ANR, Appel à Projets Générique (AAPG 2019)

QCSP Project (ANR-19-CE25-0013-02)

Deliverable D2.2
Blind Detection Algorithm For QCSP

Editor:	Lab-STICC/UBS
Deliverable nature:	Internal (scope: Consortium and ANR)
Due date:	October 2020
Delivery date:	October 15, 2020
Version:	1.0
Total number of pages:	20 pages
Keywords:	CCSK modulation, Detection, Probability of false alarm and miss detection

Abstract
This deliverable reports on the specifications of achieving Blind synchronization for the Quasi Cyclic Short Packet (QCSP).

List of Authors

Partner	Author
LAB-STICC/UBS	Kassem Saied (kassem.saied@univ-ubs.fr)
LAB-STICC/UBS	Emmanuel Boutillon (Emmanuel.Boutillon@univ-ubs.fr)
External	Ali Al Ghouwayel (ali.ghouwayel@liu.edu.lb)

Contents

Executive Summary

Work Package 2 (WP2) of the QCSP project is concerned with the proposition and evaluation of algorithms to achieve an efficient detection and synchronization of the CCSK-modulated Frame using the soft output provided to the decoder and exploiting the particular structure of the frame. In fact, detection/synchronization performance should be compatible with the decoding performance since the correct transmission of a frame requires 3 conditions: correct detection, correct synchronization and correct error correction. For a given channel, these 3 conditions should have more or less the same probability of failure in order to avoid the weakest condition dominating the error probability, therefore degrading the overall system performance.

The goal of **Task 2.2** is to revolve around the definition and evaluation of detection algorithms for scenarios of IoT systems given by WP4. It will include three aspects: find new detection techniques to improve performance, assess the detection performance through Monte-Carlo simulation and finally, develop a theoretical model of detection performance. About new detection algorithms as a future work, we would like to explore a promising method that uses the fact that CCSK symbols are linked by the NB code.

Figure 1: Gantt diagram of WP2

This deliverable is organized as follows:

Chapter 1 introduces the system and channel model, and it defines the detection problem. It also describes in details the detection algorithm specifications. It describes From one side the time-frequency decomposition protocol, and from other side the detection method it self and the main metric, which called score function.

Chapter 2 gives the theoretical model of the proposed algorithm where the expressions of the correlation functions and Probability Density Functions (PDF) are derived. Then the theoretical model is validated through a comparative study with experimental results obtained with Monte-Carlo simulations over complex AWGN channel, and the effect of different parameters that affect the CCSK-based system is discussed.

1 System Model and Algorithm Specifications

This chapter is divided into two sections. On the first side we go through the system model where we first review shortly the principle of a Cyclic Code Shift Keying (CCSK) modulation in the context of its association with Non-Binary codes. Then we present the effect of the channel at the receiver side when no time and frequency information is available. Finally, we define the detection problem based on signal detection theory. On the other side of this chapter, we discusses in details the score function, which is the detection algorithm used to detect the QCSP frame.

1.1 System Model

1.1.1 Association of CCSK and Non Binary Codes:

Consider a NB code defined over GF(q), $q = 2^p$, with K symbols of information and a total length N. The code rate of the code is thus $R_c = K/N$ and a codeword contains Kp bits of information. The input of the NB-code is a binary message $\boldsymbol{M}$ of size $m = K \times p$ information bits, equivalently K GF(q) symbols. The encoder generates a codeword $\boldsymbol{C}$ of N GF(q) symbols:

$$\boldsymbol{C} = [c_0, c_1, \ldots, c_{N-1}], \text{ with } c_k \in \mathrm{GF}(q),\ k = 0, 1, \ldots, N-1. \tag{1.1}$$

For the goal of direct sequence spread spectrum technique, the CCSK modulation uses a pseudo-random binary sequence $\boldsymbol{P}_0 = \{P_0(i)\}_{i=0,1,\ldots,q-1}$ of length q, where $P_0(i) \in \{0, 1\}$, with good auto-correlation properties. The CCSK modulation maps an element s of GF(q) to the sequence $\boldsymbol{P}_s$ defined as the circular right shift of $\boldsymbol{P}_0$ by s positions:

$$\boldsymbol{P}_s = \{P_0(i - s \bmod q)\}_{i=0,1,\ldots,q-1}. \tag{1.2}$$

The CCSK modulation rate can be defined as $R_m = p/q$, and the Spectral efficiency S_e (i.e. the number of information bit sent by channel use) is given by $S_e = R_c \times R_m = (K \times p)/(N \times q)$. After the NB encoding, a Ka7 So the CCSK frame $\boldsymbol{F}$ is defined as the concatenation of N CCSK symbols:

$$\begin{aligned} \boldsymbol{F} &= [\boldsymbol{P}_{c_0}, \boldsymbol{P}_{c_1}, \ldots, \boldsymbol{P}_{c_{N-1}}] \\ &= \coprod_{k=0}^{N-1} \boldsymbol{P}_{c_k}, \end{aligned} \tag{1.3}$$

where $\coprod$ represents the concatenation operation.

From the CCSK and NB-Code association, the de-mapping process is particularly simple [1]. The input of a NB decoder can be given as the vector of log-likelihood values $\boldsymbol{L} = \{L(s) \triangleq \log(\mathcal{P}(\boldsymbol{P}_s|\boldsymbol{Y}))\}_{s=0,1,\ldots,q-1}$, where $\boldsymbol{Y}$ is a block of length q of the received message $\boldsymbol{y}$ that passes through Gaussian channel, and $\mathcal{P}$ is the probability that the transmitted sequence is $\boldsymbol{P}_s$ given that the received block message $\boldsymbol{Y}$. For a given element $s \in$ GF(q), $L(s)$ can be expressed as the correlation between the received block message $\boldsymbol{Y}$ and expected message $\boldsymbol{P}_s$, $L(s) \cong \langle \boldsymbol{Y}, \boldsymbol{P}_s \rangle$:

$$L(s) \cong \sum_{i=0}^{q-1} Y^*(i) P_s(i) = \sum_{i=0}^{q-1} Y^*(i) P_0(i - s \bmod q), \tag{1.4}$$

for $s = 0, \ldots, q-1$. Hence, the log-likelihood vector $\boldsymbol{L}$ is the circular correlation between the received block message $\boldsymbol{Y}$ of length q and the spreading sequence $\boldsymbol{P}_0$. It can be efficiently computed in the frequency domain as:

$$\boldsymbol{L} = \mathrm{IFFT}(\mathrm{FFT}(\boldsymbol{Y})^* \odot \mathrm{FFT}(\boldsymbol{P}_0)). \tag{1.5}$$

where $\odot$ is the Hadamard product (term by term product).

See deliverable D1.1 and QCSP paper for more details.

1.1.2 Channel model

In this deliverable, we assume a low cost sensor that sporadically transmits small messages in an ALOHA protocol, i.e., without prior time and frequency synchronization to the receiver. The message is thus transmitted in an unknown time, and affected by an unknown delay (depending on the distance between sensors and receiver) and an unknown (but limited) frequency offset. It is thus convenient to express the time of arrival of the frame in the local time domain of the receiver.

Let T_c and T (in second) be the duration of a chip and a CCSK symbol respectively, such that $T = q \times T_c$. The receiver will over-sample the incoming signal with O samples per chip. In other words, the clock frequency F_e of the receiver Analog Digital Converter (ADC) is equal to $F_e = O/T_c$, with O the over-sampling factor (typically between 4 up to 8). Indexing the time by duration T_c of a chip (i.e. O clock cycles), it is possible to determine the time of arrival t_a as a real $x_a = t_a/T_c$ and by decomposing x_a as

$$x_a = k_a + r_a/O + \epsilon_a, \tag{1.6}$$

where $k_a = \lfloor x_a \rfloor$, the integer part of x_a represent the time in number of chips, r_a the closest index of the clock cycle within a chip ($r_a \in \{0, 1, \ldots, O-1\}$) and ϵ_a is the residual timing synchronization error (with $\epsilon_a \in [-\frac{1}{2O}, \frac{1}{2O}]$).

In the sequel, it is considered that the oversampling factor is high enough so ϵ_a is negligible and can be considered equal to 0. Moreover, we will also assume that by testing in parallel all the O hypothesis of the r_a value, we can always manage to set r_a equals to 0. In summary, the frame will be received at chip index k_a and affected by frequency offset f_o.

1.1.3 Detection problem

The detection problem studied in the paper is how to decide, based on the observation of $N \times q$ received samples $\boldsymbol{y} = y(n)_{n=0,1,\ldots,N\times q-1}$, which hypothesis is achieved.

The problem is to develop a reliable score function (or match filter) $S(\boldsymbol{y})$ that takes high values when H1 is fulfilled, and low values when H0 is true. Then, for a given observation, it is possible to take a decision by comparing $S(\boldsymbol{y})$ to a threshold U_0 in order to decide whether a new frame is present (H1) or not (H0). Let us recall some basic notions in detection theory that will be helpful for the derivation of the theoretical model. In detection theory, the detector can give one of the four different cases:

- Miss Detection: $\mathcal{P}_{\text{md}} = \mathcal{P}(S(\boldsymbol{y}) < U_0 |\ \text{H1})$ takes an erroneous decision by signaling the absence of any frame while a frame in fact exists.
- Correct detection: $\mathcal{P}(S(\boldsymbol{y}) \geq U_0 |\ \text{H1})$ correctly detects an existing frame (the probability of correct detection is equal to $1 - \mathcal{P}_{\text{md}}$).
- False alarm: $\mathcal{P}_{\text{fa}} = \mathcal{P}(S(\boldsymbol{y}) \geq U_0 |\ \text{H0})$ takes an erroneous decision by signaling the existence of a frame while a frame in fact does not exist.
- Correct Absence: $\mathcal{P}(S(\boldsymbol{y}) < U_0 |\ \text{H0})$ correctly indicates the absence of a frame (the probability of correct absence is equal to $1 - \mathcal{P}_{\text{fa}}$).

Based on this definition, we obtain:

$$\mathcal{P}_{\text{fa}} = \int_{U_0}^{+\infty} f_{H0}(x)dx, \quad \mathcal{P}_{\text{md}} = \int_{-\infty}^{U_0} f_{H1}(x)dx, \tag{1.7}$$

where f_{H0} and f_{H1} are the probability density functions of the random variable $S(\boldsymbol{y})$ given that H0 is true, H1 is true, respectively. Note that when only part of a frame is inside the detector filter, the output $S(\boldsymbol{y})$ may become greater than U_0, triggering potentially early or late detection. Since $S(\boldsymbol{y})$ is maximised under hypothesis H1, it is natural to consider only this hypothesis in the detection theory study. Note that once detected the synchronisation task estimates the real time of arrival of the frame.

Fig 2.2 (a) illustrates three different threshold values that correspond to various probabilities of false alarm $\mathcal{P}_{\text{fa}} = 10^{-4}, 10^{-6}$ and 10^{-10} versus the output of the correlation filter over a Gaussian channel. It can be clearly inferred from Fig 2.2 (a) that the threshold value U_0 allows a trade-off between $\mathcal{P}_{\text{fa}}$ and $\mathcal{P}_{\text{md}}$. In fact, in a perfect detector, both should be equal to zero to decide perfectly the presence or not of a new frame. In practice, high value of U_0 decreases $\mathcal{P}_{\text{fa}}$ but increases $\mathcal{P}_{\text{md}}$, while low value of U_0 has the symmetrical effect. For example, at threshold value $U_0 = 1200$ that corresponds to $\mathcal{P}_{\text{fa}} = 10^{-4}$, the probability of miss detection is approximately $\mathcal{P}_{\text{md}} = 10^{-4}$. This value increases to $\mathcal{P}_{\text{md}} = 5 \times 10^{-3}$ for U_0 corresponding to $\mathcal{P}_{\text{fa}} = 10^{-10}$. The value of U_0 will be selected according to the system requirements, in the sequel $\mathcal{P}_{\text{fa}}$ will be set to 10^{-6}. We will try to minimize $\mathcal{P}_{\text{md}}$ by proposing an efficient score function, i.e., a score function that is not computationally intensive to be calculated and allows to have low values of $\mathcal{P}_{\text{md}}$.

1.2 Algorithm Specifications

1.2.1 Time and Frequency decomposition

The blind detection algorithm splits the time and frequency domain into a regular grid composed of bins, each bin defined by a time span and a frequency span of size T_b and F_b, respectively. Thus, each bin corresponds to an arrival hypothesis of the frame with a coarse time and frequency precision. The detection method is used in each bin to assess (hypothesis H1) or not (hypothesis H0) the arrival of a frame within the bin. Let ℓ be the number of chips inside the duration T_b, thus $T_b = \ell T_c$. We will assume the frequency offset f_o varies between 0 and $F_{\max}$, thus the number of frequency bins is equal to $N_F = \frac{2F_{\max}}{F_b}$. Note that $qT_cF_b = 1$ means that the effect of frequency offset is equivalent to apply a single rotation between first chip of a CCSK symbol and first chip of the next CCSK symbol. It is thus convenient to replace f_o by $\omega_o = 2\pi f_o T_c q$ to directly translate the impact of frequency offset in a rotation effect on each CCSK symbol.

Every ℓ chips ($\ell \leq q$ typically), the last $N \times q$ received chips are extracted to form the vector $\boldsymbol{y}_\gamma = (y(\gamma\ell + i))_{i=0,1,\ldots,N\times q-1}$ (γ is thus a time index). Then, at the entry of the ρth frequency detector, $\boldsymbol{y}_{\gamma,\rho} = \boldsymbol{y}_\gamma \odot \boldsymbol{E}_\rho$, where $\boldsymbol{E}_\rho = (e^{-j\rho\omega_b n/q})_{n=0,1,\ldots,N-1}$ is computed in order to compensate the frequency offset before entering the detector, with $\omega_b = 2\pi F_b T_c q$.

Let us consider a frame arriving at chip index k_a with a frequency offset f_o. By decomposing k_a as $k_a = \gamma_a \ell + \Delta$, with $-\ell/2 < \Delta \leq \ell/2$ and f_o as $f_o = \rho_a F_b + f'_o$, with $-F_b/2 < f'_o \leq F_b/2$, we can deduce that the frame will be optimally detectable in the bin (γ_a, ρ_a) since in this bin, the locally time offset and frequency offset is minimized.

Note that several bins can be activated in case of an effective frame arrival. In that case, the precise determination of the actual bin and the fine time and frequency inside the bin should be processed. Those steps, called synchronisation, are not described in this paper, and assumed that they can be optimally performed.

To alleviate notation, the frame $\boldsymbol{y}_{\gamma,\rho}$ processed at bin (γ_a, ρ_a) will be denoted as $\boldsymbol{y}$ defined as

$$y(n) = e^{j(\omega_o n/q + \varphi)} \boldsymbol{F}(n - \Delta) + z(n), \tag{1.8}$$

where $z(n)$ are independent realizations of a complex Gaussian noise $\mathcal{CN}(0, \sigma^2)$ of zero mean and variance σ^2, φ is initial phase offset, with $\Delta \in \{-\ell/2, \ldots, \ell/2\}$ and $\omega_0 \in [-\omega_b/2, \omega_b/2]$. The frame $\boldsymbol{F}(i)$ is assumed to be zero when $i < 0$ and $i \geq Nq$. Without loss of generality, Δ will be assumed positive, i.e., $\Delta \in \{0, 1, \ldots, \ell/2\}$.

In case of reception of a frame in the optimal bin (hypothesis H1), the base band transmission model is thus a function of 3 parameters: the time offset Δ, the frequency offset ω_o and the standard deviation σ of the AWGN.

In case of no reception (Hypothesis H0), the base band transmission model is simply

$$y(n) = z(n). \tag{1.9}$$

1.2.2 Detection Method: Description of Score function

This section discusses in details the score function $S(\boldsymbol{y})$, which is the detection algorithm used to detect the CCSK frame. The received data stream $\boldsymbol{y}$ is split in the filter into consecutive segments or blocks $\boldsymbol{Y}_k$, of length q chips each:

$$\boldsymbol{y} = y(n)_{n=0,1,\ldots,N\times q-1} = \coprod_{k=0}^{N-1} \boldsymbol{Y}_k, \tag{1.10}$$

where $\boldsymbol{Y}_k = (y(n))_{n=kq,\ldots,kq+q-1}$.

Thanks to FFT operations (see (1.5)), a cross correlation is performed between the current block $\boldsymbol{Y}_k$ and the reference sequence $\boldsymbol{P}_0$. Let $\Delta \in [0, \ell/2]$ as mentioned before, be the time shift (in number of chips) between the effective time of arrival of the frame and the receiver.

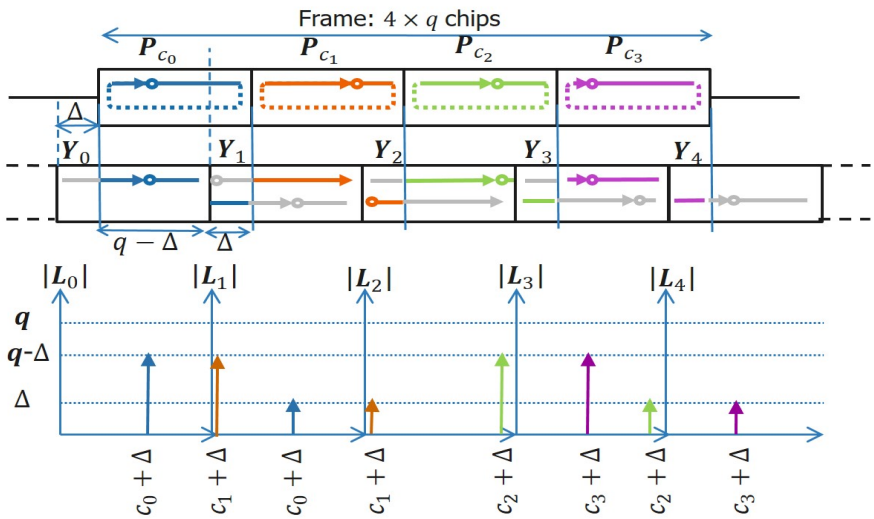

Figure 1.1: Illustration of frame detection principle

The best way to discuss and describe the proposed method (score function) is by giving an example. For that, we assume a frame contains $N = 4$ sequences as in Fig 1.1, each of length q, symbols (c_0, c_1, c_2, c_3) are associated to the four CCSK sequences $(\boldsymbol{P}_{c_0}, \boldsymbol{P}_{c_1}, \boldsymbol{P}_{c_2}, \boldsymbol{P}_{c_3})$, and a distinct color is associated to each symbol. In vector $\boldsymbol{Y}_0$, there are $q - \Delta$ chips that are aligned with the first symbol of the received message of the frame, i.e.$\boldsymbol{P}_{c_0}$, or the $\boldsymbol{P}_0$ sequence circularly shifted by c_0 chips. Relatively to $\boldsymbol{Y}_0$ and because of the delay Δ, the first Δ chips are null, then the sequence starts at time $c_0 + \Delta \pmod q$ which will be presented at the receiver as another sequence $\boldsymbol{P}_{c_0+\Delta}$. So $q - \Delta$ are aligned with the CCSK sequence $\boldsymbol{P}_{c_0+\Delta}$. Thus, the correlation vector $\boldsymbol{L}_k(s)$ related to vector Y_k will give for $k = 0$, $\boldsymbol{L}_0$ that has a spike of height $q - \Delta$ at index $c_0 + \Delta \pmod q$. Similarly, for vector $\boldsymbol{Y}_1$, there are Δ chips that are aligned with the first symbol $\boldsymbol{P}_{c_0}$ with an offset of $c_0 + \Delta$ chips (which is the sequence $\boldsymbol{P}_{c_0+\Delta}$). Thus, the correlation vector $\boldsymbol{L}_1$ will have a spike of height Δ at index $c_0 + \Delta \pmod q$. Moreover, $\boldsymbol{Y}_1$ contains $q - \Delta$ chips aligned with the second symbol of the received message, which gives a spike of height $q - \Delta$ for $\boldsymbol{L}_1$ in position $c_1 + \Delta \pmod q$ (which is the correlation with the sequence $\boldsymbol{P}_{c_1+\Delta}$ and so on).

So, the received block $\boldsymbol{Y}_k$ will have $q - \Delta$ chips of correlation with the CCSK sequences $\boldsymbol{P}_{c_k+\Delta}$ and Δ chips with other sequence $\boldsymbol{P}_{c_{k-1}+\Delta}$. $\boldsymbol{Y}_0$ is a special case as it will have $q - \Delta$ correlation with the CCSK sequence $\boldsymbol{P}_{c_0+\Delta}$.

Thus, the Score function can be obtained using a detection filter $S(\boldsymbol{y})$ of length N acting as forward accumulator:

$$S(\boldsymbol{y}) = \sum_{k=0}^{N-1} \max(|\boldsymbol{L}_k|). \tag{1.11}$$

In the absence of noise with optimized $\boldsymbol{P}_0$ auto-correlation properties where $\langle \boldsymbol{P}_s, \boldsymbol{P}_{s'} \rangle << q$ for $s \neq s'$, the filter output gives $S(\boldsymbol{y}) = N \times (q - \Delta)$.

In order to draw benefit from the second maximum shown in Fig 1.1, it is possible to sum two consecutive correlation vectors before taking its maximum (SC method, for Sum of Correlation). The score function becomes

$$S_{\mathrm{SC}}(\boldsymbol{y}) = \sum_{k=0}^{N-2} \max(|\boldsymbol{L}_k + \boldsymbol{L}_{k+1}|). \tag{1.12}$$

This method is not studied in this deliverable and will be discussed more in the next version, but it is worth mentioning that, compared to the score function $S(\boldsymbol{y})$, $S_{\mathrm{SC}}(\boldsymbol{y})$ gives a slight improvement of detection capacity when Δ is closed to $q/2$, and gives a few dB penalty when Δ is equal to 0. It is also more sensitive to a frequency offset, since the duration of coherent integration is multiplied by 2.

For a given observation received in presence of AWGN noise, the detector can take a decision whether a frame is present or not by comparing $S(\boldsymbol{y})$ to a threshold T that is found based on the Probabilities of miss detection and false alarm as defined in 1.7.

2 Theoretical Performance and Simulation Results

2.1 Theoretical model

In this section, we derive the formal performance model of the frame detection algorithm discussed in the previous section. This model allows to avoid costly estimation performance through Monte-Carlo simulation and gives insight to better analyze the impact of each parameter on the detection performance.

2.1.1 Correlation Expressions

Let us first express the exact expression of $L_k(s)$, see (1.4) for each value of s. Then, we derive the probability law of $|L_k(s)|$ with and without signal.

Definitions and notations

First, let us define the following associated operators, taking into consideration vectors $\boldsymbol{g} = [g_0\ g_1\ \dots\ g_{N-1}]$, and $\boldsymbol{h} = [h_0\ h_1\ \dots\ h_{N-1}]$:

- Sectioning a vector from index p to q:
$$\boldsymbol{g}_p^q = [g_p\ g_{p+1}\ \dots\ g_q].$$
- Concatenation of two vectors $\boldsymbol{g}$ and $\boldsymbol{h}$:
$$\boldsymbol{g} \coprod \boldsymbol{h} = [g_0\ \dots\ g_{N-1}\ h_0\ \dots\ h_{N-1}].$$
- Linear Right and Left shifts of vector $\boldsymbol{g}$ by Δ positions:
$$\mathcal{R}^{\Delta}(g) = \mathbf{0}_0^{\Delta-1} \coprod \boldsymbol{g}_0^{N-\Delta-1}$$
$$\mathcal{L}^{\Delta}(g) = \boldsymbol{g}_{\Delta}^{N-1} \coprod \mathbf{0}_0^{\Delta-1},$$
where $\mathbf{0}_0^{\Delta-1}$ is a zero vector of length Δ.
- Hadamard product of $\boldsymbol{g}$ and $\boldsymbol{h}$:
$$\boldsymbol{g} \odot \boldsymbol{h} = [g_0h_0\ g_1h_1\ \dots\ g_{N-1}h_{N-1}].$$

Based on the discussion in previous sections, $\boldsymbol{y}$ defined in (1.8) and (1.10) can be rewritten in vector-operational form as:

$$\boldsymbol{y} = \mathrm{e}^{j\varphi}\left(\mathcal{R}^{\Delta}(\boldsymbol{F}) \odot \boldsymbol{\Phi}\right) + \boldsymbol{Z}, \tag{2.1}$$

where φ is the initial phase offset, $\mathcal{R}^{\Delta}(\boldsymbol{F})$ the delayed CCSK frame by Δ chips, and $\boldsymbol{\Phi} = \{\mathrm{e}^{j2\pi f_o n}\}_{0\leq n\leq Nq-1}$ a vector representing the effect of frequency offset f_o. $\boldsymbol{Z}$ is the complex AWGN vector: $\boldsymbol{Z} = \boldsymbol{Z}_I + j\boldsymbol{Z}_Q$, where $\boldsymbol{Z}_I$ and $\boldsymbol{Z}_Q$ follow Normal distribution $\mathcal{N}(0, \frac{\sigma^2}{2})$.

Due to the specific structure of the CCSK modulation (all the sequences are cyclically shifted versions of the reference sequence $\boldsymbol{P}_0$), the delayed Frame $\mathcal{R}^{\Delta}(\boldsymbol{F})$ in (2.1) can be expressed as:

$$\mathcal{R}^{\Delta}(\boldsymbol{F}) = \left(\mathbf{0}_0^{\Delta-1} \coprod (\boldsymbol{P}_{c_0})_0^{q-\Delta-1}\right) \coprod \left(\coprod_{k=1}^{N-1} \left((\boldsymbol{P}_{c_{k-1}})_{q-\Delta}^{q-1} \coprod (\boldsymbol{P}_{c_k})_0^{q-\Delta-1}\right)\right). \tag{2.2}$$

Finally, the received vector $\boldsymbol{Y}_0$ can be written as:

$$\boldsymbol{Y}_0 = \mathrm{e}^{j\varphi}\mathcal{R}^{\Delta}\left(\boldsymbol{P}_{c_0}\right) \odot \boldsymbol{\Phi}_0^{q-1} + \boldsymbol{Z}_0^{q-1}, \tag{2.3}$$

and $\boldsymbol{Y}_k$, $k > 0$ as:

$$\boldsymbol{Y}_k = \mathrm{e}^{j\varphi}\left\{\mathcal{L}^{q-\Delta}\left(\boldsymbol{P}_{c_{k-1}}\right) + \mathcal{R}^{\Delta}\left(\boldsymbol{P}_{c_k}\right)\right\} \odot \boldsymbol{\Phi}_{kq}^{kq+q-1} + \boldsymbol{Z}_{kq}^{kq+q-1}. \tag{2.4}$$

Exact expression of $L_k(s)$

Taking into consideration the expression of $\boldsymbol{Y}_k$ defined in (2.4) and the linearity property of the scalar product, the correlation $L_k(s) = \langle \boldsymbol{Y}_k, \boldsymbol{P}_s \rangle$ can be expressed as

$$L_k(s) = L_k(s)^- + L_k(s)^+ + z_k(s), \tag{2.5}$$

where

$$\begin{aligned} L_k^-(s) &= e^{j\varphi} \langle \mathcal{L}^{q-\Delta}\left(\boldsymbol{P}_{c_{k-1}}\right) \odot \boldsymbol{\Phi}_{kq}^{kq+q-1}, \boldsymbol{P}_s \rangle \\ &= e^{j\psi_k} \sum_{n=0}^{\Delta-1} P(n - c_{k-1} - \Delta) P(n-s) \mathrm{e}^{j2\pi f_o n}, \end{aligned} \tag{2.6}$$

$$L_k^+(s) = e^{j\psi_k} \sum_{n=\Delta}^{q-1} P(n - c_k - \Delta) P(n-s) \mathrm{e}^{j2\pi f_o n}, \tag{2.7}$$

and

$$z_k(s) = \langle \boldsymbol{Z}_{kq}^{kq+q-1}, \boldsymbol{P}_s \rangle. \tag{2.8}$$

The phase offset $\psi_k = \varphi + kq2\pi f_o$ represents the sum of the initial phase shift φ and the contribution of the frequency offset f_o on the kth received block Y_k.

Let us analyze (2.5), (2.6) and (2.7) in particular useful cases.
a) When $k = 0$, (2.5) will be reduced to $L_0(s) = L_0^+(s) + z_0(s)$.
b) When $s = c_{k-1} + \Delta$, (2.6) gives

$$L_k^-(c_{k-1} + \Delta) = e^{j\psi_k} \sum_{n=0}^{\Delta-1} e^{j2\pi f_o n} = e^{j\psi_k^-} \left(\frac{\sin(\pi f_o \Delta)}{\sin(\pi f_o)} \right), \tag{2.9}$$

where $\psi_k^- = \psi_k + \pi f_o(\Delta - 1)$.
c) When $s = c_k + \Delta$, (2.7) gives

$$L_k^+(c_k + \Delta) = e^{j\psi_k^+} \left(\frac{\sin(\pi f_o(q - \Delta))}{\sin(\pi f_o)} \right), \tag{2.10}$$

where $\psi_k^+ = \psi_k + \pi f_o(q + \Delta - 1)$.
d) In the particular case where $c_{k-1} = c_k = c$, when $s = c + \Delta$:

$$L_k(c + \Delta) = e^{j(\psi_k + \pi f_o(q-1))} \left(\frac{\sin(\pi f_o q)}{\sin(\pi f_o)} \right) + z_k(s). \tag{2.11}$$

e) It is worth adding that when there is no phase and frequency offset ($\varphi = 0$ and $f_o = 0$), then (2.9), (2.10) and (2.11) give $L_k^-(c_{k-1} + \Delta) = \Delta$, $L_k^+(c_k + \Delta) = (q - \Delta)$ and $L_k(c + \Delta) = q + z_k(s)$, respectively.

From the formal expression of $L_k(s)$ for any value of s, it is possible to derive the exact probability law of $\max(|\boldsymbol{L}_k|)$ used to compute $S(\boldsymbol{y})$ in (1.11).

Finally, according to (2.8), $z_k(s)$ is the sum of q independent Complex Gaussian Random Variable (CGRV) $\mathcal{CN}(0, \sigma^2)$ multiplied by +1 or by -1. Thus, $z_k(s)$ is a realization of Complex Gaussian distribution of law $\mathcal{CN}(0, q\sigma^2)$.

Probability law of $L_k(s)$

Under the hypothesis H0 (no signal), the terms L_k^- and L_k^+ of (2.5) are null and thus, for each s, $L_k(s) = z_k(s)$ is a CGRV of law $\mathcal{CN}(0, q\sigma^2)$ as defined before.

Under the hypothesis H1 (signal exists), when $k > 0$, $L_k(s) = L_k^-(s) + L_k^+(s) + z_k(s)$. The first two terms are deterministic. Their sum can be expressed in polar coordinate as $L_k^-(s) + L_k^+(s) = \rho_k(s) e^{j\theta_k(s)}$, and thus $L_k(s)$ is a CGRV of law $\mathcal{CN}(\rho_k(s) e^{j\theta_k(s)}, q\sigma^2)$. Since we are interested in the

absolute value of $L_k(s)$, the phase $\theta_k(s)$ has no impact. The value of $\rho_k(s) = |L_k^-(s) + L_k^+(s)|$ takes particular values for $s = c_{k-1}$ and $s = c_k$, as shown in 2.1.1.
For the first symbol, when $k = 0$, $L_0(s) = L_0^+(s) + z_0(s)$, and thus $\rho_0(s) = |L_0^+(s)|$.

In next subsections, the distributions of of the absolute values $|L_k(s)|$, $s = 0, 1, \ldots, q-1$, the absolute value of each of the CGRVs are derived.

2.1.2 Probability distributions of $|\boldsymbol{L}_k(s)|$ and maximum of $|\boldsymbol{L}_k(s)|$

In this section we discuss the Probability Density Function (PDF) as well as the Cumulative Distribution Function (CDF) of $|L_k(s)|$ the absolute value of each of the CGRVs representing the elements of the correlation vector $L_k(s)$, $s = 0, 1, \ldots, q-1$, defined in previous section. Then we derive the PDF of the maximum value of $|L_k(s)|$ in both hypothesis $H0$ and $H1$.

PDF and CDF of the absolute value of $L_k(s)$, $|L_k(s)|$

The dependency of $|L_k(s)|$ on the index $k > 0$ depends only on the couple (c_{k-1}, c_k). It is thus convenient to replace k by the couple (c_{k-1}, c_k), or simply by (a, b) to lighten notation. With this notation, $L_{(a,b)}(s)$ is CGRV of law $\mathcal{CN}(\rho_{(a,b)}(s)e^{j\theta_{(a,b)}(s)}, q\sigma^2)$, where $\rho_{(a,b)}(s)$ and $\theta_{(a,b)}(s)$ are the module and the phase of $L^-_{(a,b)}(s) + L^+_{(a,b)}(s)$, respectively. Thus, $|L_{(a,b)}(s)|$ is a Rician distribution with the following PDF and CDF [2]:

$$\begin{aligned} f_{|L_{(a,b)}(s)|}(x) &= \frac{2x}{q\sigma^2} \mathrm{e}^{\left(-\frac{x^2+\rho_{(a,b)}(s)^2}{q\sigma^2}\right)} I_0\left(\frac{2x\rho_{(a,b)}(s)}{q\sigma^2}\right), \\ F_{|L_{(a,b)}(s)|}(x) &= 1 - Q_1\left(\frac{\rho_{(a,b)}(s)}{\sigma\sqrt{q/2}}, \frac{x}{\sigma\sqrt{q/2}}\right), \end{aligned} \tag{2.12}$$

where $x \in [0, +\infty[$, $I_0(z)$ is the modified Bessel function of the first kind with order zero and Q_1 is the Marcum Q-function. For a given couple $a = c_{k-1}$ and $b = c_k$, $F_{|L_{(a,b)}(s)|}(x)$ is plotted in Fig 2.1 for $s = c_{k-1} + \Delta$, $s = c_k + \Delta$ and the other $q-2$ cases when $s \neq c_{k-1} + \Delta$, $s \neq c_k + \Delta$.

PDF and CDF of the Maximum value of $|L_k(s)|$ for H1

Let us define our first hypothesis of the proposed theoretical model. According to (2.8), for any couple (s, s'), we have the inter-correlation $\mathbb{E}[z_k(s), z_k(s')]$ between $z_k(s)$ and $z_k(s')$ equal to $\langle \boldsymbol{P}_s, \boldsymbol{P}_{s'} \rangle$. Since $z_k(s)$ and $z_k(s')$ are both Gaussian variables of zero mean, they are independent if, and only if, $\mathbb{E}[z_k(s), z_k(s')] = 0$. This hypothesis will be assumed in the rest of the paper since the sequence $\boldsymbol{P}_0$ is carefully selected so that $s \neq s' \Rightarrow \langle \boldsymbol{P}_s, \boldsymbol{P}_{s'} \rangle \ll q$. In others words, variables $z_k(s)$ will be considered as independent to each others.

Let us first consider $k > 0$ and let defined $M_{(a,b)}$ as the maximum of the absolute values of $L_{(a,b)}(s)$, i.e. $M_{(a,b)} = \max\{|L_{(a,b)}(s)|, s \in GF(q)\}$. The independence hypothesis of the $z_{(a,b)}(s)$ variables also implies the independence of the $|z_{(a,b)}(s)|$ variables. Thus, the CDF of the $M_{(a,b)}$ denoted by $F_{M_{(a,b)}}$ is defined as the product of the elementary CDFs of each element $F_{|L_{(a,b)}(s)|}$, $s = 0, 1, ..., q-1$

$$F_{M_{(a,b)}}(x) = \prod_{s=0}^{q-1} F_{|L_{(a,b)}(s)|}(x) \tag{2.13}$$

for $x \in [0, +\infty[$. All the CDF functions implied in (2.13) are plotted in Fig. 2.1 for a given couple $a = c_{k-1}$ and $b = c_k$. Since all couples (a, b) are equiprobable. The average value of $F_{M_k}(x)$ is given by marginalizing $F_{M_{(a,b)}}(x)$ over all possible couples, i.e.,

$$F_{M_k}(x) = \frac{1}{q^2} \sum_{(a,b)} F_{M_{(a,b)}}(x), \tag{2.14}$$

as shown in Fig 2.1 also.

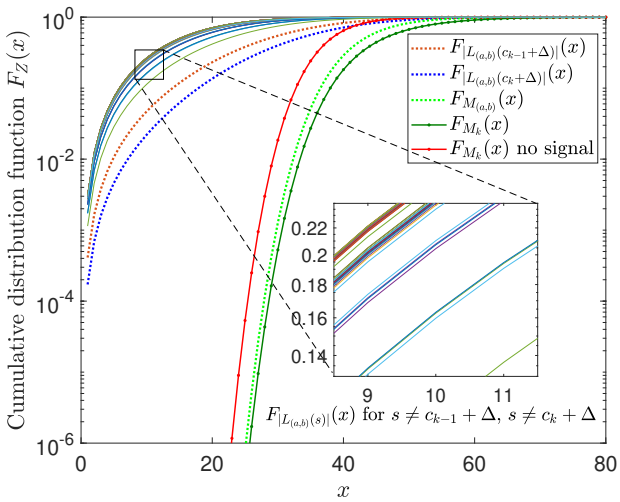

Figure 2.1: Illustration of different CDF equations for a given GF(64) received block $\boldsymbol{Y}_k$ at SNR=-7 dB, $\Delta = 24$ chips and $\omega_o = \pi/4$.

When $k = 0$, M_0 depends only on c_0 and we can replace the index 0 by the value (b) to be consistent with the previous notation, i.e., $M_0 = M_{(b)}$. Thus

$$F_{M_0}(x) = \frac{1}{q} \sum_{(b)} \prod_{s=0}^{q-1} F_{|L_{(b)}(s)|}(x). \tag{2.15}$$

The PDF of the maximum value of the absolute correlation vector denoted by f_{M_k} can be obtained by taking the derivative of F_{M_k}.

$$f_{M_k}(x) = \frac{dF_{M_k}(x)}{dx}. \tag{2.16}$$

The detection filter described in (1.11) takes the sum of N maximum values over a window of N blocks Y_k. Thus the score function can be expressed as:

$$S = \sum_{k=0}^{N-1} M_k. \tag{2.17}$$

In the sequel, we will assume that the M_k, $k = 0, 1, \ldots, N-1$, are independent and identically distributed random variables with common probability density function f_{M_k}. This is an approximation because two consecutive values $|L_k(s)|$ and $|L_{k+1}(s)|$ are not necessarily uncorrelated since the same c_k value is used in both of them. Nevertheless, considering the set of couple L_{2k}, $k = 1..N/2$ are thoroughly random, as for the set $L_{2K+1}, k = 0, ..., N/2-1$. If N is not too small, the space is explored almost randomly. Thus, the PDF of the random variable S can be defined as the convolution of f_{M_k}, $k = 0, 1, \ldots, N-1$:

$$\begin{aligned} f_S(x) &= f_{M_0}(x) * f_{M_1}(x) * \cdots * f_{M_{N-1}}(x) \\ &= f_{M_0}(x) * f_{M_k}^{*(N-1)}(x), \end{aligned} \tag{2.18}$$

where $f_{M_k}^{N-1}(x)$ is the $(N-1)$-fold convolution power of $f_{M_k}(x)$ and $x \in [0, +\infty[$. It is worth mentioning that as the number of symbols N in a packet increases, f_S converges to normal distribution according to central limit theorem. Under the hypothesis $H1$, $f_S(x)$ will be denoted as $f_S^{H1}(x)$.

CDF and PDF of the Maximum value of $|L_k(s)|$ for H0

The distribution of $L_k(s)$ when no frame has been transmitted was given as complex GRV $\mathcal{CN}(0, q\sigma^2)$. In this case, the absolute value of the complex number $L_k(s)$ is a random variable following the Rayleigh distribution [2], where the CDF and PDF of $|L_k(s)|$ are given in (2.19) for $x \in [0, +\infty[$:

$$\begin{aligned} F_{|L_k(s)|}(x) &= 1 - \mathrm{e}^{\left(-\frac{x^2}{q\sigma^2}\right)}, \\ f_{|L_k(s)|}(x) &= \frac{2x}{q\sigma^2}\mathrm{e}^{\left(-\frac{x^2}{q\sigma^2}\right)}. \end{aligned} \tag{2.19}$$

Note that (2.19) is just a particular case of (2.12) when $\rho = 0$. The analysis done in section 2.1.2 can be applied again. The PDF of the maximum value of $|L_k(s)|$ can be obtained by calculating first its CDF,

$$F_{M_k}(x) = \prod_{s=0}^{q-1} F_{|L_k(s)|}(x) = \left[1 - \mathrm{e}^{\left(-\frac{x^2}{q\sigma^2}\right)}\right]^q, \tag{2.20}$$

for $x \in [0, +\infty[$, that is also illustrated in Fig 2.1, and then finding its derivative $f_{M_k}(x)$ such that,

$$f_{M_k}(x) = \frac{2x}{\sigma^2}\mathrm{e}^{\left(-\frac{x^2}{q\sigma^2}\right)}\left[1 - \mathrm{e}^{\left(-\frac{x^2}{q\sigma^2}\right)}\right]^{q-1}. \tag{2.21}$$

Finally, under hypothesis $H0$ the PDF of the random variable S, sum of M_k, can be defined as the convolution of f_{M_k}, $k = 0, 1, \ldots, N-1$:

$$f_S^{H0}(x) = f_{M_k}^{*N}(x), \tag{2.22}$$

which is the N-fold convolution power of $f_{M_k}(x)$.

2.2 Simulation Results and Discussions

The design of the QCSP system relies on the following set of parameters as shown in the theoretical model: Galois field order q, coding rate R_c, number of CCSK symbols in a frame N and the time and frequency offsets.

In this section, after the validation of the theoretical approach, first we assess the detection performance of the system according to the parameters based on the detection probabilities $\mathcal{P}_{\text{md}}$ and $\mathcal{P}_{\text{fa}}$ under low SNRs. Then, we study the effect of the time and frequency offsets in an asynchronized channel on the system performance.

2.2.1 Confirmation of the Theoretical Model by Monte Carlo Simulation

In the previous section we derived the PDFs $f_S^{H1}(x) \backsim \mathcal{P}(X = S(y)|\text{ H1})$ in (2.18) and $f_S^{H0}(x) \backsim \mathcal{P}(X = S(y)|\text{ H0})$ in (2.22) over AWGN channel when the CCSK frame exist or is absent, respectively. In order to check the validity of the hypothesis taken to build the theoretical model, we compare it with the Monte Carlo (MC) simulation, when 10^6 CCSK frames are transmitted, in case of a frame length $N = 20$ GF(64) symbols over AWGN channel of SNR = -10 dB. Two different scenarios are tested, the first one (see Fig 2.2.a) assesses perfect synchronization conditions ($\Delta = 0, w_o = 0$), and the second case (see Fig 2.2.b) is considered for $\Delta = q/4$ and $w_o = \pi/2$. As we can see in both cases, the probability distribution functions in the theoretical model fit exactly the Monte-Carlo simulation. It is worth noting that in the theoretical model we can go through very small numbers in probabilities (here 10^{-10}) without the need to run 10^{10} iterations for a MC simulation for transmitting 10^{10} CCSK frames for example. Thus, the detection performance can be found through the derived theoretical model without the need to conduct extensive MC simulations.

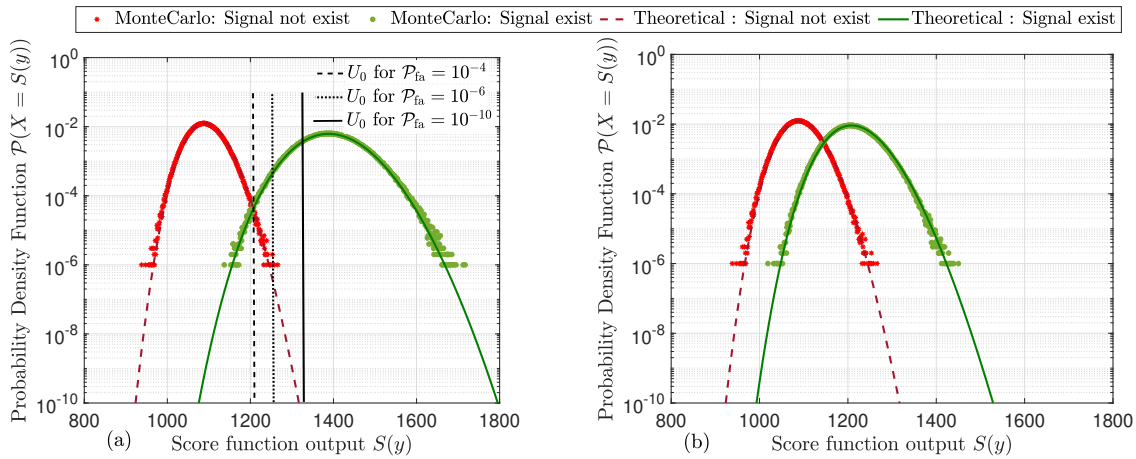

Figure 2.2: MC and Theoretical PDFs in both hypothesis H0 and H1, for a CCSK frame of N=20 symbols in GF(64) for the first scenario **(a)** SNR = -10 dB, $\Delta = 0$, no frequency offset and for the second scenario **(b)** SNR = -10 dB, $\Delta = 16$, $\omega_o = \pi/2$.

2.2.2 Performance Analysis: Effect of Galois Field Order

In this section we study the effect of the length of the spreading sequence, i. e, the order of Galois Field q. Hereafter, we define set of parameters for generating a QCSP frame and illustrating the effect of q on detection performance:

- Number of information bits: $m = 120$.
- NB-Code rate: $R_c = 1/3$.
- Threshold value U_0: is determined for a $\mathcal{P}_{\text{fa}} = 10^{-6}$ as discussed in 1.1.3.
- Perfect time and frequency synchronization: $\Delta = 0$, $w_0 = 0$.

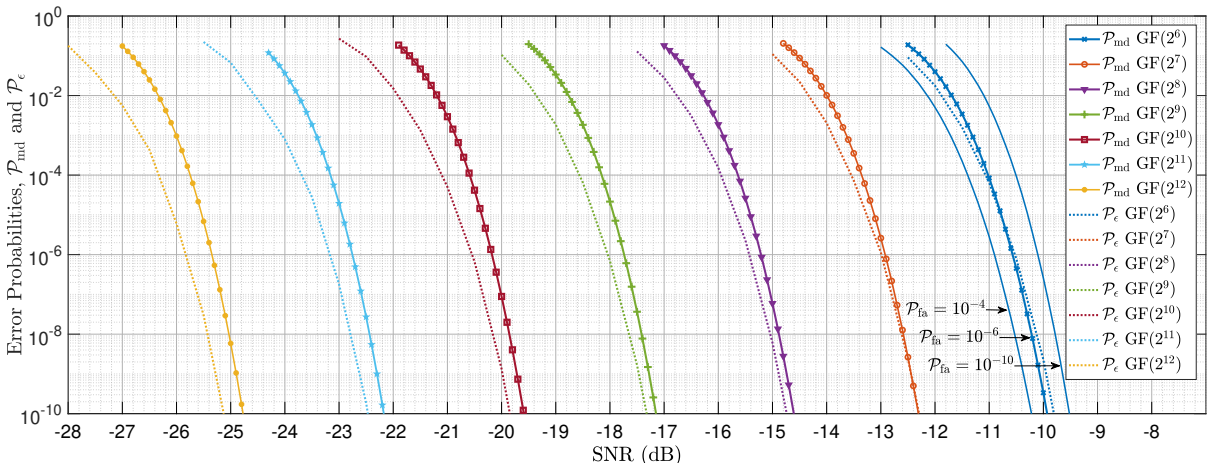

Figure 2.3: $\mathcal{P}_{\text{md}}$ and $\mathcal{P}_{\text{fa}}$ as function of SNR for a CCSK frame of $m = 120$ bits, $R_c = 1/3$ and different GF(q) orders, in an ideally synchronized channel.

Fig 2.3 shows the simulations results of $\mathcal{P}_{\text{md}}$ versus SNR for q ranging from 64 up to 4096, and for a U_0 value corresponding to $\mathcal{P}_{\text{fa}} = 10^{-6}$. For $q = 64$, $\mathcal{P}_{\text{md}}$ is plotted for three different values of

$\mathcal{P}_{\text{fa}}$: 10^{-4}, 10^{-6} and 10^{-10}. As expected, $\mathcal{P}_{\text{md}}$ increases when $\mathcal{P}_{\text{fa}}$ decreases, i.e., when the U_0 value increases. As previously discussed, the value of U_0 is selected based on the desired trade-off $\mathcal{P}_{\text{fa}} - \mathcal{P}_{\text{md}}$. This observation is valid for $q > 64$, but the corresponding curves of $\mathcal{P}_{\text{md}}$ are omitted for the sake of figure simplicity. As shown, the SNR required to obtain an acceptable $\mathcal{P}_{\text{md}}$ of the order of 10^{-4} is -11.05 dB when $q = 64$, and decreases as q increases to go down to -25.8 dB when $q = 4096$. This is a very important result that shows that the proposed detector can operate reliably at very low SNR. $\mathcal{P}_{\text{md}}$ and $\mathcal{P}_{\text{fa}}$ can be chosen depending on the target application.

2.2.3 Performance Analysis: Effect of time and frequency offset

The effect of both time and frequency shifts on the detector performance is discussed in this section. We consider a frame of length $m = 120$ bits over GF(64) with $R_c = 1/3$. Fig 2.4 plots the minimum SNR needed, for predefined probabilities ($\mathcal{P}_{\text{fa}} = 10^{-6}$ and $\mathcal{P}_{\text{md}} = 10^{-4}$), as a function of temporal offsets Δ for different frequency offsets ω_o.

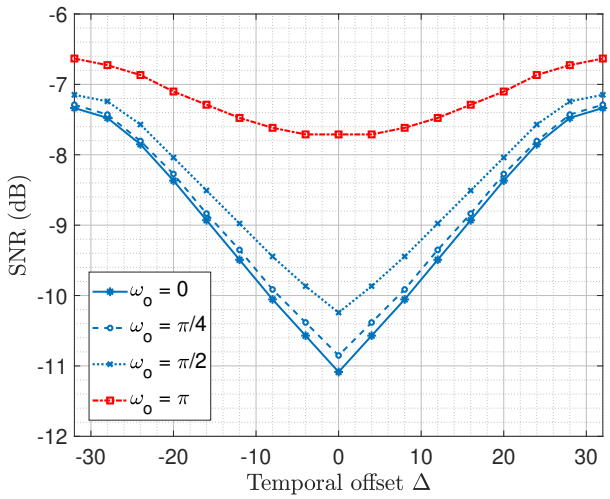

Figure 2.4: Minimum SNR required as function of different Δ and ω_0 values, for defined probabilities ($\mathcal{P}_{\text{fa}} = 10^{-6}$ and $\mathcal{P}_{\text{md}} = 10^{-4}$), in a CCSK frame of $q = 64$, $m = 120$ bits and $R_c = 1/3$.

We can figure out that the rotation of a CCSK frame during q chips by $\omega_o = \pi/2$ radian degrades the minimum SNR by less than 1 dB, while a half rotation when $\omega_o = \pi$ is more than 3 dB. For that, in a case where the frequency offset has the effect of $\omega_o \geq \pi/2$, several filters, one for each frequency offset hypothesis, needs to be performed in parallel. To reduce the overall complexity, we propose to use a similar method to the one proposed by Akopian in [3] for the detection of a GPS signal. An important result to note is the big effect of the time offset Δ. For $\Delta = 0$, the minimal SNR required is -11.1 dB. This value increases with the increase of $|\Delta|$ to attain its maximum value, SNR= -7.35 dB at $|\Delta| = 32$. The gap between $|\Delta| = 0$ and $|\Delta| = q/2$ is approximately 3.7 dB.

With the previous defined system parameters, QCSP frame can be reliably detected at -7.2 dB with time shift up to $|\Delta| = q/2$, and frequency offset up to $\pi/2$. Following this GF(64) system, we can detect also at minimal SNR by changing the values of time and frequency decomposition (time and frequency span for the grids) that discussed before in 1.2.1. For example, we can work at SNR -8.9 dB by limiting the deviation to $q/4 = 16$ chips at most, but we need 2 filters in parallel. Another solution can be taken at the receiver side, a detection filter that considered every $\ell = q/2$ instead of $\ell = q$ chips, so the last $N \times q$ chips are extracted from the stream of incoming sample and the maximum time synchronization error will be limited to $q/4$. Also, at -10.1 dB for example, we can tolerate a deviation of $q/8 = 8$ at most. For that, it will be necessary to have 4 filters in parallel to guarantee the reliable detection needed or at the receiver side the detection filter is considered every $\ell = q/4$.

Based on the application requirements we can adjust the system either to work on lower SNR with

higher complexity due to the decrease in the time and frequency span, or it will be sufficient to work on the minimal SNR for worst case scenario where $\Delta = q/2$ and $\omega_o = \pi/2$.

2.2.4 Detection-Correction approach and Polyanskiy's bound

At a very low SNR, the successful transmission of short frames as targeted by the NB-code and CCSK association in the QCSP system is a challenging problem. In fact, the overall joint probability of successful transmission in an asynchronous ALOHA system can be expressed as $\mathcal{P} = \mathcal{P}_d \times \mathcal{P}_s \times \mathcal{P}_{c/s}$, where $\mathcal{P}_d$ is the probability of detection of the frame, $\mathcal{P}_s$ is the probability of correct estimation of the synchronization parameters, and $\mathcal{P}_{c/s}$ is the probability of correction of all transmission errors by the NB-code that is conditioned by the synchronization accuracy. Aiming to maximize the probability of successful transmission, we must also maximize the probability of detection, synchronization, and decoding. Then, assuming perfect synchronization, we obtain $\mathcal{P} = \mathcal{P}_d \times \mathcal{P}_c$. The challenge here is to minimize the energy cost of the frame for a reliable transmission for a finite frame length. In order to interpret this challenge, we need first to find the minimum CCSK frame length N for a given probability of detection $\mathcal{P}_d$, where $\mathcal{P}_d = 1 - \mathcal{P}_{\text{md}} - \mathcal{P}_{\text{fa}}$. Fig. 2.5 shows the minimum CCSK frame length $N_q = N \times q$ in chips as function of SNR, for $p = 6$ (right-most curve) to $p = 12$ (left-most curve), needed for $\mathcal{P}_{\text{md}} = 10^{-4}$ and $\mathcal{P}_{\text{fa}} = 10^{-6}$, in an ideally synchronized channel (no frequency and no time offset).

At different SNR values, we can find the minimum size of the code in chips to guarantee target probabilities of detection ($\mathcal{P}_{\text{md}} \leq 10^{-4}$ and $\mathcal{P}_{\text{fa}} \leq 10^{-6}$) that correspond to each order of CCSK modulation p. It is worth noticing that a QCSP frame contains at least one CCSK symbol, i.e., q chips. It explains the flat region at high SNRs, where a unique CCSK symbol is able to guarantee both ($\mathcal{P}_{\text{md}} \leq 10^{-4}$ and $\mathcal{P}_{\text{fa}} \leq 10^{-6}$).

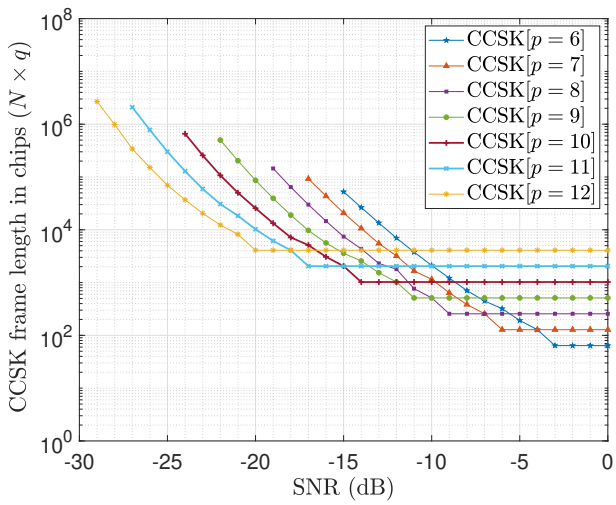

Figure 2.5: Minimum CCSK frame length in chips, needed for $\mathcal{P}_{\text{md}} \leq 10^{-4}$ and $\mathcal{P}_{\text{fa}} \leq 10^{-6}$, for different p values in an ideally synchronized channel.

The maximum achievable coding rate, denoted by R_c^*, for error correction codes with error probability $\mathcal{P}_\epsilon$ (where $\mathcal{P}_c = 1 - \mathcal{P}_\epsilon$), can be tightly approximated as in [4] by

$$R_c^* \approx R - \sqrt{\frac{V}{N}} Q^{-1}(\mathcal{P}_\epsilon) \tag{2.23}$$

where R is the channel capacity (maximum rate achievable in the asymptotic regime), V is the channel dispersion (defined in [4]) and Q^{-1} the inverse Q function where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp\left(-\frac{u^2}{2}\right) du$. We use the above approximation (known as the *normal approximation*) as a definition of the maximum

achievable coding rate in the finite code-length regime. In [4] the channel dispersion parameter is defined as

$$V = H_2(U|Y) - H(U|Y)^2, \tag{2.24}$$

where $H(U|Y)$ is the conditional entropy of the channel input U given the channel output Y, and

$$H_2(U|Y) \triangleq \mathbb{E}_Y \left[- \sum_{s \in \mathbb{Z}_q} L(s)(\log_q(L(s))^2 \right], \tag{2.25}$$

where $L(s) \triangleq \mathcal{P}(U = s|Y)$ denotes the conditional probability distribution of U given Y. Hence, $H_2(U|Y)$ can be conveniently estimated by Monte-Carlo simulation.

In practice, we fix the NB-Code rate R_c in QCSP system to $R_c = 1/3$ so we can use (2.23) to find the error probability defined as:

$$\mathcal{P}_\epsilon = Q\left(-\frac{R_c - R}{\sqrt{V/N}}\right). \tag{2.26}$$

Let us consider a QCSP frame over GF(q) with payload of $m = 120$ bits of information. We also assume a perfectly synchronized reception ($\Delta = 0$, $\omega_o = 0$). Fig. 2.3 shows both the evolution of $\mathcal{P}_\epsilon$ and $\mathcal{P}_{\text{md}}$ as a function of the SNR for several values of the Galois Field order q. We note that, as q increases, detection becomes more problematic than correction.

3 General Conclusion

The current detection algorithm achieved the performance expected by the QCSP project. It may not need any further evolution and the work should now focus on an efficient way of implementation. The current detection algorithm of QCSP frame which relies on the CCSK modulation is described by details. The whole frame is considered as a preamble sequence to perform the detection and will be for synchronization also (described in deliverable 2.3). Thanks to this structure, QCSP frame offers the capability of blind detection and self-synchronization without additional overhead. Also a formal performance model of the frame detection algorithm has been derived. This model gave some insight on the impact of each parameter on detection performance according to the QCSP frame structure (size and GF order) and the time and frequency offset.

About new detection algorithms, we would like to explore a promising method that uses the fact that CCSK symbols are linked by the NB code in the next version of this deliverable.

Bibliography

[1] O. Abassi, L. Conde-Canencia, M. Mansour, and E. Boutillon, "Non-Binary Low-Density Parity-Check coded Cyclic Code-Shift Keying," in *2013 IEEE Wireless Communications and Networking Conference (WCNC)*, April 2013, pp. 3890–3894.

[2] N. C. Beaulieu, "An infinite series for the computation of the complementary probability distribution function of a sum of independent random variables and its application to the sum of Rayleigh random variables," *IEEE Transactions on Communications*, vol. 38, no. 9, pp. 1463–1474, Sep. 1990.

[3] D. Akopian, "Fast FFT based GPS satellite acquisition methods," *IEE Proceedings - Radar, Sonar and Navigation*, vol. 152, no. 4, pp. 277–286, Aug 2005.

[4] Y. Polyanskiy, H. V. Poor, and S. Verdu, "Channel Coding Rate in the Finite Blocklength Regime," *IEEE Transactions on Information Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.

