$$^{(-1)}C(x) = \frac{1}{^{(+1)}C_l}x^l + \frac{^{(+1)}C_1}{^{(+1)}C_l}x^{l-1} + \ldots + \frac{^{(+1)}C_{l-1}}{^{(+1)}C_l}x + 1 \quad (5)$$

In the first part of the algorithm (Fig. 2*a*) the numbers $^{(+1)}z$ and $^{(-1)}z$ of the correctly generated output digits of the current shift-register structure, with regard to the components of the given sequence as well as the discrepancies $^{(+1)}\Delta$ and $^{(-1)}\Delta$, are evaluated in both directions. If a stop criterion, which is specific for each application (i.e. some upper bound of $N$ or $L$) is not achieved, the length of a new LFSR is calculated. After this the new LFSR is computed in the next part of the algorithm (Fig. 2*b*) which contains the fundamental steps of the conventional BMA (Fig. 2*c*). The two-sided synthesising algorithm is realised by the insertion of a reversal of intermediate results within the synthesising process in the second part of Fig. 2*b*. This preprocessing of the polynomials and variables to resume the synthesis for further correction steps in the opposite direction is the decisive part of the extended algorithm. An example in Fig. 3 explains in detail how the algorithm works.

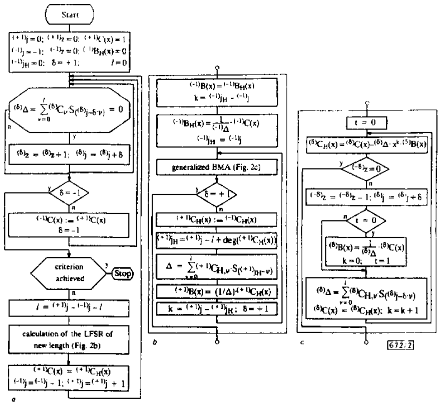
Start
criterion achieved
Stop
calculation of the LFSR of new length (Fig. 2b)
generalized BMA (Fig. 2c)
a
b
c
672/2

**Fig. 2** *Modified Berlekamp-Massey algorithm for a two-sided shift-register synthesis, two-sided calculation of LFSR of new length, and generalised Berlekamp-Massey algorithm for both directions of processing*

*a* Modified Berlekamp-Massey algorithm
*b* Calculation of LFSR of new length
*c* Generalised Berlekamp-Massey algorithm

| $\underline{S}=(\ldots, S_{-3}, S_{-2}, S_{-1}, S_0, S_1, S_2, \ldots)=(\ldots, 2, 4, 3, 0, 5, 6, \ldots)$ | |
|---|---|
| Fig.2a | $^{(+1)}j=0$ $^{(+1)}z=0$ $^{(+1)}C(x)=1$<br>$^{(-1)}j=-1$ $^{(-1)}z=0$ $l=0$ $\delta=+1$ |
| | $^{(+1)}j=1$ $^{(+1)}z=1$ $^{(+1)}\Delta=5$<br>$^{(-1)}j=-1$ $^{(-1)}z=0$ $^{(-1)}\Delta=3$ $\delta=-1$ |
| | $l=2$ |
| Fig.2b | $^{(-1)}B(x)=0$ $k=1$ |
| Fig.2c | $^{(-1)}C_H(x)=1$ |
| | $^{(+1)}z=0$ ? no |
| | $^{(+1)}j=1$ $^{(+1)}z=0$ $^{(+1)}\Delta=5$ $^{(-1)}C(x)=1$<br>$^{(-1)}j=-2$ $^{(-1)}z=0$ $^{(-1)}\Delta=4$ $^{(-1)}B(x)=5$ $k=1$ |
| | $^{(-1)}C_H(x)=1+x$ |
| | $^{(+1)}z=0$ ? yes |
| Fig.2b | $\delta=+1$ ? no |
| | $^{(+1)}C_H(x)=1+x$ $^{(+1)}j_H=0$ $\Delta=3$<br>$^{(+1)}B(x)=5+5x$ $k=1$ $\delta=+1$ |
| Fig.2c | $^{(+1)}C_H(x)=1+3x+3x^2$ |
| | $^{(-1)}z=0$ ? yes |
| Fig.2b | $\delta=+1$ ? yes |
| Fig.2a | $^{(+1)}C(x)=1+3x+3x^2$ $^{(+1)}j=2$ $^{(-1)}j=-3$ |
| | $^{(+1)}\Delta=^{(-1)}\Delta=0$ STOP |

672/3

**Fig. 3** *Example of algorithm's run for a given sequence cutting S with components being members of the finite field GF(7)*

*Applications:* The two-sided shift-register synthesising algorithm can be applied to such problems where a fixed beginning or end of the given sequence is not known *a priori*. One example is found in the decoding process of some inhomogenous block codes where the construction is based on Reed-Solomon codes [2]. In this case only the centre of the syndrome, but no syndrome size, is known before solving the key equation. Other applications are visible in cases where we are not only interested in the final but also in intermediate results of the synthesising process. An example is given in the design of stream ciphers in cryptography [5], as seen in Fig. 4. The linear complexity profile of a finite sequence differs for various starting points within the sequence using the two-sided and the conventional LFSR synthesising algorithm.

$\underline{S} = (\ldots, S_{-4}, S_{-3}, S_{-2}, S_{-1}, S_0, S_1, S_2, S_3, \ldots) = (\ldots, 5, 2, 4, 3, 0, 5, 6, 3, \ldots)$

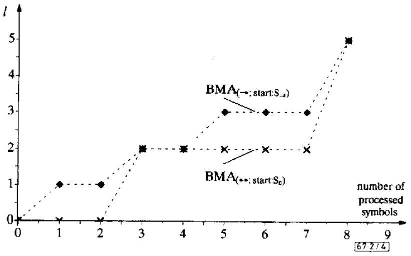

**Fig. 4** *Different linear complexity profiles as results of two-sided ($BMA_{(\leftrightarrow)}$) and conventional ($BM_{(\rightarrow)}$) LFSR synthesising algorithm*

*Acknowledgment:* The author is grateful to J. Massey of the Swiss Federal Institute of Technology (Zürich) for all helpful suggestions.

© IEE 1995 *3 January 1995*
*Electronics Letters Online No: 19950438*

M. Fleischmann (*Technical University Munich, Chair for Communications, Arcisstraße 21, D-80290 München, Germany*)

## References

1 BLAHUT, R.E.: 'Theory and practice of error control codes' (Addison-Wesley Publishing Company, MA, 1984)
2 FLEISCHMANN, M.: 'The construction and decoding of inhomogenous block codes'. Proc. 1994 IEEE Int. Symp. Information Theory, Norway, July 1994, pp. 101
3 MASSEY, J.L.: 'Shift-register synthesis and BCH decoding', *IEEE Trans.*, 1969, **IT-15**, (1), pp. 122–127
4 MICHELSON, A.M., and LEVESQUE, A.H.: 'Error-control techniques for digital communications' (John Wiley & Sons, New York, 1985)
5 RUEPPEL, R.A.: 'Analysis and design of stream ciphers' (Springer-Verlag, Berlin, 1986)

# BER and outage probability for land mobile satellite channel with maximal ratio combining

C. Tellambura, A.J. Mueller and V.K. Bhargava

*Indexing terms: Bit error rate, Mobile radio systems, Satellite relay systems, Phase shift keying*

An exact analytical technique is presented for computing the average bit error rate (BER) and outage probability of differentially detected PSK in the land mobile satellite channel (LMSC) when $L$ branch maximal ratio combining (MRC) is employed. Following a previous empirical study, the LMSC is modelled as a weighted sum of Rice and Suzuki distributions. Numerical results are provided.

*Introduction:* With the growing interest in satellite communications to provide personal communications services (PCSs), exact analytical expressions for the BER and outage probability are required in order to design effective signalling and error control coding schemes. A previous study [1] suggests a composite model for the fading of the received signal in the LMSC, based on empirical measurements. The channel can be in a 'good' or 'bad' state a fraction of the time. The fading in the 'good' state is relatively benign and is represented by a Rician distribution. The fading in the 'bad' state is modelled by a Rayleigh distribution superimposed on a lognormal distribution, known as a Suzuki distribution [3].

This work extends the previous study [1] in three ways: by using a moment generating function (MGF) approach, a computationally simple formula for the BER is derived; the BER formula is generalised for $L$ branch MRC antenna diversity; the BER outage probability is determined.

For a static AWGN channel, the signal-to-noise ratio (SNR) is a fixed quantity, but for the fading channel, it is a random variable. Thus, we are interested in the expected value of the BER given by the integral over the range $0 < S < \infty$:

$$\overline{P}_e = E_S[P_e] = \int_0^\infty P_e(S)p(S)dS \qquad (1)$$

where $S$ is the instantaneous signal power, $P_e(S)$ is the BER as a function of $S$ and $p(S)$ is the probability distribution (PDF) of the faded signal power. The MGF of $S$ is given as $m(z) = E_S[\exp(-zS)]$ (which is related to the characteristic function as $m(z) = \psi(jz)$). An elementary but useful observation is that if $P_e(S)$ is an exponential function of $S$, then the average BER, $\overline{P}$, can be obtained directly from the MGF. This fact is fully exploited in the following development.

*Analysis:* During periods of Rician fading, the PDF of the momentary received power follows a noncentral chi-squared distribution with two degrees of freedom. Using the previous notation [1], the PDF of the received power is $p_{Rice}(S) = c\exp[-c(S+1)]I_0(2c\sqrt{S})$ where the Rician factor $c = C/M$ represents the direct-to-multipath power ratio and $I_0(x)$ is the zero-order modified Bessel function of the first kind. Note that this Rician model is obtained by setting the unfaded mean signal power to unity.

When shadowing is present, the momentary received power obeys the central chi-squared distribution with two degrees of freedom. Referred to as Rayleigh fading, the PDF for a mean power $S_0$ is $p_{Rayl}(S|S_0) = (\exp[-S/S_0])/S_0$. The mean power $S_0$ fluctuates with shadowing and has a lognormal PDF given as

$$p_{ln}(S_0) = \frac{10}{\sqrt{2\pi}\sigma\ln(10)S_0}\exp\left[-\frac{(10\log S_0 - \mu)^2}{2\sigma^2}\right] \qquad (2)$$

where $\sigma$ is the logarithmic standard deviation in dB and $\mu$ is the local mean power in dB. The combined Suzuki distribution is then

$$p_{Suzuki}(S) = \int_0^\infty p_{Rayl}(S|S_0)p_{ln}(S_0)dS_0 \qquad (3)$$

For the time shared model proposed in [1], where $A$ is the time share factor, the net probability distribution of the received power is

$$p(S) = (1-A)p_{Rice}(S) + Ap_{Suzuki}(S) \qquad (4)$$

When $L$ branch MRC antenna diversity is used at the receiver, the total signal power $S$ is the sum of the received signal power $P_i$, $i = 1,...,L$ from each antenna. Assuming sufficient antenna separation, the multipath fading components (Rician or Rayleigh) for each antenna are independent and identically distributed. We further assume that the signals received in different diversity branches experience the same shadowing effects. That is, in the bad state, for $i = 1,...,L$, the mean of $P_i$ is given by $S_0$ (eqn. 2). This is reasonable in that shadowing is a larger-area effect.

*(i) Average BER:* The MGF for the Rician fading process [2] with $L$ branch MRC diversity is

$$m_1(z) = \left(\frac{c}{c+z}\right)^L \exp\left(\frac{-zcL}{c+z}\right) \qquad (5)$$

Following the derivation of the Suzuki MGF without diversity given in [3], but using the MGF for Rayleigh fading [2] with $L$ branch diversity, the MGF for the Suzuki distribution with diversity can be obtained. Using Hermitian integration, the exact closed form expression for the MGF is

$$m_2(z) = \frac{1}{\sqrt{\pi}}\sum_{i=1}^{n} w_i\left[1 + z10^{(\sqrt{2}\sigma x_i+\mu)/10}\right]^{-L} + R_n \qquad (6)$$

where $x_i$ and $w_i$ are the $i$th abscissa and weight, respectively, of the $n$th order Hermite polynomial (tabulated in [4]) and $R_n$ is a remainder term, tending to zero as $n \to \infty$.

For a static AWGN channel, assuming matched filter reception, the BER expression [2] for DPSK is $P_e(S) = \exp[-S(E_{link}/N_0)]/2$ where $E_{link}/N_0$ is the SNR for an unfaded link. Therefore, in light of eqns. 4 – 6, the average BER becomes

$$\overline{P}_e = \frac{1}{2}[(1-A)m_1(z) + Am_2(z)]\bigg|_{z=E_{link}/N_0} \qquad (7)$$

For the fading distribution parameters obtained in [1] through measurements for the Munich area, eqn. 7 can be evaluated. Fig. 1 illustrates the BER for $L$ = 1, 2 and 3 for the city and highway environments. For comparison, the BER for an ideal Gaussian channel is also shown. At the $10^{-2}$ BER level, the use of two-branch diversity reception reduces the required SNR by 8 and 5 dB for the city and highway environments, respectively.

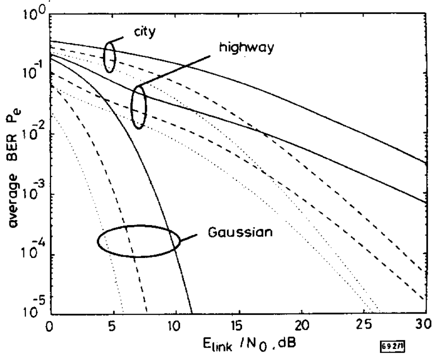

**Fig. 1** *BER for DPSK with $L$ = 1, 2 and 3 for city and highway environments around Munich*

The BER performance for Gaussian is provided for comparison
——— $L = 1$
- - - - $L = 2$
········· $L = 3$

*(ii) Outage probability:* The BER outage probability $P_{out}$ is defined as the probability that the instantaneous BER exceeds some threshold $\varepsilon$. Because $P_e(S)$ is a monotonically decreasing function of $S$, $P_{out}$ can be written as $P_{out} = P(S < \hat{S}) = CDF(\hat{S})$ where $\hat{S}$ is the solution to $P_e(S) = \varepsilon$. For DPSK, assuming a static AWGN channel and matched filter reception, $\hat{S} = [-\ln(2\varepsilon)]/[E_{link}/N_0]$.

The CDF for Rician fading [2] with $L$ branch MRC diversity is

$$CDF_1(S) = 1 - Q_L\left(\sqrt{2c}, \sqrt{2cS}\right) \qquad (8)$$

where $Q_n(x)$ is the generalised Marcum $Q$ function [2, 4].

Performing the inverse Laplace transform on eqn. 6, a closed form expression of the corresponding PDF can be obtained from which, through integration, the CDF can be found:

$$CDF_2(S) \simeq \frac{1}{\sqrt{\pi}}\sum_{i=1}^{n} w_i\left[1 - e^{-S/a_i}\left(\sum_{m=0}^{L-1}\frac{(S/a_i)^m}{m!}\right)\right] \qquad (9)$$

where $a_i$ is equal to 10 raised to the power $(\sqrt{2}\sigma x_i+\mu)/10$.

From eqns. 4, 8 and 9, the outage probability can be written as

$$P_{out} = (1-A)CDF_1(S) + ACDF_2(S)\bigg|_{S=\hat{S}} \qquad (10)$$

Fig. 2 illustrates the outage probability for an unfaded link SNR of 10dB, $L$ = 1, 2 and 3 for the Munich city and highway environments, as well as for the ideal Gaussian environment. At the $10^{-1}$ threshold, the use of diversity reception reduces the outage from 45% for no diversity to 24% for two branch or 14% for three branch diversity in the city environment.

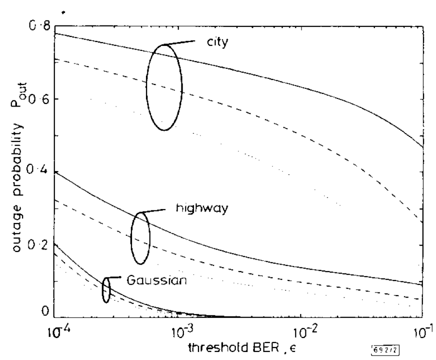

**Fig. 2** *Outage probability for DPSK with L = 1, 2 and 3 for city and highway environments around Munich*

The BER performance for Gaussian is provided for comparison
——— $L = 1$
- - - $L = 2$
········ $L = 3$
$SNR$ = 10dB

*Conclusions:* In this Letter, exact expressions for the average BER and outage probability for the Rician/Suzuki channel model were derived for the general case of $L$ branch MRC diversity. The BER and outage probability performance for DPSK in the city and highway environments around Munich was determined. This showed that MRC diversity provides significant improvements in the BER and outage probability. Furthermore, using the BER and outage probability expressions developed, the gains from diversity as a function of other system parameters such as satellite elevation angles and time share factors could be easily obtained. All the results herein can be readily modified to the case of non-coherent binary FSK by substituting $E_{link}/N_0$ with $E_{link}/(2N_0)$.

*19 December 1994*
*Electronics Letters Online No: 19950461*

C. Tellambura, A.J. Mueller and V.K. Bhargava (*Department of Electrical and Computer Engineering, University of Victoria, PO Box 3055, MS 8610, Victoria, British Columbia, V8W 3P6, Canada*)

## References

1 CYGAN, D.: 'Analytical evaluation of average bit error rate for the land mobile satellite channel', *Int. J. Satell. Commun.*, 1989, 7, pp. 99–102

2 PROAKIS, J.G.: 'Digital communications' (McGraw-Hill, New York, 1989)

3 LINNARTZ, J.-P.: 'Narrowband land-mobile radio networks' (Artech, MA, 1993)

4 ABRAMOWITZ, M., and STEGUN, I.: 'Handbook of mathematical functions' (Washington: National Breau of Standards, 1972)

# Bit-interleaved Hamming code for linearly repeatered terrestrial SDH transmission systems

Y. Yamabayashi, M. Tomizawa, T. Kataoka, Y. Kobayashi and K. Hagimoto

*Indexing terms: Synchronous digital hierarchy, SONET, Error correction codes*

A bit-interleaved SEC shortened Hamming code is proposed for all SDH levels. The error caused by ASE noise in a 156Mbit/s optical preamplifier is successfully corrected.

One of the important applications of Er-doped fibre amplifiers (EDFAs) is as linear repeaters (L-REPs) because they reduce the number of regenerators (REPs) in end-to-end transmission and decrease total network cost. Decreasing the number of REPs yields higher cost effectiveness; however, optical noise accumulation in the L-REPs limits the REP span [1]. Overcoming such degradation of signal quality is a crucial issue for implementing longer-span systems. To that end, the forward error-correction (FEC) code is the most promising digital technology for cost-effective and high-quality transmission systems.

Efforts are now being made to apply FEC coding techniques in optical transmission systems, particularly in submarine transoceanic systems. Usually, multiple-error-correcting codes, such as the Bose-Chandhuri-Hocquenghem code [2] or the Reed-Solomon code [3], are selected. Despite their excellent correcting capability, these codes increase the line rate, which may not be affordable in terrestrial high-speed systems. Line rate increases can be avoided if the check bits can be mapped into the existing unused overhead bytes in the signal frame. Grover and Moore proposed an STS-1 path (52 Mbit/s) that is encoded in the (6208, 6195) cyclic Hamming code [4]. 13 check bits are mapped into the path overhead (POH) auxiliary bytes in the SONET format. It requires no modification to the physical interface or the section termination circuits on the line. However, it is not straightforward to apply this proposal to paths other than STS-1. Concatenated virtual containers, such as VC-4-$X$c ($X$ = 1,4,16), will be introduced soon to convey ATM cells. Different codes have to be devised for those high-speed paths. In an interesting development, Paxal *et al.* have proposed the Reed-Solomon (524, 522) code [5], where the STM-1 payload is divided into three parts and each fraction is coded in 12 parallel manner. The FEC is independent of path size; however, an FEC circuit must be deployed in each REP, and all REP circuits would have to be customised. In addition, the code requires different coding circuits for different STM-$N$ ($N$ > 1) systems, while the decoding process in each REP causes the accumulation of significant end-to-end delay. In this Letter we propose a single cyclic Hamming code for all SDH signal variants that is compatible with non-FEC systems: it also suppresses delay accumulation [5].

First, we consider where to deploy coding/decoding circuits in SDH network elements: path terminating equipment (PTE) [4], line terminating multiplexer (LT-MUX) or REP [5]. The LT-MUX is adopted as the practical solution considering the various SDH levels possible. In the LT-MUX, the FEC circuit can be applied regardless of multiplexing number $N$ because the STM-$N$ frame is a byte-multiplex construction of the STM-1 frame. Moreover, the coding circuit supports all AU-4-$X$c because they are mapped into STM-1 at the LT-MUX. The codeword is the administrative unit (AU)-4, and the check bits are mapped into the multiplex section overhead (MSOH). The number of possible check bytes is 24 × $N$ for any STM-$N$ system, so there is no byte shortage for correction purposes as $N$ increases. Placing the FEC code in the LT-MUX offers an intermediate value of delay accumulation between that in PTE and that in REP. In the prototypical model which has 5000km end-to-end paths with LT-MUXs every 2500km and REPs every 250km, placing FEC in REPs yields 110 times larger delay than in PTE, while in LT-MUX the delay is increased by a factor of 10. In the LT-MUX, the FEC function should be placed between multiplex section protection (MSP) and multiplex section termination (MST) to prevent the MSP from switching the transmission line before error correction. BIP-$N$ $X$ 24 is kept for watching the raw performance of the line BER independent of coding; protection switching can be initiated based on the FEC output.

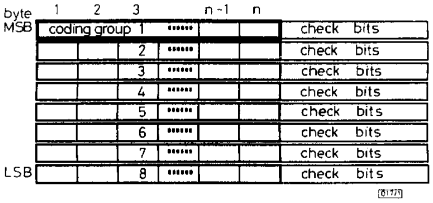

**Fig. 1** *Bit-interleaved coding*