IJCSC International Journal of Computer Science & Communication Vol. 1, No. 2, July-December 2010, pp. 369-372

Pseudo Random Binary Sequences Analysis for the Modeling of Optical DPSK Transmission Systems

Hadjia Badaoui[1], Yann Frignac[2] & Mohammed Feham[1]

[1]Laboratoire STIC, Département de Génie électrique, Faculté de Technologie, Université Abou-Bekr Belkaid, BP 230, Pôle Chetouane - 13000 Tlemcen - Algeria
[2]Institut Telecom & Management SudParis, France
Email: elnbh@yahoo.fr

ABSTRACT

This paper refers to the generation and analysis of data sequences called pseudo-random binary sequences witch show very interesting properties. To emulate a real traffic data transmission using DPSK modulation format with four levels of phase, we are moving towards pseudo-random binary sequence. In particular, we will focus on the autocorrelation function analysis and statistical properties. A PRBS Analysis for a length of 1023 bits has been made to confirm its properties. The simulations results are then presented and discussed.

Keywords: PRBS, PRQS, LSFR Register, Irreducible Primitive Polynomial, Galois Field, Autocorrelation Function, State Changes Sequence

1. INTRODUCTION

The pseudo-random sequences are of great importance for a variety of applications. They are easily produced by recursive procedures and are known by several names. These sequences are used in several fields such as DSSS (Direct Sequence Spread Spectrum), decryption and encryption cryptography, scrambling techniques (scrambling), error detection and many other applications [1-5]. To estimate the performance of an optical transmission system, we have to test it experimentally or through numerical simulations for the principle of the latter lies in the numerical solution of nonlinear equation that describes the Schrödinger propagation of a light wave. But this equation is not solvable analytically, except for special cases (eg solitons). The basic pattern of an optical signal transmitted in fiber is called a symbol. At the beginning of transmission, the data sent by transmitter to receiver do no damage. During propagation, due to the interaction of different effects (chromatic dispersion, nonlinearities, noise, etc.) some transmitted symbols are more degraded than others. So as not to overestimate or underestimate the performance of the sequence data that is supposed to test the performance of the system should contain as many cases eventually degraded by the transmission case that not much affected. The sequences of the most realistic (or rather the ideal case) are random sequences of infinite length. Simulating an optical transmission with such a sequence then requires a very long time to load and large memory space, which can easily exceed the power of the machine. So the best solution is the use of said sequences or pseudo-random binary sequences (PRBS). These sequences are deterministic sequences that contain all possible arrangements of m symbols (except one). Another interesting property of such sequences is that their autocorrelation function resembles the autocorrelation function of white process [6]. For these reasons we call them pseudo-random (PRS). The choice of the length of the sequence used can have an impact on the results of the simulation. Indeed, if the accumulated dispersion in the system is high and the sequence is too short a pulse from a time-temporally widens a bit longer than the length of the sequence, which involves disruption of simulation results (Note that this is just an amplitude modulation format, such NRZ). So the length of sequences used for the simulations is a very important parameter.

2. PSEUDO-RANDOM BINARY SEQUENCES GENERATION

The theory of pseudo-random generation based on the Galois field properties. They have an odd length, equal to $2^m - 1$ bits. The pseudo random binary sequences can be constructed using a linear shift feedback register (LFSR) by one or more exclusive-or gates. The shift register is composed of m cells, in general, each capable of holding a bit. At each clock pulse, the bits are shifted by a section on the right. Bit driven from the main section to the right is the output of the register. As bits are shifted to the right, it is necessary to provide a new registry value to the last cell on the left. This value is provided by a feedback function that calculates the new bit depending on the input of exclusive-or gates. The coefficients $\{ai\} \in$

{0, 1} with $i = 0 : 2^m - 2$. The bits are shifted through the register to the right with each clock pulse. The recurrence relation is given by equation (1):

$$a_{i+4} = a_{i+1} \oplus a_i \qquad (1)$$

Where the summation corresponds to a modulo-2 summation, moreover, equivalent to a gate "XOR". It has two inputs and one output. For the output is at logic "1", it requires a minimum of only one of two inputs is equal to "1".

The connections of the shift register are based on a primitive irreducible polynomial of m order (Galois polynomial) we can choose from a number of primitive polynomials of the same order. They are in the form:

$$h(x) = \sum_{i=0}^{m} h_i x^i \qquad (2)$$

Where :

$$\begin{cases} h_0 = h_m = 1 \\ h_j \in \{0,1\}, \quad 0 < j < m \end{cases} \qquad (3)$$

The connections of the shift register correspond to the primitive polynomials coefficients, in fact there is always the first and the last link since $h_0 = h_m = 1$.

Fig. 1 shows a diagram of an LSFR register own a primitive polynomial $h(x)$.

If $hj = 1$, the feedback connection between two neighbouring cells a_{i+j} and a_{i+j-1} exist. In contrary if $hj = 0$, it does not.

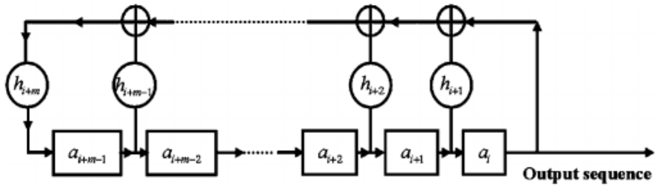

Fig.1: LSFR Schematic Register for a Primitive Polynomial

3. PRBS SEQUENCE PROPERTIES

We distinguish some interesting properties of PRBS sequences witch we will describe in the following subsections.

3.1. Autocorrelation Function

The autocorrelation function of a pseudo-random binary sequence $a_0 a_1 \ldots\ldots a_{L-1}$ of length L is given by [7]:

$$\begin{cases} \rho(0) = 1 \\ \rho(i) = -\dfrac{1}{L} \quad 1 \le i \le 2^m - 2 \end{cases} \qquad (4)$$

Fig. 2 illustrates the principle of the autocorrelation function of a pseudo-random binary sequence.

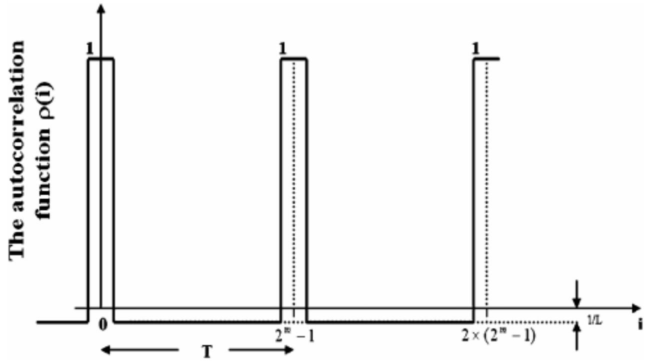

Fig.2: The Autocorrelation Function of a Pseudo-random Binary Sequence

The autocorrelation function is periodic. That is to say:

$$\rho(i) = \rho(i + L) \qquad (5)$$

The PRBS sequence is unusual, when correlated to guarantee only one maximum correlation at the origin. Indeed, it is a random sequence of bits of finite length so that two successive bits will be virtually uncorrelated, The autocorrelation function of a real sequence (or complex) $a_0, a_1, a_2, .., a_{L-1}$ is defined as:

$$\rho(i) = \frac{1}{L} \sum_{j=0}^{L-1} (-1)^{a_j + a_{j+i}} \qquad (6)$$

With: $i = 0, \pm 1, \pm 2, \ldots$

A correlation function involving a physical level -1 or 1 to a binary sequence (as $(-1)^{a_0}$,$(-1)^{a_1}$,...,$(-1)^{a_{L-1}}$ is given by:

$$\rho(i) = \frac{1}{L} \sum_{j=0}^{L-1} (-1)^{a_j + a_{j+i}} \qquad (7)$$

With: $i = 0 : 2^m - 2$,

L is the length of the sequence and $a_{i+L} = a_i$

Equation (7) is obtained by replacing all the bits "1" to a value of "–1" and bit "0" with value "1".

3. 2. Periodicity

PRBS sequences generated, are periodic sequences of period $2^m - 1$ bits. The PRBS sequence length L is defined as follows:

$$L = 2^m - 1 \qquad (8)$$

Indeed, as their length is odd, there is necessarily an imbalance between the number of "1" and the number of "0". The equal probability of "1" and "0" in a PRBS is not perfectly satisfied.

The number of "1" is equal to: 2^{m-1} and the number of "0" is equal to: $2^{m-1} - 1$.

4. BINARY PSEUDO-RANDOM SEQUENCES ANALYSIS RESULTS

To characterize any sequence relative to its ability to possess the pseudo-random properties, we will be interested in testing the autocorrelation function of binary sequences commonly used for numerical simulations and the state changes sequence for a number of m cells constituting the LSFR register equal to 10. In our case we use a primitive polynomial $h(x) = x^{10} + x^3 + 1$. In addition, we will conduct a statistical analysis of a PRBS sequence and the state changes sequence. In the figures 3 (a), (b) and (c) we represent respectively the spectrum, the autocorrelation function of a PRBS sequence, the spectrum of the state changes sequence and its autocorrelation function for $m = 10$.

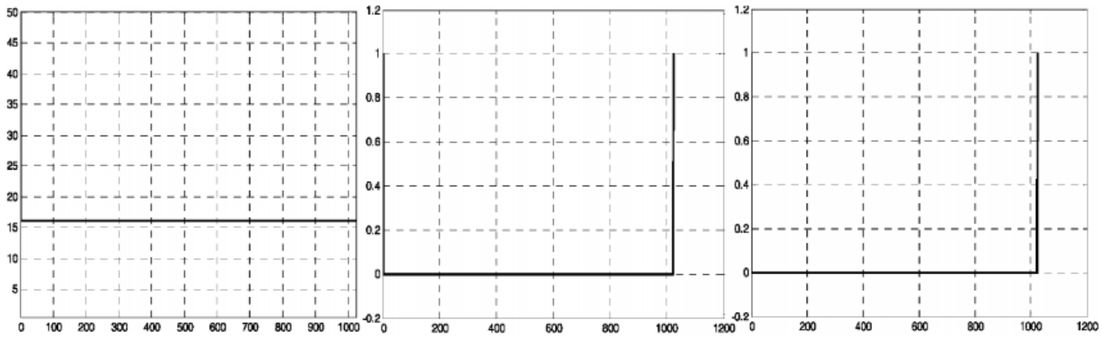

Fig.3: (a) The Spectrum of a PRBS Sequence of 1023 Bits, (b) The Autocorrelation Function of PRBS Sequence of 1023 Bits; (c) The Autocorrelation Function of the State Changes Sequence of 1023 Symbols

Notice that the state changes sequence is obtained by multiplexing between a bit and the precedent bit to get a symbol. What Follows, we say that the state changes sequence is a quaternary sequence can take values 0, 1, 2 or 3. For example, a bit sequence "0101110" has its sequence of state changes "1213320". The autocorrelation function of a PRBS sequence is treated as a Dirac peak at the origin of amplitude equal to 1, this reflects the fact that, when correlated to guarantee only one maximum of correlation. On the other hand, if we shift the sequence of one bit the autocorrelation function is always zero, that is to say, the PRBS sequence is uncorrelated beyond the origin confirming that the bits are completely independent.

Similarly, and from Fig. 3 (b), we note that the autocorrelation function of the state changes sequence is similar to the PRBS, but it is not a quaternary pseudo-random sequence. The property of transitions of the PRBS sequence need to make it a PRQS is that it does not contain all possible sequences of m symbols.

In the case of a PRBS sequence, we have four cases of correlation and the probability of two bits is identical to the related probability of being different. Indeed, during the computation of the correlation function if the two bits are adding a "1" to the correlation function and are removed if they are different "1". In contrary, in the case of a PRQS sequence was 16 cases of correlation and the possibility of having two similar symbols is less likely than to have two different symbols. The correlation function quantifies the level of similarity between the symbols. If both symbols are equal we add a "1" and if we remove a different "1/3 ". According to the statistics of a PRBS, we note that the number of "1" is greater than the number of "0". Indeed, since the length of the sequence is large enough, the probability of having "0" is almost equal to that of "1". This is similar to the state changes sequence which contains a number of zeros less than the other symbols namely '1 ', '2', '3 '. This is illustrated in the Table 2.

Table 2
A PRBS Sequence of 4095 Bits Statistical Analysis

States	0	1	0	1	2	3
Number	2047	2048	1023	1024	1024	1024
Probability	0.4998	0.5001	0.2498	0.2500	0.2500	0.2500

The length of the binary sequence to simulate is a very important parameter. Studies shown very long sequences, until 2^{15} bit or more up are needed for the simulation results of a 40 Gbit/s are Significant [8].

5. CONCLUSION

To emulate a real traffic data transmission using DPSK modulation format with two levels of phase, we are moving towards pseudo-random binary sequence, PRBS Analysis for a length of 1023 bits have been made to confirm its properties such as the states counting and its autocorrelation function.

REFERENCES

[1] D. van den Borne, E. Gottwald, G.D. Khoe & H. de Waardt, "*Bit Pattern Dependence in Optical DQPSK*", *IEEE*, **43**, N°. 22, Oct. 2007.

[2] Y. Frignac, "Contribution à l'Ingénierie des Systèmes de Transmission Terrestres sur Fibre Optique Utilisant le Multiplexage en Longueur d'onde de Canaux Modulés au Débit de 40 Gbits/s", Thèse de Doctorat, Ecole Nationale Supérieure des Télécommunications, Avril. 2003.

[3] Ramamtanis Petros, Badaoui Hadjira, Frignac Yann, "Quaternary Sequences Comparison for the Modeling of Optical DQPSK Dispersion Managed Transmission Systems, OFC '09 : Optical Fiber Communication Conference", *IEEE*, 22-26 March 2009, San Diego, Ca, United States, 2009, ISBN 978-1-4244-2606-5.

[4] D. Van den Born, E. Gottwald, G. D. Khoe and H. de. Waardt, "Pseudo Random Sequences for Modelling of Quatrenary Modulation Formats", *12 th Optoelectronics and Communications Conference*, Technical Digest, July 2007, Pacifico Yokohama. Pp. 722-723.

[5] A. Afaq, "Development of State Model Theory for External Exclusive NOR Type LSFR Structures", *Proceedings of World Academy of Science, Engineerings and Technology*, **10**, Dec. 2005.

[6] John Proakis, "Digital Communications", 4th Edition.

[7] Ramantanis Petros, Badaoui Hadjira, Frignac Yann, "Comparaison des Séquences de Données Pour l'estimation de la Perfomance des Systèmes de Transmission Optique DQPSK", *28ièmes Journées Nationales d'Optique Guidée & Horizons de l'Optique*, 06-09 Juillet 2009, Lille, France, 2009.