required to be as large as $(t/n)^{1/2}$ in magnitude, where $t > 1$ is simply a convenient parameter, then the number of simultaneous users is reduced by a factor of t compared to what the Gaussian approximation would predict. Finally, recent bounds by Kabatyovskii and Levenshtein for sphere-packing problems are applied to give upper bounds on M so that the $(t/n)^{1/2}$ bound on the cross-correlations can be met. For $t = 1$, the upper bound is $n^2/2$ vectors, which, for n large, is quite generous. How closely this can be approached is not known.

II. MODEL AND ANALYSIS

We consider the following simple model of direct-sequence, binary, spread-spectrum communication. We have a bandwidth W over which $u + 1$ independent users simultaneously communicate binary information with a central station at the rate $R = 1/T$ b/s. The individual information rates are small compared with the available bandwidth; thus, $TW >> 1$. There are M subscribers or potential users of the system and M may be large compared with $u + 1$, the maximum number of simultaneous users allowed. Each potential user is permanently assigned a coded carrier (or code vector). The ith subscriber's carrier $c_i(t)$ is written as

$$c_i(t) = \sum_{k=1}^{n} x_k^{(i)} \psi_k(t), \tag{1}$$

where $\psi_k(t)$ are orthonormal basis functions in the $n = 2WT$ dimensional space of functions approximately limited to W Hz in bandwidth and to T s in duration.

The entire system operates synchronously and every T seconds the ith user square-wave modulates his carrier by ± 1, the independent, identically distributed (i·i·d) binary data that he wishes to transmit.

We may consider the n real number $x_k^{(i)}$, $k = 1, \cdots, n$ forming a vector $\mathbf{x}^{(i)}$ in real n space and the collection of vectors $\{\mathbf{x}^{(i)}\}_1^M$ belonging to the different subscribers is sometimes called a code. We only consider equal energy codes and set

$$E = \int_0^T c_i^2(t)\, dt = \sum_{k=1}^{n} (x_k^{(i)})^2. \tag{2}$$

In the analysis, we distinguish the user whose performance we will be interested in by the subscript $i = 1$; the other users are designated by $i = 2, \cdots, u + 1$. Thus, in a typical T-second interval the received signal will be a time translate of

$$b_1 c_1(t) + \sum_{i=2}^{u+1} b_i c_i(t), \tag{3}$$

the b_i being the binary data, i·i·d for each user and also between users.† We assume correlation detection of (3), and thus the receiver bases its decision of b_1 on the sign of

$$b_1 \int_0^T c_1^2(t)\, dt + \sum_{i=2}^{u+1} \int_0^T c_1(t) c_i(t)\, dt = E b_1 + E \sum_{i=2}^{u+1} b_i \rho_{1i}. \tag{4}$$

In (4) we have introduced the normalized cross-correlation,

$$\rho_{ij} = \frac{\displaystyle\int_0^T c_i(t) c_j(t)\, dt}{E} = \sum_{k=1}^{n} x_k^{(i)} x_k^{(j)}. \tag{5}$$

This equals the cosine of the angle between $\mathbf{x}^{(i)}$ and $\mathbf{x}^{(j)}$ in n-space. Thus, when $|\rho_{ij}|$ is small, the vectors $\mathbf{x}_i$ and $\mathbf{x}_j$ are almost orthogonal.

Assume that $b_1 = 1$ in (4). Then the probability of error, Pe, is

$$\text{Pe} = \Pr\left[1 + \sum_{i=2}^{u+1} b_i \rho_{1i} < 0\right]. \tag{6}$$

† Such a system where the "spreading" function is modulated by the data is usually termed a direct-sequence system. Frequency hopping is another spread-spectrum technique. The relative practicality of the two techniques depends on particular circumstances.

This depends on the distribution of the noise-like quantity

$$q = \sum_{i=2}^{u+1} b_i \rho_{1i}, \tag{7}$$

where (assuming unit energy)

$$\rho_{1i} = \sum_{k=1}^{n} x_k^{(i)} x_k^{(1)}. \tag{8}$$

First let us consider not a specific code, but rather an average over all possible codes assuming all the unit vectors $\mathbf{x}^{(i)}$ are uniformly and independently distributed over the unit sphere.† In this case, note (letting $\langle\,\rangle$ denote an average)

$$\langle \rho_{ij}^2 \rangle = \frac{1}{n} \quad i \neq j, \tag{9}$$

which follows from noting that, for a unit vector, the sum of the squares of its n direction cosines add to 1, while each must have the same average.

Using the random coding assumption, the moment-generating function $M_q(s)$ of q may be shown to be

$$M_q(s) \equiv \langle e^{sq} \rangle$$

$$= \langle e^{sv} \rangle^u = \left[\frac{1}{B(1/2, (n-1)/2)} \int_{-1}^{1} e^{sv}(1 - v^2)^{n-3/2}\, dv \right]^u, \tag{10}$$

where, in (10), $B(1/2, (n-1)/2)$ is the beta function and

$$p(v) = \frac{1}{B(1/2, (n-1)/2)} (1 - v^2)^{(n-3)/2} \tag{11}$$

is the probability density of any direction cosine v of a vector uniformly distributed over a sphere in n-dimensions. A saddle point evaluation of (10) yields, for $n \gg 3$ and s/n small,

$$M_v(s) \approx e^{s^2/2n}. \tag{12}$$

Since the Chernoff bound[4] states that, for any random variable q,

$$\Pr[q < A] \leq e^{-sA} M_q(s) \quad \text{for any} \quad s < 0, \tag{13}$$

then

$$\mathrm{Pe} = \Pr[q < -1] \leq e^{s} M_q(s) \approx e^{((s^2 u/2n)+s)}. \tag{14}$$

† We could also assume that $x_k^{(i)} = \pm 1$, i·i·d, and obtain similar numbers.

Optimizing the inequality in (12) over s yields[†] $s_{opt} = -n/u$, and thus

$$\mathrm{Pe}(u) \le e^{-(n/2u)}, \tag{15}$$

where $\mathrm{Pe}(u)$ is the error rate for $(u + 1)$ simultaneous users.

We begin our discussion of (15) by reconsidering the performance question from a different point of view. Assume that the interfering power resulting from users 2 through $u + 1$ is uniformly distributed over the band W. If each user has power P, then the one-sided power spectral density N_0 thus obtained is

$$N_0 = \frac{uP}{W} = \frac{uE}{TW}. \tag{16}$$

Further assume this noise is Gaussian. As is well known, the error rate for antipodal signals, each of energy E (this is what our transmitters are using), is, in white noise of spectral-density N_0, given by

$$\mathrm{Pe} = Q\left(\sqrt{\frac{2E}{N_0}}\right) < e^{-(E/N_0)},$$
$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} e^{-y^2/2}\, dy. \tag{17}$$

The bound in (17) is exponentially correct. Using (16), the Gaussian approximation yields

$$\mathrm{Pe}(u) \le e^{-(TW/u)} = e^{-(n/2u)}, \tag{18}$$

where we have introduced the dimension $n = 2WT$. This is precisely the same as the random coding bound (15). We use the random coding argument to interpret the result of the standard Gaussian approximation. The first interpretation is that there must be a code of $(u + 1)$ vectors so that each of the $(u + 1)$ users has error rate $\mathrm{Pe}(u)$.[‡] A second interpretation is that, to achieve $\mathrm{Pe}(u)$, no limit need be placed on the number M of subscribers. They can, in fact, be assigned codes at random. The average error rate a user sees with u other users present is (15). But (15) clearly then refers to a $\mathrm{Pe}(u)$ averaged over all possible combinations of u users; it is not an error rate that can be met for any set of u other users. Some combinations of $u + 1$ users will give very bad error rates.

To see what the guaranteed level of performance can be for any $u + 1$ users selected out of a subscriber population of size M, reconsider

[†] The fact that $s_{opt} = -n/u$ justifies treating s/n small in (10).

[‡] More precisely, one can guarantee that a code exists so that a fraction $(1 - (1/\alpha))$ of the users has an error rate no larger than $\alpha \cdot \mathrm{Pe}(u)$.

(6) with the ρ_{1i} fixed. Then the standard Chernoff bound yields

$$\text{Pe} \leq \exp\left[-\frac{1}{2}\left(\sum_{i=2}^{u+1} \rho_{1i}^2\right)^{-1}\right]. \tag{19}$$

Suppose we have designed our code so that, out of the entire population of M subscribers,

$$\max_{i,j,i \neq j} |\rho_{ij}| = \rho_{\max}.$$

Then from (19),

$$\text{Pe} \leq e^{(-1/2u\rho_{\max}^2)}. \tag{20}$$

If $\rho_{\max}^2 = 1/n$, the Gaussian approximation again results. In random coding $\langle \rho_{ij}^2 \rangle = 1/n$, but nothing was said about $\rho_{\max}$ and thus nothing could be said about a guaranteed error rate.

Given M unit vectors in n space, how small can $\rho_{\max}$ be? One result in this direction is due to Welch.[5] He states that

$$\rho_{\max}^2 \geq \frac{1}{M-1}\left[\frac{M}{n} - 1\right]. \tag{21}$$

If n is large and M large compared to n, then (21) already states $\rho_{\max}^2 \geq \dfrac{1}{n}$.†

Rephrasing our question, given the dimension n and $\rho_{\max}$, how large can M be? That is, how many vectors $\mathbf{u}_i$ can we put on the unit sphere so that

$$|\rho_{ij}| = |\mathbf{u}_i \cdot \mathbf{u}_j| \leq \rho_{\max}? \tag{22}$$

This sphere-packing problem is different from the conventional one which requires

$$\rho_{ij} = \mathbf{u}_i \cdot \mathbf{u}_j \leq \rho_{\max}. \tag{23}$$

The number of vectors M will be much smaller under condition (22) than under condition (23). Luckily, our sphere-packing problem (22) was one of the packing problems recently considered by Kabatyonskii and Levenshtein.[6] Precise values of M are not known, but upper bounds are.

An extension of their work provides us with the following. For $k = 0, 1, 2, \cdots$,

† If $(n+1)$ vectors are the vertices of the regular simplex in n-space, then $\rho_{\max}^2 = 1/n^2$. Then (21) is exact for $M = n$ and $M = n + 1$.

$$M \le \frac{(1 - \rho_{\max}^2)}{(2k+1) - (n+2k)\rho_{\max}^2} (n+2k) \frac{(n/2)_k}{(1/2)_k}, \tag{24}$$

provided the denominator in (24) is positive.† In (24), we have used the notation

$$(\alpha)_k = \alpha(\alpha+1) \cdots (\alpha+k-1)$$
$$(\alpha)_0 = 1. \tag{25}$$

It is useful to write $\rho_{\max}^2$ as

$$\rho_{\max}^2 = \frac{t}{n}. \tag{26}$$

If we set $t = k =$ integer and use the same k in (24), and further assume $k^2 \ll n$, we have approximately

$$M \lesssim \frac{1}{(k+1)} \frac{n^{k+1}}{(2k-1)!!}. \tag{27}$$

Equation (24) is plotted in Fig. 1 for $n = 100$ as a function of t. The part of the curve for smallest t uses $k = 0$, the next set of t values uses $k = 1$, and so on.

In general, the value of the upper bound at $t = 1$ (where the Gaussian assumption agrees with random coding) is given by $n^2/2$. How closely this upper bound can be achieved is not clear. If, however, $t = 4$, a result of van Lint and interpreted for the present situation by Welch,[5] indicates that at least 10^4 binary (± 1) waveforms are available, compared with the bound of 4×10^5. The point is indicated by the small circle in Fig. 1.

III. CONCLUSIONS

Consideration of our simplified model has provided the following insights. Treating many other users as background Gaussian noise for a particular user is a good approximation in that a code can be found which (at least approximately) provides the calculated error rate for each simultaneous user. This is no bargain, however, for the orthogonal code would be even better in performance in the present problem, permitting more simultaneous users.‡ Evaluated as a pure modulation

† The bound (24) is valid for a real vector space. For a complex space, the following larger bound applies ($\rho = \rho_{\max}$):

$$M_{\text{complex}} \le \frac{1-\rho^2}{k+1-(n+k)\rho^2} \frac{(n)_{k+1}}{k!}.$$

‡ More explicitly, (18) states that, for a small error rate, we require $2u \ll n = 2WT$, or $u \ll WT = W/R$. However, in this model, FDM with double-sideband modulation allows about W/R users with zero error rate.

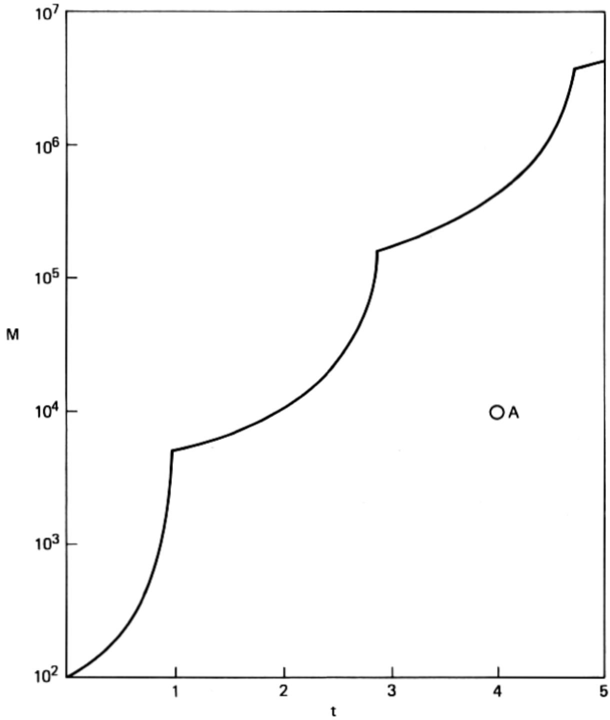

Fig. 1—Upper bound on number of signals M vs $t = n\rho^2_{max}$ for $n = 100$. The point A is known to be achievable using binary codes.

method for accommodating $(u + 1)$ known and fixed users in a white-noise channel, spread spectrum has little to offer over SSB-FDM. The only advantage for spread spectrum on the type of channel that we have considered would be as a multi-access scheme for M potential users.† Selecting codes at random for this situation still permits us to use the Gaussian approximation with u "other" simultaneous users to calculate an error rate $\text{Pe}(u)$, but only in an average sense. Namely, it is an average over all possible $(u + 1)$ users selected out of the M subscribers. To guarantee a level of performance for any $(u + 1)$ users, the departure from strict orthogonality must not be too severe, and this puts a definite restriction on the number M of potential users.

† The potential absence of channel assignment for spread spectrum is the basis of the Cooper-Nettleton (Ref. 2) proposal for spread spectrum for mobile radio. Other considerations may make spread spectrum an attractive alternative. For example, it can provide frequency diversity for a frequency-hopped system when there is fading. Such a scheme has been proposed by Goodman et al. (Ref. 7) for mobile radio, modifying Viterbi's (Ref. 8) proposal for satellites. Also in satellite systems, the Doppler shift can be large compared to data rates for individual users. Viterbi (Ref. 8) has suggested that spread spectrum would not need the large guard bands between channels that FDM would require.

While upper bounds on M were given in the text, the exact value is not known, nor, in general, did we discuss explicit construction of suboptimum codes.

IV. ACKNOWLEDGMENTS

It is a pleasure to acknowledge several helpful general discussions on spread-spectrum communications with H. E. Rowe. The author is particularly indebted to N. J. A. Sloane for alerting him to Ref. 6.

APPENDIX

Derivation of Eq. (24)

A brief outline is presented to guide the reader who wishes to rederive (24) from the results of Ref. 6.

We first summarize the relevant results of Ref. 6, given on pages 10 and 11 of that work. We will be concerned with the interval $-1 \le t \le 1$ and expansions in Jacobi polynomials $P_i^{\alpha\beta}(t)$, i denoting the degree of the polynomial. The parameters α and β depend on the dimensionality n and type (real or complex) of space that we are considering. For a real space $\alpha = (n-3)/2$, $\beta = -1/2$ $(n \ge 3)$, while for a complex space $\alpha = n-2$, $\beta = 0$ $(n \ge 2)$. Let s be a real number $-1 \le s < 1$ and denote by $R(\alpha, \beta, s)$ the set of polynomials

$$f(t) = \sum_{i=0}^{l} f_i P_i^{\alpha\beta}(t) \tag{28}$$

of degree $l = 1, 2, \cdots$ such that

$$(i) \qquad f_i \ge 0, \qquad i = 0, \cdots, k \quad \text{where} \quad f_0 > 0. \tag{29a}$$

$$(ii) \qquad f(t) \le 0 \quad \text{for} \quad -1 \le t \le s. \tag{29b}$$

Then the maximum number M of unit vectors $\mathbf{u}_i$ in n-space such that

$$|\mathbf{u}_i \cdot \mathbf{u}_j| \le \rho$$

satisfies

$$M \le \inf_{f(t) \epsilon R(\alpha,\beta,2\rho^2-1)} \frac{f(1)}{f_0}. \tag{30}$$

The evaluation of $f(1)/f_0$ for any particular allowed $f(t)$ further upper bounds (30). We choose the polynomials

$$f(t) = (t-s)(t+1)^k \qquad k = 0, 1, \cdots. \tag{31}$$

The verification of (29b) is thus trivial, as is the evaluation of $f(1)$. The verification of (29a) as well as the evaluation of f_0 is a direct calculation. We evaluate f_i using the orthogonality properties of the Jacobi polynomials $P_i^{\alpha\beta}(t)$ with respect to the weight function $w(t) = (1 - t)^\alpha(1 + t)^\beta$. The required normalization may be found in Ref. 9, p. 262, formula 1. If we rewrite (31) as

$$f(t) = (t + 1)^{k+1} - (1 + s)(t + 1)^k, \tag{32}$$

then the integrals needed to evaluate f_i may be calculated from Ref. 8, p. 263, formula 3. One then directly verifies that $f_i > 0$ $(i > 0)$ is positive whenever f_0 is, and the indicated evaluation of f_0 results in (24) for the real case.

REFERENCES

1. J. P. Costas, "Poisson, Shannon and the Radio Amateur," Proc. IRE, *47* (December 1959), pp. 2058–2068.
2. G. R. Cooper and R. W. Nettleton, "A Spread-Spectrum Technique for High-Capacity Mobile Communications," IEEE Trans. Vech. Tech., *VT-27*, No. 4 (November 1978), pp. 264–275.
3. P. S. Henry, "Spectrum Efficiency of a Frequency-Hopped-DPSK-Mobile Radio System," 29th IEEE Vehicular Technology Conference Record, March 1979, pp. 7–12.
4. Robert G. Gallager, *Information Theory and Reliable Communication*, New York: John Wiley, 1968. See pp. 126–128 for the Chernoff bound.
5. L. R. Welch, "Lower Bounds on the Maximum Cross Correlation of Signals," IEEE Trans. Info. Theory, *IT-20*, No. 3 (May 1974), pp. 397–399.
6. G. A. Kabatyanskii and V. I. Levenshtein, "Bounds for Packings on a Sphere and in Space," Problems of Information Transmission, *14*, No. 1 (January–March 1978), pp. 1–17.
7. D. J. Goodman, P. S. Henry, and V. K. Prabhu, "Preliminary Assessment of Multilevel FSK for Mobile Radio," unpublished work.
8. A. J. Viterbi, "A Processing Satellite Transponder for Multiple Access by Low-Rate Mobile Users," Proc. Digital Satellite Commun. Conf., Montreal, October 23–25, 1978.
9. Peter Beckmann, *Orthogonal Polynomials for Engineers and Physicists*, Boulder: Golem Press, 1973.