ON THE OPTIMAL LABELING FOR PSEUDO-CHAOTIC PHASE HOPPING

Zbigniew Galias∗

Department of Electrical Engineering
University of Mining and Metallurgy
al. Mickiewicza 30, 30–059 Kraków, Poland

Gian Mario Maggio†

Center for Wireless Communications
University of California, San Diego
La Jolla, CA 92093-0407, U.S.A.

ABSTRACT

In this paper we introduce the PCPH (Pseudo-Chaotic Phase Hopping) telecommunication scheme, which is obtained by combining pseudo-chaotic encoding with N-ary phase shift keying. For this system, we address the problem of finding the optimal constellation labeling in order to minimize the error probability.

1. INTRODUCTION

Recently, it has been demonstrated that useful digital information can be embedded in a chaotic signal for communication purposes [1, 2, 3, 4]. The basic idea consists of controlling the dynamics of a chaotic system in order to obtain the desired symbolic sequence [1]. Symbolic dynamics may be defined as a "coarse-grained" description of the evolution of a dynamical system [5]. Namely, by partitioning the state space and associating a symbol to each partition, a trajectory of the dynamical system can be analyzed as a symbolic sequence. From this perspective, a chaotic system may be seen as a natural information source [6]. Hayes *et al.* in [1] first suggested to control the evolution of a dynamical system in order to encode useful information. More sophisticated control techniques were developed by Schweizer *et al.* [2]. Recently, similar ideas have been successfully applied in the context of UWB impulse radio [3, 7] and of DCSK (Differential Chaos Shift Keying) systems [4]. In particular, the PCTH (Pseudo-Chaotic Time Hopping) communication system [7] relies upon a pseudo-chaotic encoder whose output mimics the dynamics of the chaotic Bernoulli shift [8]. In PCTH the output of the pseudo-chaotic encoder drives a pulse position modulator (PPM), resulting in a random-like distribution of the pulses in the time domain. On the receiver side the information is retrieved by using standard Viterbi detection [9].

In this work we consider a combination of the pseudo-chaotic coding described in [7] with N-PSK (N-ary phase shift keying), realizing a spread-spectrum system that we call pseudo-chaotic phase hopping (PCPH). For such system we are interested in finding the optimal constellation labeling, that is the symbol labeling minimizing the BER (bit error rate).

2. PSEUDO-CHAOTIC PHASE HOPPING

The block diagram of the PCPH scheme is shown in Fig. 2.

∗E-mail: galias@zet.agh.edu.pl. This work was supported in part by the University of Mining and Metallurgy, grant no. 11.11.120.182.

†E-mail: gmaggio@ucsd.edu. Corporate affiliation with STMicroelectronics, AST-San Diego, e-mail: gian-mario.maggio@st.com.

2.1. Pseudo-Chaotic Encoder

The pseudo-chaotic encoder performs a spreading of the input sequence $c(k)$, mimicking the chaotic dynamics of the Bernoulli shift map, defined by [8]:

$$x_{k+1} = 2x_k \mod 1 \tag{1}$$

whose graph is shown in Fig. 1. The state x can be represented as a binary expansion:

$$x = 0.b_1b_2b_3\ldots \equiv \sum_{j=1}^{\infty} 2^{-j} b_j \tag{2}$$

where each of the bits b_j is either 0 or 1, and $x \in I = [0, 1]$. The successive iterates of x are obtained by moving the separating point one position to the right (multiplication by 2) and setting to zero the integer digit (modulo 1 operation). The information is encoded by associating the symbol "0" to the subinterval $I_0 = [0, 0.5)$ and the symbol "1" to $I_1 = [0.5, 1]$, as shown in Fig. 1.

In this work the Bernoulli shift process is approximated by means of an M-bit shift register followed by a DAC (digital/analog converter), as illustrated in Fig. 2. Correspondingly, the generic state x_l (with $l = 1, 2, \ldots, 2^M$) can be expressed as:

$$x_l = 0.b_1b_2\ldots b_M \equiv \sum_{j=1}^{M} 2^{-j} b_j \tag{3}$$

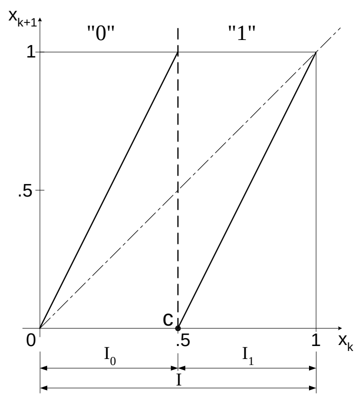

Fig. 1. The Bernoulli shift map. The invariant interval $I = [0, 1]$ is partitioned with respect to $c = 0.5$. The subintervals I_0 and I_1 are assigned the binary symbols "0" and "1", respectively.

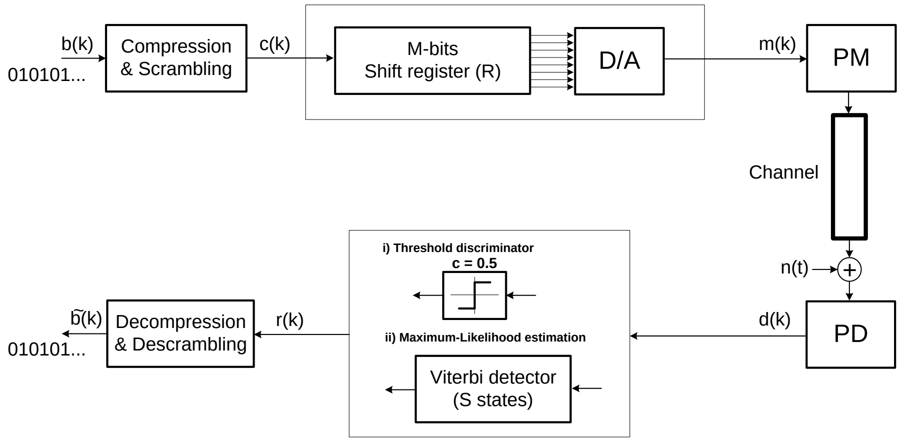

Fig. 2. Simplified block diagram of the PCPH scheme.

where b_1 and b_M represent the MSB (most significant bit) and the LSB (least significant bit), respectively. The shift operation corresponds to a multiplication by a factor 2, while the modulo 1 operation is realized by discarding the shifted MSB at each step. The shift register is fed with the input sequence $c(k)$, which we assume to be i.i.d.[1] At each step the most recent bit of information is assigned the LSB position while the old MSB is discarded. Note that from the viewpoint of information theory the shift register structure implementing the Bernoulli shift may be seen as a form of convolutional coding [10].

2.2. PCPH Signal

In order to study the PCPH modulation we consider a discrete-time baseband model of a telecommunication system. This model can be shown to be equivalent to sampling (according to a sampling interval $t_0 = 1/f_0$) the continuous-time signal transmitted over an RF (radio frequency) bandlimited channel, utilizing N-ary phase shift keying. Given the k-th pseudo-chaotic iterate, x_k, we define the corresponding symbol s_k as follows: $s_k = [\cos(\varphi_k), \sin(\varphi_k)]$, where $\varphi_k = 2\pi x_k$, and $\varphi_0 = 2\pi/2^{M+1}$ is a phase offset. The corresponding signal-space diagram is shown in Fig. 3. Note that with these notations $\varphi_k \in [0, 2\pi]$. Thus, the invariant interval $I = [0, 1]$ of the Bernoulli shift, with its definition of symbolic dynamics, maps to the unit circle in the signal space. Then, for each bit of information we transmit the vector:

$$Y = [Y_1, Y_2] = \left[\sqrt{\frac{E_b}{2}}\cos(\varphi_k), \sqrt{\frac{E_b}{2}}\sin(\varphi_k)\right]$$

where E_b denotes the energy per bit.

2.3. PCPH Decoder

By assuming the input $c(k)$ to be an i.i.d. sequence, the optimal decoder for the PCPH signal is represented by a trellis matched to the dynamics of the Bernoulli shift, seen as convolutional encoder. In this work we consider soft Viterbi decoding [9] and for illustrating the branch metric computations we consider the normalized vector $y = \sqrt{2/E_b}Y$. At each step, the input of the Viterbi algorithm is a vector $\tilde{y} = [\tilde{y_1}, \tilde{y_2}]$ representing the received symbol affected by noise. By assuming that each sample is perturbed independently by additive white Gaussian noise (AWGN) it can be shown that the observation probability of receiving $\tilde{y}$, if the symbol $s_k = [s_{k1}, s_{k2}]$ was sent, is proportional to $e^{\left((\tilde{y_1}-s_{k1})^2+(\tilde{y_2}-s_{k2})^2\right)/2\sigma_n^2}$, where σ_n is the noise variance. This in terms of logarithms, according to the usual formulation of the Viterbi algorithm, translates into the branch metric: $d_k = \sqrt{(\tilde{y_1} - s_{k1})^2 + (\tilde{y_2} - s_{k2})^2}$, whose geometrical interpretation is shown in Fig. 3.

3. BER PERFORMANCE

This section is devoted to the characterization of the PCPH scheme in the presence of noise, in terms of BER (bit error rate). We consider here the interference on the channel to be just AWGN (additive white Gaussian noise). The analysis is carried out as a function of the ratio E_b/N_0, where E_b is the energy per user bit and N_0 is the single-sided spectral noise density. In particular, we study the

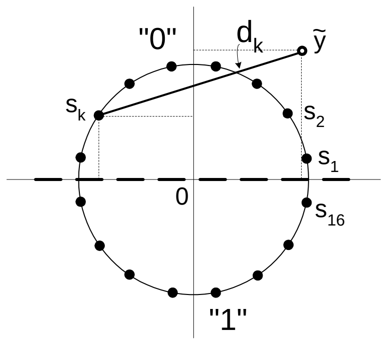

Fig. 3. Signal-space diagram for the PCPH signal (for $M = 4$) illustrating the geometrical meaning of the branch metric d_k.

[1] In practice this may be achieved by inserting a data compression and/or a data scrambling block in front of the shift register.

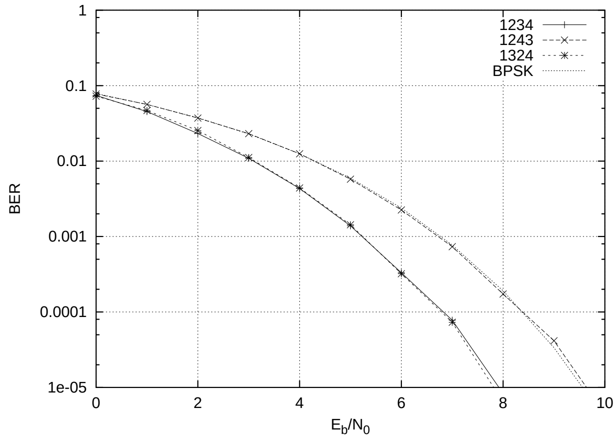

Fig. 4. BER performance of PCPH ($N = 4$). The BPSK (binary phase shift keying) curve is also plotted for reference purposes.

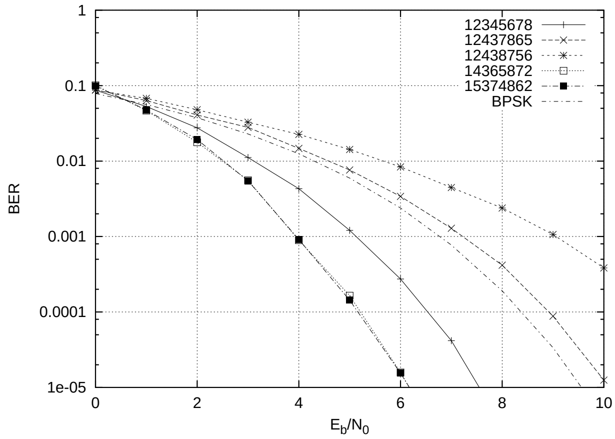

Fig. 5. BER performance of PCPH ($N = 8$).

influence of the constellation labeling on the BER performance in order to find the optimal symbol labeling.

3.1. Optimal Labeling

We define a symbol labeling by a permutation $p_1 p_2 \dots p_N$, meaning that for the pseudo-chaotic iterate x_k we transmit the symbol s_{p_k}. Given N symbols there are clearly $N!$ possible permutations. As the symbols are positioned on the unit circle it follows that some of the permutations are equivalent. For example, the identity permutation 12345678 is equivalent to 34567812 (shift of two positions). Thus, it suffices to consider only permutations with 1 on the first position. Also, because of the symmetry of the circle with respect to the axis it is possible to further reduce the number of permutations which need to be analyzed. Actually, it can be shown that there are $P' = (\frac{N}{2} - 1)(N - 3)!(N - 1)$ classes of non-equivalent permutations. A few examples are given in Table 1. Note that different permutations correspond to different chaotic

Table 1. Number of possible permutations, P, and of non-equivalent permutations, P', as a function of $N(= 2^M)$.

M bits	$N(= 2^M)$	$P(= N!)$	P'
1	2	2	1
2	4	16	3
3	8	40320	2520
4	16	2.092×10^{13}	6.538×10^{11}

maps, characterized by different BER performances. For instance, the "Gray/binary" permutation applied to the Bernoulli shift produces the tent map [8]. The case $N = 2$ ($M = 1$ bit) is trivial as there are only two possible labelings (12 and 21) which are completely equivalent.

The case $N = 4$ ($M = 2$ bits) is the first non-trivial one and it admits three non-equivalent permutations: 1234, 1243 and 1324. The BER curves for these three permutations are shown in Fig. 4 from which it follows that the identity permutation 1234 and the 1324 permutation are optimal. In order to understand why certain permutations result in a better BER performance, we computed the distance between sequences with a single error. If two sequences differ only in one position, then they correspond to the sequence of states differing at two (for $M = 2$) subsequent positions (as the different bit is present in M states only). Hence, for $M = 2$ it is sufficient to consider four pairs of sequences of length three: $0x0$, $1x0$, $0x1$, $1x1$, where x is either 0 or 1. For each pair we can compute the distance between the corresponding sequence of states. For example, for $M = 2$ and for a pair of sequences 001 and 011 we have:

$$d = (u_1 - w_1)^2 + (v_1 - z_1)^2 + (u_2 - w_2)^2 + (v_2 - z_2)^2,$$

where (u_1, v_1) is the state after 00, (u_2, v_2) is the state after 01 (for the sequence 001), (w_1, z_1) is the state after 01, and (w_2, z_2) is the state after 11 (for the sequence 011). Since after the sequence 00 the system is in the state 1, it follows that $(u_1, v_1) = (\cos 2\pi x_{p_1}, \sin 2\pi x_{p_1})$. For a given permutation we compute the minimum distance $d_{\min}$ over all pairs of sequences and also the sum Σ of these distances. The results are reported in Table 2. Clearly the minimum distance $d_{\min}$ should be as large as possible in order to minimize the BER. One can see very strong correlation between $d_{\min}$ (or Σ) and the BER performance. It is interesting to note that for all permutations the distance between two sequences different only by one element does not depend on the choice of sequences.

For the case $N = 8$ ($M = 3$ bits) there are 16 pairs of sequences with single error: $00x00$, $10x00$, $01x00$, $11x00$, $00x10$, $10x10$, $01x10$, $11x10$, $00x01$, $10x01$, $01x01$, $11x01$, $00x11$, $10x11$, $01x11$, $11x11$. For all the 2520 non-equivalent permutations we computed the distance between sequences of states cor-

Table 2. Characterization of the non-equivalent permutations in terms of BER and minimum distance ($N = 4$).

Permutation	BER for $E_b/N_0 = 5$dB	$d_{\min}$	Σ
1234	0.0014	6	24
1243	0.0059	4	16
1324	0.0014	6	24

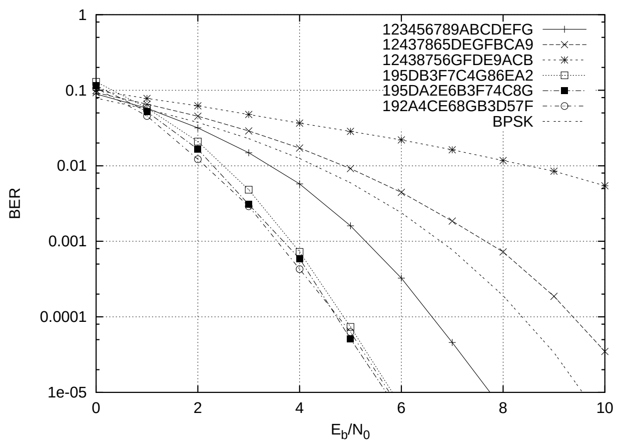

Fig. 6. BER performance of PCPH ($N = 16$).

responding to these pairs. The minimum distance 9.41 is realized, among the others, by the permutation 13465782. The latter permutation, though, is outperformed in terms of BER by others. This indicates that the single-error analysis alone is not sufficient to predict correctly the BER performance of a given permutation. Indeed, for the permutation 13465782 the distance between some sequences differing at two subsequent positions is 7.17. In other words, for this permutation two subsequent bits received with errors are more likely than an isolated error. In order to study the probability of multi-error events we have to consider sequences with more than one different bit. In the light of the observations above we propose to use the following criterion, valid under the hypothesis that there exists dominant error events. Let us consider all sequences that can differ at p subsequent positions (*i.e.* the number of different bits can be from 1 to p). For each pair of these sequences we compute the distance of the corresponding symbol sequences. Then, we choose the permutation with largest minimum distance over all such pairs. By applying this criterion in the case $N = 8$, up to $p = 6$, we found that the maximum $d_{\min}$ is achieved for four permutations, namely: 14365872, 14725836, 15374862, 15376284. In Fig. 5 we show the BER curves corresponding to two of these permutations (the performance of optimal permutations coincides) and some other permutations, including the identity permutation, the "Gray/binary" (12438756) and the "binary/Gray" (12437865). Incidentally, the "Gray/binary" permutation is one of the 429 permutations with the smallest minimum distance ($d_{\min} = 1.76$). From Fig. 5 one can verify that the BER curves for the optimal permutations actually exhibit the best performance. Indeed they are more than 1 dB better than the identity permutation at BER=10^{-3} and 5 dB better than the "Gray/binary". In practice, it is sufficient to consider only relatively small values of p. In fact, it is clear that for larger p the $d_{\min}$ will not increase. For example, in the case under consideration ($N = 8$) it is enough to consider $p = 2$ in order to correctly identify the optimal labeling. Pairs of sequences with larger number of different bits lead to distance larger than $d_{\min}$ for $p = 2$.

For $N = 16$ it is not feasible to consider all permutations, even if we restrict ourselves to the non-equivalent ones. Instead, to find the optimal labeling we use an heuristic argument based on the observation that for $N = 4, 8$, one of the optimal permutations is such that: $|p_{2k+1} - p_{2k}| = N/2$, for all k. For this class of permutations the least significant bit (LSB) plays a dominant role in the transmitted signal immediately after entering the shift register. On the other hand, for the identity permutation, the significance of the bit increases with time and its major contribution occurs just before being discarded. The maximum $d_{\min} = 12.1$ (for $p = 4$) within this class is achieved by the permutation 195DB3F7C4G86EA2. In Fig. 6 we show the BER curves for a few selected labelings. Note that, as predicted, the permutation 195DB3F7C4G86EA2 exhibits an excellent BER performance. However, other permutations like 192A4CE68GB3D57F turn out to be slightly better. This can be explained by the fact that in this case the assumption about the existence of a dominant error event is not exactly valid. A more comprehensive analysis should take into account other relevant factors such as the number of error events realizing d_{min} (it should be as small as possible), and the distance/number of corresponding events close to d_{min}. Finally, as for $N = 8$, the "Gray/binary" permutation 12438756GFDE9ACB, corresponding to the tent map, exhibits the worst performance ($d_{\min} = 0.609$).

4. CONCLUSIONS

In this work we have presented the PCPH (Pseudo-Chaotic Phase Hopping) communication scheme. This scheme exhibits an excellent BER performance, compared to other chaos-based communication systems. Also, we discussed the optimal constellation labeling (hence the optimal map) that minimizes the error probability.

We have proposed and tested a simple criterion for choosing a particular symbol permutation that minimizes the probability of error, without the need for computing the BER curves. The criterion is based on computation of distances between sequences corresponding to single and multi-error events.

5. REFERENCES

[1] S. Hayes, C. Grebogi and E. Ott, "Communicating with chaos," *Phys. Rev. Lett.*, vol. 70, no. 20, pp. 3031–34, May 1993.

[2] J. Schweizer and M. P. Kennedy, "Predictive Poincaré control: A control theory for chaotic systems," *Phys. Rev. E*, vol. 52, no. 5, pp. 4865–76, November 1995.

[3] G.M. Maggio and L. Reggiani, "Applications of symbolic dynamics to UWB impulse radio," In *Proc. ISCAS 2001*, Sydney, Australia, May 6-9 2001.

[4] G.M. Maggio and Z.Galias, " Enhanced DCSK Using Symbolic Dynamics," In *Proc. GLOBECOM'01*, San Antonio, Texas, vol. 2, pp. 1157–1161, November 25-29 2001.

[5] B. Hao and W. Zheng, *Applied Symbolic Dynamics and Chaos*, World Scientific, Singapore, 1998.

[6] R. Shaw, "Strange attractors, chaotic behavior and information flow," *Z. Naturforschung A*, vol. 36A, no. 1, 1981.

[7] G.M. Maggio, N. Rulkov and L. Reggiani, "Pseudo-chaotic time hopping for UWB impulse radio," *IEEE Trans. CAS-I*, vol. 48, no. 12, pp. 1424-35, December 2001.

[8] E. Ott, *Chaos in Dynamical Systems*, Cambridge University Press, Cambridge (U.K.), 1993.

[9] J.G. Proakis. *Digital communications*. 3rd ed., McGraw-Hill, New York, 1995.

[10] D. Lind and B. Marcus, *An introduction to symbolic dynamics and coding*, Cambridge University Press, 1995.