

NON-RELATIVELY MEASURABLE SPREAD-SEQUENCES FOR SECURE TRANSMISSION OF DIRECT-SEQUENCE SPREAD-SPECTRUM SIGNALS

Jacek Leśkow ^(a), Antonio Napolitano ^(b)

^(a) Zakład Ekonometrii, Wyższa Szkoła Biznesu WSB-NLU
Nowy Sącz, Poland, leskow@wsb-nlu.edu.pl

^(b) Università di Napoli "Parthenope", Dipartimento per le Tecnologie
via Acton 38, I-80133 Napoli, Italy, antonio.napolitano@uniparthenope.it

ABSTRACT

In this paper, a new technique to design signals for secure transmissions is proposed. The proposed technique does not allow to an unauthorized third party to discover the modulation format and, hence, to demodulate the signal. The proposed signal-design technique consists in adopting a non relatively measurable sequence as spreading sequence for a direct-sequence spread-spectrum signal. Non relatively measurable sequences are such that the appropriate time averages do not converge as the data-record length approaches infinite. Thus, none of their statistical functions defined in terms of infinite-time averages is convergent. Therefore, also the modulated continuous-time signal exhibits non convergent statistical functions. Consequently, all modulation classification methods based on measurements of statistical functions such as the autocorrelation function, moments, and cumulants fail to identify the characteristics of the modulation format. Simulation results are provided to show the lack of convergence, as the data record is increased, of the estimators of the second-order cyclic statistics of the designed signal.

1. INTRODUCTION

Automatic classification of the modulation format of communications signals is a relevant problem in military and commercial communications systems. It consists in automatically determining the modulation type of the signal present in the data record. In the context of the signal interception, modulation classification can be seen as the intermediate step between detection and demodulation. In particular, in non-cooperative signal reception, the modulation format of the received signal needs to be determined before proceeding to the demodulation and possible decryption of the data.

Several techniques for automatic modulation classification have been developed in the last two decades. They are based on measurements of statistical functions of the received signal. For example, the algorithms proposed in [2], [12], [14] are based on second- and higher-order moments and cumulants. The modulation-classification algorithms in [3], [4], [5], [7], [8], [11], and [13] exploit second- and higher-order cyclostationarity properties of signals.

In the present paper, a new signal-design technique is proposed, which does not allow to discover the modulation format on the basis of measurements of statistical functions. Thus, the proposed technique is suitable to be exploited in the design of secure transmission systems where the goal is to avoid the signal demodulation by an unauthorized third party. This is obtained by generating a signal whose time-averaged statistical functions such as the autocorrelation function, moments, and cumulants are not convergent as the data-record is increased. Consequently, estimates of these functions, as well as estimates of spectral functions such as the power spectrum and moment and cumulant spectra, exhibit a significant variability as the data-record length changes (e.g., increases).

The proposed signal-design technique exploits the concept of relative measure of functions and sequences. Such a concept is central in the functional (or, equivalently, nonstochastic or fraction-of-

time) approach for signal or time-series analysis [6], [9], [10]. In this approach, the fraction-of-time distribution function (or, equivalently, empirical distribution function) of a signal or time series $x(t)$ is defined as the infinite-time average of the indicator of the set $\{t \in \mathbb{R} : x(t) \leq \xi\}$. If such a time average exists for almost all values of $\xi \in \mathbb{R}$, then $x(t)$ is said relatively measurable (RM). Starting from this distribution function, all familiar statistical functions and parameters, such as moments and cumulants, can be defined. If the observed time series at hand is interpreted as a sample-path or realization of a stochastic process satisfying appropriate ergodicity properties, then the above mentioned statistical functions, defined in terms of time averages, are equal to their stochastic counterparts defined in terms of ensemble averages. For signals belonging to the class of the non relatively-measurable functions, the fraction-of-time distribution function does not exist. That is, the above mentioned infinite-time average does not exist for almost all values of ξ . Thus, also the other statistical functions do not exist, in the sense that the infinite-time averages in their definitions are not convergent. Therefore, the modulation type of signals that are not RM functions cannot be determined by measurements of time-average based statistical functions. Consequently, the modulation format of these signals cannot be determined by an unauthorized third party and, hence, they are suitable to be exploited for the design of secure transmission systems.

In the paper, the concept of relative measurability for functions of a continuous variable [9], [10] is extended to sequences. Then, a non RM sequence, instead of a pseudo-noise (PN) sequence, is used as spreading sequence for a direct-sequence spread-spectrum (DSSS) signal. Consequently, the resulting signal turns out to be a non RM signal. Since digitally modulated signals are almost-cyclostationary [6], a complete second-order cyclostationary analysis is carried out for the designed signal by estimating its cyclic autocorrelation function, as a function of the cycle frequency and the lag parameter, when these two parameters vary in a wide range of values. Moreover, for comparison purpose, the same analysis is carried out for a conventional DSSS signal using a PN spreading sequence. Simulation results show the effectiveness of the proposed signal-design technique. In fact, unlike for the conventional DSSS signal, the estimator of the cyclic autocorrelation function of the designed non RM signal does not converge as the data-record length increases. Finally, the problem of signal reception and synchronization for the authorized party is briefly discussed.

2. RELATIVE MEASURABILITY OF SETS AND SEQUENCES

Let A be a set of integer numbers. According to the definitions given in [9], [10] for sets of real numbers, the *relative measure* of A is defined as

$$\mu_R(A) \triangleq \lim_{N \rightarrow \infty} \frac{1}{2N+1} \sum_{n=-N}^N \mathbf{1}_{\{n \in A\}} \quad (1)$$

provided that the limit exists. In (1), $\mathbf{1}_{\{n \in A\}}$ is the indicator of the set A , that is, $\mathbf{1}_{\{n \in A\}} = 1$ for $n \in A$ and $\mathbf{1}_{\{n \in A\}} = 0$ for $n \notin A$. Thus, the sum in (1) represents the number of elements in the set of integers $\{-N, \dots, N\}$ belonging to A . If the limit in (1) exists, then the set A is said relatively measurable.

From definition (1) it follows that $\mu_R(A)$ represents the proportion of integer numbers that belong to the set A . Thus, finite sets have zero relative measure, and only infinite sets can have non-zero relative measure. By following the guidelines given in [10] for the sets of real numbers, it can be shown that: the class of RM sets of integers is not closed under union and intersection; the relative measure μ_R is additive, but is not σ -additive; and if A is a RM set, then $\bar{A} \triangleq \mathbb{Z} - A$ is RM.

Let $\{x_n\}_{n \in \mathbb{Z}}$ be a sequence of real numbers, and define

$$\begin{aligned} F_x(\xi) &\triangleq \mu_R(\{n \in \mathbb{Z} : x_n \leq \xi\}) \\ &= \lim_{N \rightarrow \infty} \frac{1}{2N+1} \sum_{n=-N}^N \mathbf{1}_{\{x_n \leq \xi\}} \end{aligned} \quad (2)$$

where $\mathbf{1}_{\{x_n \leq \xi\}}$ is the indicator of the set $\{n \in \mathbb{Z} : x_n \leq \xi\}$. If the limit in (2) exists $\forall \xi \in \mathbb{R} - \Xi_0$, where Ξ_0 is an at most countable set, then the sequence x_n is said to be *relatively measurable*. The function $F_x(\xi)$ defined in (2) has values in $[0, 1]$ and is non decreasing. Thus, it has all the properties of a distribution function, except the right-continuity in the discontinuity points. Furthermore, as for every bounded nondecreasing function, the set of discontinuity points is at most countable.

The function $F_x(\xi)$ allows to define all the familiar probabilistic parameters. Furthermore, if x_n is a RM, not necessarily bounded sequence, and if $g(\cdot)$ is a continuous bounded function of bounded variation such that for any $\ell \in \mathbb{R}$ the equation $g(\xi) = \ell$ admits at most a finite number of solutions in any finite interval, then the following *fundamental theorem of expectation* can be proved:

$$\lim_{N \rightarrow \infty} \frac{1}{2N+1} \sum_{n=-N}^N g(x_n) = \int_{\mathbb{R}} g(\xi) dF_x(\xi) \quad (3)$$

where the integral is in the Riemann-Stieltjes sense.

It can be shown that the set of RM sequences is not closed under addition and multiplication. However, the sum and the product of two sequences is RM provided that at least one of them is bounded and the sequences are jointly RM. Two sequences $\{x_n\}_{n \in \mathbb{Z}}$ and $\{y_n\}_{n \in \mathbb{Z}}$ are said to be *jointly RM* if the limit

$$\begin{aligned} F_{xy}(\xi_1, \xi_2; m) &\triangleq \mu_R(\{n \in \mathbb{Z} : x_{n+m} \leq \xi_1\} \cap \{n \in \mathbb{Z} : y_n \leq \xi_2\}) \\ &= \lim_{N \rightarrow \infty} \frac{1}{2N+1} \sum_{n=-N}^N \mathbf{1}_{\{x_{n+m} \leq \xi_1\}} \mathbf{1}_{\{y_n \leq \xi_2\}} \end{aligned} \quad (4)$$

exists for $m = 0$ and for all $(\xi_1, \xi_2) \in \mathbb{R}^2 - \Xi_0$, where Ξ_0 is at most a countable set of lines. The function $F_{xy}(\xi_1, \xi_2; m)$ has all the properties of a bivariate joint distribution function with the exception of the right continuity in the discontinuity points. Furthermore, the following *fundamental theorem of expectation for the bivariate case* holds,

$$\lim_{N \rightarrow \infty} \frac{1}{2N+1} \sum_{n=-N}^N g(x_{n+m}, y_n) = \int_{\mathbb{R}^2} g(\xi_1, \xi_2) dF_{xy}(\xi_1, \xi_2; m) \quad (5)$$

where $\{x_{n+m}\}_{n \in \mathbb{Z}}$ and $\{y_n\}_{n \in \mathbb{Z}}$, for any $m \in \mathbb{Z}$, are two jointly RM, not necessarily bounded, sequences. Moreover, the function $g(\xi_1, \xi_2)$ is continuous, bounded, and of bounded variation, and for any $\ell \in \mathbb{R}$ the equation $g(\xi_1, \xi_2) = \ell$ admits at most a finite number of solutions in any finite rectangular set. It can be shown that two almost-periodic sequences are jointly RM.

The fact that RM sets are not closed under union and intersection and that the relative measure μ_R is additive, but is not σ -additive are properties different from those of the Lebesgue measure. Consequently, the distribution function and the expectation operator based on time averages, that are built from the relative measure μ_R , have properties slightly different from those of the distribution function and the expectation operator of the classical probability theory, which is based on ensemble averages built from the Lebesgue measure on the sample space. In particular, the fact that non RM sets and functions are not difficult to be built (unlike non Lebesgue-measurable sets and functions) will be exploited in Section 3 to design signals whose statistical functions, defined in terms of time averages, are not convergent as the data-record length approaches infinity.

3. SIGNAL DESIGN

In this section, a non RM signal is constructed by adopting a non RM sequence as spreading sequence for a DSSS signal.

Let us consider the signal

$$x(t) = \sum_{n=-\infty}^{+\infty} s_{\lfloor n/N_c \rfloor} c_n g(t - nT_c) \cos(2\pi f_0 t + \phi_0). \quad (6)$$

In (6), $\{s_n\}_{n \in \mathbb{Z}}$ is an information sequence of binary independent and identically distributed (i.i.d.) symbols, $\{c_n\}_{n \in \mathbb{Z}}$ is a binary spreading or coding sequence independent of $\{s_n\}_{n \in \mathbb{Z}}$, $\lfloor \cdot \rfloor$ denotes integer part, N_c is the number of chip per bit, T_c is the chip period, and $g(t)$ is a Nyquist-shaped chip pulse with excess-bandwidth factor η . If $\{c_n\}_{n \in \mathbb{Z}}$ is a maximal-length PN binary sequence, then the signal $x(t)$ models a long-code DSSS signal used in code-division multiple-access (CDMA) systems [6].

In the following, a non RM sequence is constructed. The adoption of such a non RM sequence as spreading sequence for the signal $x(t)$ defined in (6) makes $x(t)$ non RM and, hence, with statistical functions defined in terms of time averages that are not convergent.

Let A be the set

$$A \triangleq \bigcup_{k \in \mathbb{N}} \{n \in \mathbb{Z} : a_{2k} \leq |n| < a_{2k+1}\}, \quad (7)$$

where $\{a_k\}_{k \in \mathbb{N}}$ is the sequence

$$a_0 = 0, \quad a_k = a_{k-1} + b^k, \quad k \in \mathbb{N}, \quad b > 1. \quad (8)$$

Since a_k grows exponentially with k , it can be easily seen that the sequence

$$m^{(N)}(A) \triangleq \frac{1}{2N+1} \sum_{n=-N}^N \mathbf{1}_{\{n \in A\}} \quad (9)$$

oscillates in $[0, 1]$ as $N \rightarrow \infty$. Therefore, for the set A , the limit (1) does not exist, that is, A is not RM.

A non RM (band-pass) DSSS-like signal can be obtained by considering a spreading sequence c_n in (6) such that, for $n \in A$ and $n \in \bar{A} \triangleq \mathbb{Z} - A$, two different spreading subsequences with different statistical properties are adopted. Specifically, let the spreading or coding sequence c_n be defined as

$$c_n \triangleq q_A(n) \mathbf{1}_{\{n \in A\}} + \tilde{q}_A(n) \mathbf{1}_{\{n \in \bar{A}\}}. \quad (10)$$

In (10), $q_A(n)$ is the pseudo-random sequence [1]

$$q_A(n) \triangleq \cos(\pi \lfloor P_A(\lfloor n/N_c \rfloor) \rfloor) \quad (11)$$

where

$$P_A(n) \triangleq p_2 n^2 + p_1 n + p_0 \quad (12)$$

with incommensurate coefficients p_1 and p_2 , and $\tilde{q}_{\bar{A}}(n)$ is the N_c -periodic sequence

$$\tilde{q}_{\bar{A}}(n) \triangleq \sum_{k=-\infty}^{+\infty} q_{\bar{A}}(n - kN_c) \quad (13)$$

with

$$q_{\bar{A}}(n) \triangleq \sum_{k \in I_1} \delta_{n-k} - \sum_{k \in I_2} \delta_{n-k}. \quad (14)$$

In (14), the sets I_1 and I_2 constitutes a partition of $\{0, 1, \dots, N_c - 1\}$, that is, $I_1 \cap I_2 = \emptyset$ and $I_1 \cup I_2 = \{0, 1, \dots, N_c - 1\}$, and δ_n is the Kronecker delta ($\delta_n = 1$ for $n = 0$ and $\delta_n = 0$ for $n \neq 0$).

Due to the different patterns $q_A(n)$ and $\tilde{q}_{\bar{A}}(n)$, and the lack of relative measurability of A (and, hence, of \bar{A}), the sequence c_n is not RM. In fact, let $\mathcal{S}_N \triangleq \{-N, \dots, N\}$, we have

$$\{n \in \mathcal{S}_N : c_n \leq \xi\} = \{n \in \mathcal{S}_N \cap A : q_A(n) \leq \xi\} \cup \{n \in \mathcal{S}_N \cap \bar{A} : \tilde{q}_{\bar{A}}(n) \leq \xi\}. \quad (15)$$

Consequently, since the sequence $m^{(N)}(A)$ defined in (9) oscillates in $[0, 1]$, the finite-time distribution function

$$F_c^{(N)}(\xi) \triangleq \frac{1}{2N+1} \sum_{n=-N}^N \mathbf{1}_{\{c_n \leq \xi\}} \quad (16)$$

as $N \rightarrow \infty$, approaches alternatively the distribution function of $q_A(n)$ and that of $\tilde{q}_{\bar{A}}(n)$ (which can be shown to be both RM), that is, it is not convergent. Analogously, it can be shown that the lag-product sequence $c_{n+m} c_n$ is not RM in n . Moreover, for any RM sequence v_n with lag product $v_{n+m} v_n$ RM in n , the two sequences $c_{n+m} c_n$ and $v_{n+m} v_n$ are not jointly RM in n , the sequence $d_n \triangleq v_n c_n$ has the lag product which is not RM, and the continuous-time signal $z(t) \triangleq \sum_{n \in \mathbb{Z}} d_n g(t - nT_c)$ exhibits a lag product $z(t + \tau)z(t)$ non RM in t . Thus, the signal $x(t)$ defined in (6) with spreading sequence c_n given by (10)–(14) has non RM lag product $x(t + \tau)x(t)$ and, consequently, non convergent autocorrelation function.

Note that the sequence c_n is not obtained by periodically switching between two RM subsequences. The periodic switching, in fact, produces a cyclostationary sequence, that is, with statistical properties significantly different from those of the designed non RM sequence.

Finally, observe that, for the signal $x(t)$ defined in (6) with spreading sequence c_n given by (10)–(14), reception is made exactly as for long-code DSSS signals used in CDMA systems. Specifically, after the carrier demodulation, in the case of perfect chip synchronization, by sampling with sampling frequency $1/T_c$, one obtains the sequence

$$x_k \triangleq \left[\sum_{n=-\infty}^{+\infty} s_{[n/N_c]} c_n g(t - nT_c) \right]_{t=kT_c} = s_{[k/N_c]} c_k. \quad (17)$$

Then, by multiplying the received sequence x_k and the spreading sequence c_k , accounting for the fact that $c_k^2 = 1 \forall k$, and decimating the result by N_c , one gets the information sequence s_k . For the sequence synchronization purpose, as for long-code DSSS signals, the receiver should get via an auxiliary channel the status of the spreading sequence. Thus, in the case of perfect synchronization, the performance of the receiver for the signal $x(t)$ defined in (6) with spreading sequence c_n given by (10)–(14) is the same as that of the receiver for the conventional long-code DSSS signal (where c_n is a PN sequence).

4. NUMERICAL RESULTS

Digitally modulated signals are almost-cyclostationary [6]. The central parameter of their second order wide-sense characterization is the *cyclic autocorrelation function* [6]

$$R_x^\alpha(\tau) \triangleq \lim_{T \rightarrow \infty} R_{x_T}^\alpha(\tau) \quad (18)$$

where

$$R_{x_T}^\alpha(\tau) \triangleq \frac{1}{T} \int_{t_0-T/2}^{t_0+T/2} x(t + \tau)x(t) e^{-j2\pi\alpha t} dt \quad (19)$$

is the *cyclic correlogram*. The magnitude and phase of $R_x^\alpha(\tau)$ represent the amplitude and phase, respectively, of the finite-strength additive sinusoidal component at frequency α contained in the autocorrelation function. Thus, a complete second-order wide-sense characterization of $x(t)$ can be obtained by estimating $R_x^\alpha(\tau)$ as a function of the two variables α and τ . The cyclic correlogram (19) is an estimator of the cyclic autocorrelation function (18). It converges, as $T \rightarrow \infty$, in the temporal mean-square sense to the cyclic autocorrelation function, provided that the signal $x(t)$ fulfills some mild conditions expressed in term of summability of its temporal second- and fourth-order cumulants [6].

Two experiments have been conducted, aimed at showing the different behavior of the cyclic correlogram of the signal $x(t)$ defined in (6) when the spreading sequence is a PN sequence and when it is the non RM sequence defined by (10)–(14).

In both the experiments, time is discretized by an oversampling factor $Q = 8$ so that $T_c = QT_s$, where T_s is the sampling period. A binary information sequence s_n is transmitted. Moreover, $\eta = 0.85$, $N_c = 8$, $f_0 = 0.15/T_s$, and $\phi_0 = 0$. In the experiments, the magnitude of the cyclic correlogram $R_{x_T}^\alpha(\tau)$ as a function of τ/T_s and αT_s is evaluated by a data record length $T = NT_s$, with (a) $N = 2^{11}$, (b) $N = 2^{13}$, and (c) $N = 2^{15}$.

In the first experiment (Fig. 1), the signal $x(t)$ defined in (6) with PN spreading sequence, is considered. Such a signal is a RM band-pass DSSS signal. From Fig. 1, the *convergence* of the estimator as the data-record length is increased is evident.

In the second experiment (Fig. 2), $x(t)$ is the signal defined in (6) with spreading sequence c_n given by (10)–(14) and $b = 10$ in (8). The coefficients of the polynomial $P_A(n)$ (see (12)) are $p_2 = \sqrt{2}$, $p_1 = \sqrt{3}$, $p_0 = 0$, and $I_1 = \{1, 4, 5, 7\}$ and $I_2 = \{0, 2, 3, 6\}$ in $q_{\bar{A}}(n)$ (see (14)). As a consequence of the *non relative measurability* of the lag-product waveform $x(t + \tau)x(t)$, we have that the cyclic autocorrelation $R_x^\alpha(\tau)$ *does not exist* for any $\alpha \in \mathbb{R}$. In particular, the time-averaged autocorrelation function $R_x^0(\tau)$ and the power spectrum do not exist. From Fig. 2, the *lack of convergence* of the estimator as the data-record length is increased is evident. In particular, for a fixed cycle frequency, the shape and strength of the cyclic correlogram are significantly different for different data-record lengths.

This lack of convergence makes the designed signal suitable to be exploited in secure transmission systems where the modulation format should not be discovered by statistical function measurements.

REFERENCES

- [1] J. Bass, *Cours de Mathématiques*. Tome III, Masson & Cie, Paris, 1971.
- [2] B. F. Beidas and C. L. Weber, "Higher-order correlation-based approach to modulation classification of digitally frequency-modulated signals," *IEEE Journal on Selected Areas in Communications*, vol. 13, n. 1, pp. 89-101, January 1995.
- [3] D. Boiteau and C. Le Martret, "A general maximum likelihood framework for modulation classification," in *Proc. of IEEE International Conference of Acoustics, Speech, and Signal Processing (ICASSP 1998)* vol. 4, pp. 2165-2168, 1998.
- [4] O. A. Dobre, Y. Bar-Ness, and W. Su, "Higher-order cyclic cumulants for higher-order modulation classification," in *Proc. of IEEE Military Communications Conference (MILCOM 2003)*, October 13-16, 2003.
- [5] O. A. Dobre, Y. Bar-Ness, and W. Su, "Robust QAM modulation classification algorithm using cyclic cumulants," in

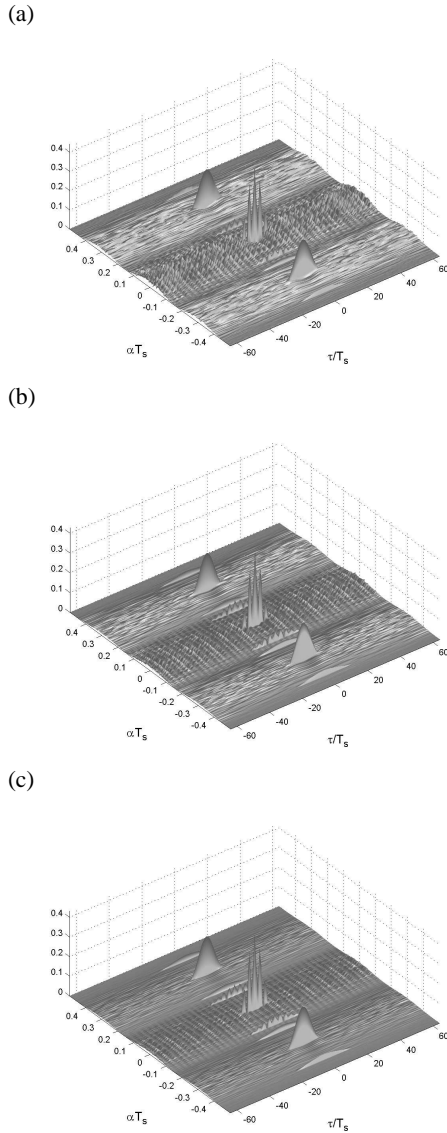


Figure 1: RM band-pass DSSS signal: Magnitude of the cyclic correlogram $R_{X_T}^\alpha(\tau)$, evaluated by a data record length $T = NT_s$; (a) $N = 2^{11}$, (b) $N = 2^{13}$, and (c) $N = 2^{15}$.

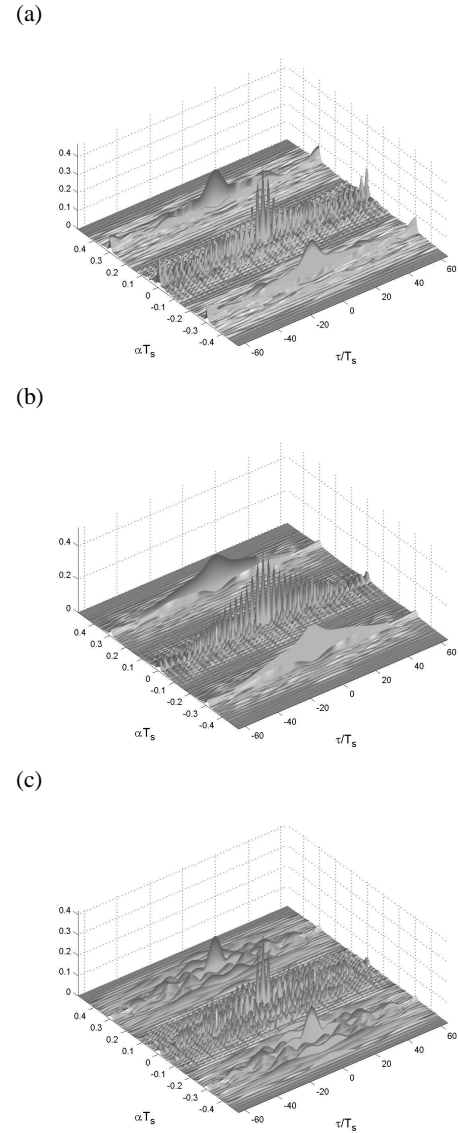


Figure 2: Non RM band-pass DSSS-like signal: Magnitude of the cyclic correlogram $R_{X_T}^\alpha(\tau)$, evaluated by a data record length $T = NT_s$; (a) $N = 2^{11}$, (b) $N = 2^{13}$, and (c) $N = 2^{15}$.

Proc. of *IEEE Wireless Communications and Networking Conference (WCNC 2004)*, March 21-25, 2004.

- [6] W.A. Gardner, *Statistical Spectral Analysis: A Nonprobabilistic Theory*. Prentice Hall, Englewood Cliffs, NJ, 1987.
- [7] P. Gournay and P. Nicolas, "Cyclic spectral analysis and time-frequency analysis for automatic transmission classification," in Proc. of *Quinzieme Colloque GRETSI*, Juan-les-Pins, France, September 13-16, 1995.
- [8] Y. K. Kim and C. L. Weber, "Generalized single cycle classifier with applications to SQPSK v.s. 2^k PSK," in Proc. of *IEEE Military Communications Conference (MILCOM 1989)*, October 15-18, 1989.
- [9] M. Kac and H. Steinhaus, "Sur les fonctions indépendantes IV," *Studia Mathematica*, vol. 7, pp. 1-15, 1938.
- [10] J. Leśkow and A. Napolitano, "Foundations of the functional approach for signal analysis," *Signal Processing*, in press, 2006.
- [11] P. Marchand, J. L. Lacoume, and C. Le Martret, "Multiple hypothesis modulation classification based on cyclic cumulants of different orders," in Proc. of *IEEE International Conference of Acoustics, Speech, and Signal Processing (ICASSP 1998)* vol. 4, pp. 2157-2160, 1998.
- [12] S. S. Soliman and S.-Z. Hsue, "Signal classification using statistical moments," *IEEE Transactions on Communications*, vol. 40, n. 5, pp. 908-916, May 1992.
- [13] C. M. Spooner, "Classification of cochannel communication signals using cyclic cumulants," in Proc. of *Twenty-Ninth Annual Asilomar Conference on Signals, Systems, and Computers*, Pacific Grove, CA, October 29–November 1, 1995.
- [14] A. Swami and B. M. Sadler, "Hierarchical digital modulation classification using cumulants," *IEEE Transactions on Communications*, vol. 48, n. 3, pp. 416-429, March 2000.