Exact and Analytically Approximate Bit Error Rates in Chaos Communication

Anthony J LAWRANCE* and Gan OHAMA**

*School of Mathematics and Statistics, University of Birmingham, Birmingham, B15 2TT UK
**Faculty of Economics, Shiga University, Hikone, Shiga 552-8522, Japan
*A.J.Lawrance@bham.ac.uk **ohama@biwako.shiga-u.ac.jp

Abstract

The calculation of bit error rates from correlation decoders in chaos communication systems, such as chaos shift-keying (CSK), has in many past papers typically involved use of the so-called analytical approximation, also called the standard Gaussian assumption (SGA). While often mathematical convenient, the SGA ignores the close probabilistic interplay of the statistical noise and dynamical behaviour. It is moments based and leads to inexact results; at best these are asymptotic or lower bounds to the exact bit error rates. The first purpose of this paper is to outline an approach to obtaining *exact* bit error rates. A second theme is that optimal decoders must be based on maximising the likelihood of the received bit data; this points to correlation decoders often being sub-optimal, in the sense of not giving the lowest bit error rates and further to their having different rates associated with each bit type. Outline treatments of correlation and optimal decoders for CSK systems and their exact bit error rates will be given. A fuller version of this work is in preparation.

I. Introduction

Every communication system requires an estimate of bit type based on received signal information; the estimate is often supplied by some form of correlation decoder, comparing a chaotic spreading sequence carrying a bit with the same sequence without the bit. A natural concern with any decoder is its accuracy, the standard assessment being that of bit error probability or rate; accuracy is not certain because of noise in the communication channel, generally additive white Gaussian noise (AWGN). The calculation of bit error probabilities for correlation decoders has therefore been undertaken for many systems. Conventionally, a rather general and approximate formula, emanating from Pursley [1] is used, and referred to as the standard Gaussian assumption or analytic approximation; originally for non-chaotic systems, it is based on the central limit theorem from statistics and moment calculations. In using it for chaos-based systems, there is very little recognition of the close interplay of the chaotic dynamics and the channel noise.

It is a purpose of this paper to obtain from first statistical and dynamical principles *exact* results for bit error probabilities in simple chaos-based communication systems. In so doing the aim is to lay a general foundation for departing from existing inexact approaches. The exact approach makes use of the implicit distributional behaviour of chaotic processes and the widely employed assumption of AWGN in the channel. A further advantage of exact results is that they enable detailed and accurate comparison of bit error rates using different amounts and types of spreading. To briefly exemplify the approach, single user CSK systems are treated. Existing literature on bit error rates for particular chaos-based models making use of the SGA includes Lipton & Dabke [2], Milanovic *et al* [3], Kolumban [4], Lawrance & Balakrishna [5], Sushchik *et al* [6] and Tam *et al* [7].

A fundamentally important issue in communications is the choice of decoding method, an operation requiring statistical estimation of bit type. Following a theme of Hasler at NOLTA2000, for instance in Schimming & Hasler [8], this is optimally based on the received and available bit data by using the standard statistical method of maximum likelihood estimation. For all but the simplest systems, the implication is that correlation decoders are not optimal; for instance, standard CSK systems, for which the likelihood optimal decoder will be presented here. Likelihood optimal decoders should induce nirvana in chaos communications.

II. Chaos-Based Communication Systems

In the *coherent antipodal* version of CSK messages to be sent are in binary form, here with a bit being coded by $b = \pm 1$. The bit is stored in a vector segment $x = (x_1, x_2, \ldots, x_N)$ of N successive values from a chaotic sequence $\{X_t\}$, the *spreading* or *reference sequence*, generated by a chaotic map $\tau(z)$, $c \leq z \leq d$. The chaotic sequence is assumed to have been started with a random value from an invariant distribution of the map, thus conferring this distribution on each subsequence variable from $\{X_t\}$; the common means of $\{X_t\}$ are denoted by $\mu = E(X_t)$ and the common variances by σ_X^2. In the simplest CSK systems the stored bit sequence is of the form $\mu + b(x - \mu)$ where the spreading sequence x is assumed to be known at the receiver without noise. The bit is thus signified by either leaving the chaotic sequence unchanged as $x\,(b=1)$, or reflecting it about its mean as $2\mu - x\,(b=-1)$. To avoid the reflected values being out of range, the spreading distribution is assumed to be symmetric. This system is equivalent to using the map $\tau(z)$ to generate the binary $+1$ symbol and switching to the map $-\tau(z)$ to generate the symbol -1; it is thus the simplest form of CSK in which distinct maps are used. The transmission channel is subject to AWGN $\{\epsilon_t\}$ with variance σ^2 and $\epsilon = (\epsilon_1, \epsilon_2, \ldots, \epsilon_N)$ denotes the noise associated with a bit sequence. Thus the received bit sequence $r = (r_1, r_2, \ldots, r_N)$ is of the form

$$r = \mu + b(x-\mu) + \epsilon. \tag{1}$$

When using a correlation decoder, the received bit b is estimated as ± 1 according as

$$C(x,r) \equiv \sum_{i=1}^{N}(x_i-\mu)(r_i-\mu) \geq, < 0. \tag{2}$$

One could statistically complain that this is more of a covariance decoder.

III. Bit Error Probability for a Simple Chaos Shift-Keying Model

The probability that a bit is estimated as -1 given that a $+1$ was transmitted is the $+1$ *bit error rate*; preferably, this should be the same as the -1 bit error rate when a -1 is transmitted. If these are not the same, the overall error probability depends undesirably on the relative proportions of the bit values transmitted. As mentioned in Section I, the aim is to calculate the bit error probabilities *exactly*, rather than approximately from the signal to noise or interference standard deviation ratio ρ and the much used standard Gaussian approximation formula $\frac{1}{2}\mathrm{erfc}\big(\sqrt{\rho}\big)$, see Kennedy, Rovatti and Setti [9], pp22-23, for instance. The exact result will be the unattainable but desired outcome of a very large Monte-Carlo simulation of the system.

Taking the conventional correlation decoder first, as given by (2), its $+1$ error rate is theoretically

$$BER(N) = P\{C(X,R) < 0 | b=1\} \tag{3}$$

where X and R denote the vectors x and r as random variables, as appropriate to a probability expression. From (2) and when $b=1$,

$$C(X,R) = \left\{\sum_{i=1}^{N}(X_i-\mu)^2 + \sum_{i=1}^{N}\epsilon_i(X_i-\mu)\right\} \tag{4}$$

The exact approach will involve evaluation of (3) conditionally on $X = (X_1, \ldots, X_N)$ and then over the stationary or invariant distribution of the spreading sequence; thus

$$\begin{aligned} BER(N) &= P\left\{\textstyle\sum_{i=1}^{N}\epsilon_i(X_i-\mu) < -\sum_{i=1}^{N}(X_i-\mu)^2\right\} \\ &= \\ &\int_{x\subset(c,d)^N} P\left\{\sum_{i=1}^{N}(X_i-\mu)\epsilon_i < -\sum_{i=1}^{N}(X_i-\mu)^2 \,\middle|\, X=x\right\} \\ &\qquad\qquad \times f_X(x)dx. \end{aligned} \tag{5}$$

The first term is now a linear combination of independent Gaussian variables with mean zero and variance $\sigma^2\sum_{i=1}^{N}(x_i-\mu)^2$; thus the most general result is

$$BER(N) = \int_{x\subset(c,d)^N} \Phi\left(-\sqrt{\sum_{i=1}^{N}(x_i-\mu)^2}\Big/\sigma\right) f_X(x)dx, \tag{6}$$

$0 \leq BER(N) \leq \frac{1}{2}$, where $\Phi(\cdot)$ is the distribution function of a standardized Gaussian random variable. This result holds for any type of spreading sequence assumed to have stationary probabilistic behaviour, and not necessarily chaotic ones, but only for Gaussian noise. Also, it is easy to see that the same result holds for the -1 error probability as well.

Some generality can be extracted from (6) before giving explicit calculations. An alternative form of (6) is

$$BER(N) = E\left\{\Phi\left(-\sqrt{\sum_{i=1}^{N}(X_i-\mu)^2}\Big/\sigma\right)\right\} \tag{7}$$

where expectation is taken over the spreading sequence X as dependent random variables. The limiting result for long spreading sequences, large N, is particularly interesting, being

$$BER(N) \simeq \frac{1}{2}\mathrm{erfc}\left\{(\sigma_X/\sigma)\sqrt{\frac{N}{2}}\right\}. \tag{8}$$

The expression thus reveals the standard Gaussian assumption or analytical approximation result $\frac{1}{2}\mathrm{erfc}\big(\sqrt{\rho}\big)$ where ρ is a standard error ratio of signal to noise, of spreading to noise in this case. By Jensen's inequality applied to (7), (8) will be a *lower bound* for the error probability, and so

$$BER(N) \geq \frac{1}{2}\mathrm{erfc}\left\{(\sigma_X/\sigma)\sqrt{\frac{N}{2}}\right\}. \tag{9}$$

Thus it is seen that the analytical approximation is in fact just a lower bound and the exact bit error may be larger than this.

The lower bound result (9) shows that for high spreading factor N the bit error probability depends only on the standard deviation of the spreading sequence and not on any statistical dependence it might have. It is also evident, other aspects being fixed, that high variance of the spreading distribution is associated with low probability of error, and that variance of the spreading sequence tending to zero implies the error probability tending to $\frac{1}{2}$, equivalent to guessing. The finite-ranged distribution with the highest variance is the balanced end-points binary, suggesting that the continuous $\beta\left(\frac{1}{2}, \frac{1}{2}\right)$ may be a good spreading distribution, as often turns out to be the case.

IV. Exact Bit Error Probability Calculations

Although primarily concerned with chaotic spreading sequences, white Gaussian ones are of interest as a low performance reference and by offering immediate tractability. Since the Gaussian distribution function $\Phi(\cdot)$ in (7) has a chi-squared distributed random variable with N degrees of freedom χ_N^2 in its argument, the exact bit error rate becomes

$$BER(N) = E\left\{\Phi\left[\left(-\left[\sigma_X/\sigma\right]\sqrt{\chi_N^2}\right)\right]\right\}. \qquad (10)$$

Reverting to chaotic spreading, the result (6) for the $BER(N)$ of antipodal CSK systems can be written as

$$\int_{x=c}^{d} \Phi\left(-\sqrt{\sum_{i=1}^{N}\left(\tau^{(i-1)}(x)-\mu\right)^2}\bigg/\sigma\right) f(x)dx. \qquad (11)$$

This key general result fully involves the chaotic dynamics and statistics of the map through its iterations $\tau^{(i-1)}(x)$, $i = 1, 2, \ldots, N$ and invariant density function $f(x)$. The required integral is only one-dimensional which is highly convenient, although its integrand may have many turning points. Evaluation will simply need a symbolic algebra package and an accurate numerical integration routine.

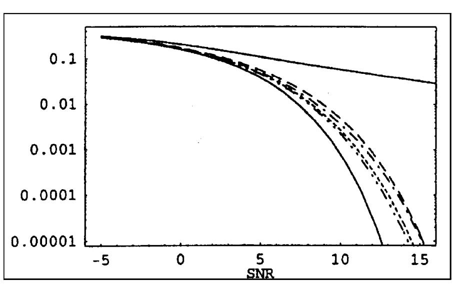

Figure 1. Bit error rate $BER(N)$ plotted against signal to noise ratio SNR in the case of chaotic logistic spreading for spreading factors $N = 1$ (upper solid line), $N = 2$ (dashed line), $N = 3$ (dot-dashed line), $N = 4$ (dotted line), $N = 5$ (dot dot dashed line) and lower bound (lower solid line).

Use of (11) is limited here to that of logistic map spreading. In Figure 1 $BER(N)$ is plotted on the log scale against SNR, the 'per bit signal to noise ratio' and measured in decibels as $20\log\left(\left(\sigma_X/\sigma\right)\sqrt{N}\right)$. This definition thus incorporates a compensation for different spreading factors N and the use of the transmission channel. The beneficial effect of chaotic spreading is immediately noticeable; the curves $N = 2, 3, 4, 5$ are bunched together much lower than the $N = 1$ case, although still a little way above the lower bound, but showing that the benefits of extensive spreading will not be great - a conclusion which could not reliably be obtained from approximate calculations.

A comparison of several spreading methods gave the order from smallest to largest BER: balanced binary (lower bound), logistic map, shift map and independent Gaussian.

V. A Brief General Treatment of Optimal Decoding in CSK Systems

In general coherent antipodal CSK systems, for each bit to be transmitted, each of two chaotic maps generate a reference segment; the maps are individually associated with a particular bit type. According to the type of bit to be sent, the appropriate segment is transmitted, necessarily through a noisy channel. In the simplest situation, the receiver has exact copies of both these reference segments without noise. The receiver thus has to identify the origin of the chaotic segment received to decode the bit. A sketch of optimal decoder results and bit error probabilities for this system, employing the previous general approach, will be given.

Suppose that the chaotic reference processes are denoted by $\{X_t\}$ and $\{Y_t\}$, both with means μ, and that these are associated with bit values $+1$ and -1, respectively. The received segments in a particular case will be denoted by $\{x_i + \epsilon_i\}$, $\{y_i + \epsilon_i\}$, $i = 1, 2, \ldots, N$ according as $b = +1$ or $b = -1$, respectively. Thus, as a function of b, the received message segment $(r_1, r_2, \ldots, r_n)$ is

$$r(b) = \left\{\frac{1+b}{2}x_i + \frac{1-b}{2}y_i + \epsilon_i, \quad i = 1, 2, \ldots, N\right\}. \qquad (12)$$

The likelihood of this received segment as a function of b, assuming AWGN with probability density function $f_\epsilon(\cdot)$, is given by $l\left(b|r, x, y\right)$ as

$$\begin{aligned} & \prod_{i=1}^{N} f_\epsilon\left\{r_i - \tfrac{1+b}{2}x_i - \tfrac{1-b}{2}y_i\right\} f_X(x) f_Y(y) \\ = \; & \prod_{i=1}^{N} \tfrac{1}{\sigma\sqrt{2\pi}} \exp\left\{-\tfrac{1}{2\sigma^2}\left(r_i - \tfrac{1+b}{2}x_i - \tfrac{1-b}{2}y_i\right)^2\right\} \\ & \times f_X(x) f_Y(y). \end{aligned} \qquad (13)$$

The likelihood ratio can now be presented as

$$l(+1|r,x,y)/l(-1|r,x,y) =$$

$$\exp\left\{\frac{1}{\sigma^2}\left[C(r,x) - C(r,y) - S(x,y)\right]\right\} \quad (14)$$

where

$$S(x,y) = \frac{1}{2}\left[\sum_{i=1}^{N}(x_i-\mu)^2 - \sum_{i=1}^{N}(y_i-\mu)^2\right].$$

The result (14) produces an explicit likelihood optimal decoder as

$$\hat{b} = \begin{cases} +1 \text{ if } C(r,x) \geq C(r,y) + S(x,y) \\ -1 \text{ if } C(r,y) > C(r,x) + S(y,x) \end{cases}. \quad (15)$$

The form of this optimal decoder is seen to be an interesting and simple modification of the known *maximum correlation decoder*. The exact bit error probabilities for the optimal decoder (15) can be explicitly obtained, both when the reference segments are perfectly known and with noisy transmitted reference segments. In the former case, the $+1$ bit error rate is

$$E\left\{\Phi\left(-\frac{1}{2}\sqrt{\sum_{i=1}^{N}(X_i-Y_i)^2}\Big/\sigma\right)\right\}, \quad (16)$$

applying equally to -1 bits.

For the so-called maximum correlation decoder, the exact error rate for bit type $+1$ is

$$E\left\{\Phi\left(-\frac{1}{\sigma}\,\frac{\sum_{i=1}^{N}(X_i-\mu)(Y_i-\mu)}{\sum_{i=1}^{N}(X_i-Y_i)^2}\right)\right\}. \quad (17)$$

This detector is definitely sub-optimal because of (17) possibly being greater than one-half and different to the -1 rate, as apparent by symmetry from (17).

Further results for optimal decoders with transmitted and hence noisy reference sequences can also be obtained, along with their associated exact bit errors. Theoretically exact studies confirm their superiority.

VI. References

1. M.B. Pursley, "Performance evaluation for phase-coded spread-specturm multiple-access communication - Part 1: System Analysis", *IEEE Transactions on Communications*, vol. Com. **25**, pp 795-803, 1977.

2. J.M.Lipton and K.P. Dabke, "Spread spectrum communications based on chaotic systems", *International Journal of Bifurcation and Chaos*, **12A**, 2361-2374, 1996.

3. V. Milanovic, K.M. Syed and M. Zaghloul, "Combating noise and other channel distortions in chaotic communications", *International Journal of Bifurcation and Chaos*, **7**, 215-225, 1997.

4. G. Koloumban, "Theoretical noise performance of correlator-based chaotic communications systems", *IEEE Transactions on Circuits and Systems - I: Fundamental Theory and Applications*, **47**, 12, 1692-1701, 2000.

5. A.J.Lawrance and N. Balakrishna, "Statistical aspects of chaotic maps with negative dependency in a communications setting", *Journal of the Royal Statistical Society, Series B*, **63**, 843-853, 2001.

6. M. Sushchik, L.S. Tsimring and A.R. Volkovskii, "Performance analysis of correlation-based communication schemes utilizing chaos", *IEEE Transactions Circuits and Systems -I: Fundamental Theory and Applications*, **47**, 1684-1691, 2000.

7. W.M. Tam, F.C.M. Lau, C.K. Tse and M.M. Yip, "An approach to calculating the bit-error rate of a coherent chaos-shift-keying digital communication system under a noisy multiuser environment", *IEEE Transactions on Circuits and Systems - I: Fundamental Theory and Applications*, **49**, 210-233, 2002.

8. T. Schimming and M. Hasler, "Optimal detection of differential chaos-shift-keying", *IEEE Transactions on Circuits and Systems - I: Fundamental Theory and Applications*, **47**, 1712-1719, 2000.

9. M.P. Kennedy, R. Rovati and G. Setti (eds), *Chaotic Electronics in Telecommunications*. CRC Press, London, 2000.