Closed-Form Cramér-Rao Lower Bounds for CFO and Phase Estimation from Turbo-Coded Square-QAM-Modulated signals

Faouzi Bellili, Achref Methenni, and Sofiène Affes
INRS-EMT, 800, de la Gauchetière Ouest, Bureau 6900, Montreal, Qc, H5A 1K6, Canada.
Emails: {bellili,methenni,affes}@emt.inrs.ca.

***Abstract*—We consider the problem of joint phase and carrier frequency offset (CFO) estimation from turbo-coded square-QAM modulated signals. We derive for the first time the closed-form expressions for the exact Cramér-Rao lower bounds (CRLBs) of this estimation problem. In particular, we introduce a new recursive process that enables the construction of arbitrary Gray-coded square-QAM constellations. Some hidden properties of such constellations will be revealed and carefully handled in order to decompose the likelihood function (LF) into the sum of two analogous terms. This decomposition makes it possible to carry out *analytically* all the statistical expectations involved in the Fisher information matrix (FIM). The new analytical CRLB expressions corroborate the previous attempts to evaluate the underlying perfromance bounds *empirically*. In the low-to-medium signal-to-noise ratio (SNR) region, the CRLB for code-aided (CA) estimation lies between the bounds for completely blind [non-data-aided (NDA)] and completely data-aided (DA) estimation schemes, thereby highlighting the coding gain potential in CFO and phase estimation. Most interestingly, in contrast to the NDA case, the CA CRLBs start to decay rapidly and reach the DA bounds at relatively small SNR thresholds. The derived bounds are also valid for LDPC-coded systems and they can be evaluated in the same way when the latter are decoded using the turbo principal.**

***Index Terms*—Carrier phase shift, carrier frequency offset (CFO), Cramér-Rao lower bound (CRLB), turbo/LDPC codes, code-aided (CA), extrinsic information, Gray mapping, square QAMs.**

I. Introduction

CURRENT and next-generation wireless communication systems are called upon to provide high quality of service, while satisfying the increasing demand for higher data rates. In order to meet these requirements, the use of powerful error-correcting codes such as turbo codes [1] in conjunction with high spectral efficiency modulations such as high-order quadrature amplitude modulations (QAMs) is advocated. In this context, turbo codes and QAM signals have already been adopted for 4G mobile communication systems such as Mobile WiMAX (IEEE 802.16e) [2], long-term evolution (LTE), LTE-advanced (LTE-A) and beyond (LTE-B) [3].

Yet, turbo codes are known to be very sensitive to synchronization errors. In fact, even small values for the carrier frequency offset (CFO) and/or phase shift may entail severe performance degradations. One of the obvious solutions to this problem consists in using turbo codes in conjunction with a coherent detection scheme. In other words, the carrier phase shift and the CFO are estimated and compensated for before proceeding to data decoding. As such, the synchronization parameters are estimated directly from the received samples at the output of the matched filter. In doing so, two estimation schemes can be envisaged i) NDA estimation with no *a priori* knowledge about the transmitted symbols or ii) DA estimation using perfectly known pilot sequences. Yet, turbo-coded systems are primarily intended to operate at low SNR thresholds. On one hand, in such adverse SNR conditions, NDA techniques result in high estimation errors affecting thereby the overall system performance. On the other hand, accurate DA synchronization requires large training sequences which limits, in turn, the effective system capacity.

To circumvent this problem and properly synchronize turbo-coded systems, a more elaborate solution known as *turbo synchronization* has gained considerable attention over the last two decades. It consists in using the soft information (either the *a posteriori* probabilities or the *extrinsic* information) provided by the turbo receiver at each decoding iteration in order to enhance the synchronization performance. In other words, the estimation task is assisted by the decoder and will thus be refered to as *code-aware* or *code-aided* (CA) estimation, as opposed to non-code-aided (NCA) estimation (i.e., NDA scenario).

Many techniques for CA estimation of the phase shift and the CFO have been reported in the open literature (see [4-11] and references therein). The performance of such CA estimators is usually assessed in terms of error variance; yet it still requires to be gauged against an absolute benchmark. The Cramér-Rao lower bound (CRLB), a well known fundamental bound [12], meets this requirement since it sets the minimum achievable variance for any unbiased estimator. Most interestingly, the *stochastic* CRLB (unknown and random transmitted symbols) is known to be achieved asymptotically by the stochastic maximum likelihood (ML) estimator. Yet, even under uncoded transmissions, the complex structure of the LF makes it extremely hard, if not impossible, to derive analytical expressions for this bound, especially for high-order modulations. Therefore, it is often evaluated empirically (in both NCA and CA estimations). Indeed, the stochastic CRLBs for the carrier phase and CFO NDA estimation were first evaluated empirically in both cases of uncoded PSK- and symmetric-QAM-modulated signals [13]. It was not until recently, though, that the closed-form expressions of the *stochastic* CRLBs were ultimately established for arbitrary square QAM-modulated signals in [15, 22] for the estimation of various channel parameters, but still in the traditional NCA scenario.

In coded transmissions, however, the LF becomes even more complicated and developing CRLBs in closed form is obviously a lot more difficult. Thus, exhaustive Monte-Carlo simulations have been recently adopted by Noels *et al.* in [23, 24] to evaluate *empirically* the CA CRLBs for the carrier phase and CFO estimation from turbo-coded linearly-modulated signals. However, no analytical expressions for such interesting CA CRLBs are yet available in the open literature. Motivated by these facts, we derive for the very first time the closed-form expressions for the considered CRLBs in CA estimation from any turbo-coded square-QAM-modulated signal and show that they corroborate the aforementioned attempts [23, 24] to evaluate these bounds *empirically*.

We structure the rest of this paper as follows. In section II, we present the system model. In section III, we derive the log-likelihood function of the system. In section IV, we derive the different FIM elements and the analytical expressions for the considered CA CRLBs. In section V, we present some graphical representations for the newly derived bounds and, finally, draw out some concluding remarks in section VII.

We mention beforehand that some of the common notations will

Work supported by the Discovery Grants Program of NSERC and a Discovery Accelerator Supplement (DAS) Award.

be used in this paper. In fact, vectors and matrices are represented in lower- and upper-case bold fonts, respectively, and j is the pure complex number that verifies $j^2 = -1$. The operators $\Re\{.\}$, $\Im\{.\}$, $\{.\}^*$ and $|.|$ return, respectively, the real part, imaginary part, the conjugate and amplitude of any complex number. Moreover, $P[.]$ and $p[.]$ denote the probability mass function (PMF) and the pdf for discrete and continuous random variables, respectively. The statistical expectation is denoted as $E\{.\}$.

II. System Model

A binary sequence of information bits is fed into a turbo encoder consisting of two identical recursive and systematic convolutional codes (RSCs) which are concatenated in parallel via an interleaver of size L. The coded bits are then fed into a puncturer which selects an appropriate combination of the parity bits, from both encoders, in order to achieve the desired overall rate R. The obtained coded bits (systematic and parity bits) are scrambled with an outer interleaver, and then mapped onto any square-QAM Gray-coded constellation. The information-bearing symbols are transmitted over the wireless channel and the analog received signal is sampled at the output of the matcheded filter. With *imperfect* phase and frequency synchronization, the obtained samples are modeled as follows:

$$y(k) \quad = \quad S\ x(k)e^{j(2\pi k\nu+\phi)} + w(k), \tag{1}$$

for $k = k_0, k_0+1, \cdots, k_0+K-1$ where k_0 is the time instant of the first observed sample and K is the total number of recorded data. The K unknown transmitted symbols, $\{x(k)\}_k$ are drawn from any M-ary Gray-coded square-QAM constellation whose alphabet is denoted as $\mathcal{C}_p = \{c_1, c_2, \cdots, c_M\}$. By *square* QAM we mean $M = 2^{2p}$ (i.e., QPSK, $16-$QAM, $64-$QAM, etc...). The noise components, $\{w(k)\}_k$, are modeled by zero-mean circular complex Gaussian random variables with independent real and imaginary parts (each of variance σ^2). For more convenience, we stack the unknown phase and frequency offsets (respectively, ϕ and ν) into the vector $\boldsymbol{\alpha} = [\phi \quad \nu]^T$. They are to be estimated from all the received samples gathered in the observation vector $\boldsymbol{y} = [y(k_0), y(k_0+1), \cdots, y(k_0+K-1)]^T$. Without loss of generality (w.l.o.g), we assume that the energy of the transmitted symbols is normalized to one[1] (i.e., $\mathrm{E}\{|x(k)|^2\} = 1$) so that the average SNR of the system is given by $\rho = \mathrm{E}\left\{S^2|x(k)|^2\right\}/2\sigma^2 = S^2/2\sigma^2$. The CRLB is a practical lower bound that verifies[2] the inequality $\mathrm{E}\left\{[\widehat{\boldsymbol{\alpha}}-\boldsymbol{\alpha}][\widehat{\boldsymbol{\alpha}}-\boldsymbol{\alpha}]^T\right\} \succeq \mathbf{CRLB}(\boldsymbol{\alpha})$ for any unbiased estimator $\widehat{\boldsymbol{\alpha}}$ of $\boldsymbol{\alpha}$ which is given by:

$$\mathbf{CRLB}(\boldsymbol{\alpha}) = \boldsymbol{I}^{-1}(\boldsymbol{\alpha}), \tag{2}$$

where $\boldsymbol{I}(\boldsymbol{\alpha})$ is the Fisher information matrix (FIM) with entries:

$$[\boldsymbol{I}(\boldsymbol{\alpha})]_{i,l} = -\mathrm{E}\left\{\frac{\partial^2 L(\boldsymbol{y};\boldsymbol{\alpha})}{\partial\alpha_i\partial\alpha_l}\right\} \qquad i,l = 1,2. \tag{3}$$

in which $\{\alpha_i\}_{i=1,2}$ are the elements of the parameter vector $\boldsymbol{\alpha}$ and $L(\boldsymbol{y};\boldsymbol{\alpha}) \triangleq \ln\left(p[\boldsymbol{y};\boldsymbol{\alpha}]\right)$ is the log-likelihood function (LLF) of the system ($p[\boldsymbol{y};\boldsymbol{\alpha}]$ is the pdf of $\boldsymbol{y}$ parameterized by $\boldsymbol{\alpha}$).

III. Derivation of the LLF

Due to space limitations, we will present in this paper the main derivation steps without delving too much into details. For detailed proofs of the upcoming results, the reader is referred to the complete journal version of this work in [25]. Throughout this paper, we assume that the constellation is Gray coded. Each point of the alphabet, $\{c_m\}_{m=1}^{M}$, is mapped onto a unique sequence of $\log_2(M)$ bits denoted here as $\bar{b}_1^m\bar{b}_2^m\cdots\bar{b}_l^m\cdots\bar{b}_{\log_2(M)}^m$. For the sake of clarity, this mapping will be denoted as follows:

$$c_m \longleftrightarrow \bar{b}_1^m\bar{b}_2^m\cdots\bar{b}_l^m\cdots\bar{b}_{\log_2(M)}^m. \tag{4}$$

The same notation is used to refer to the k^{th} bit sequence, $b_1^k b_2^k\cdots b_l^k\cdots b_{\log_2(M)}^k$, that is conveyed by the k^{th} symbol $x(k)$, i.e., $x(k) \longleftrightarrow b_1^k b_2^k\cdots b_l^k\cdots b_{\log_2(M)}^k$. Due to the large-size interleaver, the coded bits can be assumed as statistically independent. This assumption is indeed pervasive in CA estimation (see [4, 23, 24] and references therein). Consequently, the transmitted symbols (which are *soft* representations for different blocks of such independent bits) can also be considered as independent, i.e.:

$$p[\boldsymbol{y};\boldsymbol{\alpha}] = \prod_{k=k_0}^{k_0+K-1} p[y(k);\boldsymbol{\alpha}], \tag{5}$$

where $p[y(k);\boldsymbol{\alpha}]$ is the pdf of the individual received sample, $y(k)$, which is given by:

$$\begin{aligned} p[y(k);\boldsymbol{\alpha}] &= \sum_{c_m\in\mathcal{C}_p} P[x(k)=c_m]p[y(k);\boldsymbol{\alpha}|x(k)=c_m], \\ &= \sum_{c_m\in\mathcal{C}_p} \frac{P[x(k)=c_m]}{2\pi\sigma^2}\exp\left\{\frac{|y(k)-S_{\phi,\vartheta}\ c_m|^2}{2\sigma^2}\right\}, \end{aligned} \tag{6}$$

in which we use the notation $S_{\phi,\vartheta} = Se^{j(2\pi k\vartheta+\phi)}$. Now, in the case of square-QAM modulations where each constellation point represents $2p$ bits (i.e., $\log_2(M) = 2p$), and again, due to the independence of the coded bits, the *a priori* probabilities are factorized as follows:

$$P[x(k)=c_m] = \textstyle\prod_{l=1}^{2p} P\left[b_l^k = \bar{b}_l^m\right], \quad m = 1,2,\cdots,M. \tag{7}$$

We also define the so-called log-likelihood ratio (LLR) of each transmitted bit, b_l^k, as follows:

$$L_l(k) = \ln\left(\frac{P[b_l^k=1]}{P[b_l^k=0]}\right). \tag{8}$$

Then, by using $P[b_l^k=0] + P[b_l^k=1] = 1$, it can be shown that:

$$P[b_l^k=1] = \frac{e^{L_l(k)/2}}{2\cosh\left(L_l(k)/2\right)},\ P[b_l^k=0] = \frac{e^{-L_l(k)/2}}{2\cosh\left(L_l(k)/2\right)}. \tag{9}$$

These two results can be combined to obtain a single generic formula:

$$P[b_l^k = \bar{b}_l^m] = \frac{e^{(2\bar{b}_l^m-1)\frac{L_l(k)}{2}}}{2\cosh\left(L_l(k)/2\right)}, \tag{10}$$

where $\bar{b}_l^m$ can be 0 or 1 depending on which symbol c_m is transmitted during the k^{th} period. Therefore, recalling that $\log_2(M) = 2p$ (for square-QAM constellations) and injecting (10) in (7), it follows that:

$$P[x(k)=c_m] = \underbrace{\left(\prod_{l=1}^{2p}\frac{1}{2\cosh\left(L_l(k)/2\right)}\right)}_{\beta_k}\prod_{l=1}^{2p} e^{(2\bar{b}_l^m-1)\frac{L_l(k)}{2}}. \tag{11}$$

Now, by denoting $I(k) \triangleq \Re\{y(k)\}$ and $Q(k) \triangleq \Im\{y(k)\}$, it can be shown that the pdf in (6) is given by:

$$p[y(k);\boldsymbol{\alpha}] = \frac{1}{2\pi\sigma^2}\exp\left\{-\frac{I(k)^2+Q(k)^2}{2\sigma^2}\right\}D_{\boldsymbol{\alpha}}(k), \tag{12}$$

[1]If the transmit energy, P, is not unitary, it can be easily incorporated as an unknown scaling factor into the channel coefficient which becomes $\sqrt{P}S$ instead of S in (1).

[2]Note that $\boldsymbol{A} \succeq \boldsymbol{B}$ for any two square matrices $\boldsymbol{A}$ and $\boldsymbol{B}$ means that $\boldsymbol{A}-\boldsymbol{B}$ is positive semi-definite.

where

$$D_{\boldsymbol{\alpha}}(k) = \sum_{c_m \in \mathcal{C}_p} P[x(k) = c_m] e^{-\frac{S^2|c_m|^2}{2\sigma^2}} \exp\left\{\frac{\Re\left\{c_m y(k)^* S_{\phi,\vartheta}\right\}}{\sigma^2}\right\}. \quad (13)$$

After taking the logarithm of (12) and dropping the constant terms that do not depend neither on ϕ nor on ν, the *useful* LLF reduces simply to $L(\boldsymbol{y};\boldsymbol{\alpha}) = \sum_{k=K_0}^{k_0+K-1} \ln\big(D_{\boldsymbol{\alpha}}(k)\big)$. At this stage, it is still impossible to derive analytical expressions for the considered CRLBs without further manipulating the term $D_{\boldsymbol{\alpha}}(k)$. Actually, considering the special case of square-QAM-modulated signals, and judiciously exploiting the structure of the Gray mapping mechanism, we are able to factorize $D_{\boldsymbol{\alpha}}(k)$ into the product of two analogous terms. In fact, when $M = 2^{2p}$ for any integer $p \geq 2$ (i.e., square-QAM constellations), we have $\mathcal{C}_p = \{\pm(2i-1)d_p \pm j(2n-1)d_p\}_{i,n=1,2,\ldots,2^{p-1}}$, where $2d_p$ is the intersymbol distance in the I/Q plane. For normalized-energy square-QAM constellations $\big($i.e., $\frac{1}{2^{2p}}\sum_{m=1}^{2^{2p}}|c_m|^2 = 1\big)$, it can be shown that:

$$d_p = \frac{2^{p-1}}{\sqrt{2^p \sum_{m=1}^{2^{p-1}}(2m-1)^2}}. \quad (14)$$

Now, by defining $\tilde{\mathcal{C}}_p$ to be the top-right quadrant of the constellation, we have $\mathcal{C}_p = \tilde{\mathcal{C}}_p \cup (-\tilde{\mathcal{C}}_p) \cup \tilde{\mathcal{C}}_p^* \cup (-\tilde{\mathcal{C}}_p^*)$ and thus (13) can be rewritten as:

$$\begin{aligned} D_{\boldsymbol{\alpha}}(k) = \sum_{\tilde{c}_m \in \tilde{\mathcal{C}}_p} & \exp\left\{-\frac{S^2|\tilde{c}_m|^2}{2\sigma^2}\right\} \times \\ & \Bigg(P[x(k) = \tilde{c}_m]\exp\left\{\frac{\Re\{\tilde{c}_m y^*(k) S_{\phi,\vartheta}\}}{\sigma^2}\right\} \\ & + P[x(k) = -\tilde{c}_m]\exp\left\{\frac{\Re\{-\tilde{c}_m y^*(k) S_{\phi,\vartheta}\}}{\sigma^2}\right\} \\ & + P[x(k) = \tilde{c}_m^*]\exp\left\{\frac{\Re\{\tilde{c}_m^* y^*(k) S_{\phi,\vartheta}\}}{\sigma^2}\right\} \\ & + P[x(k) = -\tilde{c}_m^*]\exp\left\{\frac{\Re\{-\tilde{c}_m^* y^*(k) S_{\phi,\vartheta}\}}{\sigma^2}\right\}\Bigg). \end{aligned} \quad (15)$$

Next, we describe a simple process for the recursive construction of any Gray-coded square-QAM constellation. Some hidden properties of such constellations will be revealed — from this recursive process — and carefully exploited in order to factorize the term $D_{\boldsymbol{\alpha}}(k)$ in (15). In fact, starting from any basic QPSK constellation and a given $2^{2(p-1)}$-QAM Gray-coded constellation, it is possible to build a 2^{2p}-QAM Gray-coded one as follows:

- *step 1*: build the top right quadrant of the desired 2^{2p}-QAM constellation from all the points[3] of the available $2^{2(p-1)}$-QAM constellation.
- *step 2*: build the three remaining quadrants of the new 2^{2p}-QAM constellation by symmetries on: i) the x-axis to obtain the bottom-right quadrant, ii) the y-axis to obtain the top-left quadrant; and iii) the center point to obtain the bottom-left quadrant. Yet, the points of the original $2^{2(p-1)}$-QAM constellation represent each $2(p-1)$ bits only. Therefore, two bits are still missing in each point of the new 2^{2p}-QAM constellation that must represent $2p$ bits.
- *step 3*: copy the two missing bits from each quadrant of a basic Gray-coded QPSK constellation to all the points that belong to the same quadrant of the new constellation.

[3]The same points' layout in the original $2^{2(p-1)}$-QAM constellation is used, i.e., the constellation is placed as is in the new quadrant.

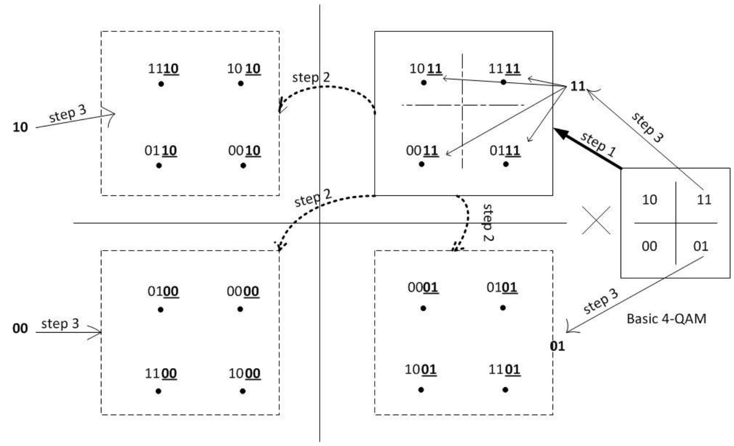

Fig. 1. Recursive construction of Gray-coded square-QAM constellations illustrated here from 4-QAM to 16-QAM.

As one example given in Fig. 1, we illustrate the recursive construction of a Gray-coded 16-QAM constellation from a 4-QAM Gray-coded one. In the sequel, we will use w.l.o.g as a basic QPSK constellation the one depicted in Fig. 1 and assume that the two bits added in "*step 3*" always occupy the two least significant positions. Due to symmetries in "*step 2*", each four symbols $\tilde{c}_m$, $\tilde{c}_m^*$, $-\tilde{c}_m$ and $-\tilde{c}_m^*$ have the same $2(p-1)$ most significant bits (MSBs), $\bar{b}_1^m\bar{b}_2^m\bar{b}_3^m\ldots\bar{b}_{2p-3}^m\bar{b}_{2p-2}^m$, for any symbol $\tilde{c}_m \in \tilde{\mathcal{C}}_p$. Thus, if we consider these $2(p-1)$ MSBs alone and define:

$$\mu_{k,p}(c_m) \triangleq \prod_{l=1}^{2p-2} e^{(2\bar{b}_l^m - 1)\frac{L_l(k)}{2}}, \quad \forall c_m \in \mathcal{C}_p, \quad (16)$$

we can then immediately see that:

$$\mu_{k,p}(\tilde{c}_m) = \mu_{k,p}(-\tilde{c}_m) = \mu_{k,p}(\tilde{c}_m^*) = \mu_{k,p}(-\tilde{c}_m^*),\ \forall \tilde{c}_m \in \tilde{\mathcal{C}}_p. \quad (17)$$

As seen from the right-hand side of (16), $\mu_{k,p}(c_m)$ is not defined for $p = 1$, i.e., for QPSK constellations. We extend its definition for the latter by taking $\mu_{k,1}(c_m) = 1\ \ \forall\ c_m \in \mathcal{C}_1$. It will be seen later that this choice is consistent with all the derivations. Moreover, by recalling the *basic* QPSK depicted in Fig. 1, the two remaining LSBs are given by "$\bar{b}_{2p-1}^m\bar{b}_{2p}^m$" = "11", "00", "01", and "10", for each $\tilde{c}_m \in \tilde{\mathcal{C}}_p$, $-\tilde{\mathcal{C}}_p$, $\tilde{\mathcal{C}}_p^*$, and $-\tilde{\mathcal{C}}_p^*$, respectively. Using these results along with (16) and (17) in (11), it follows that for any $\tilde{c}_m \in \tilde{\mathcal{C}}_p$, we have:

$$P[x(k) = \tilde{c}_m] = \beta_k\ \mu_{k,p}(\tilde{c}_m)\ e^{\frac{L_{2p-1}(k)}{2}} e^{\frac{L_{2p}(k)}{2}}, \quad (18)$$

$$P[x(k) = \tilde{c}_m^*] = \beta_k\ \mu_{k,p}(\tilde{c}_m)\ e^{-\frac{L_{2p-1}(k)}{2}} e^{\frac{L_{2p}(k)}{2}}, \quad (19)$$

$$P[x(k) = -\tilde{c}_m] = \beta_k\ \mu_{k,p}(\tilde{c}_m)\ e^{-\frac{L_{2p-1}(k)}{2}} e^{-\frac{L_{2p}(k)}{2}}, \quad (20)$$

$$P[x(k) = -\tilde{c}_m^*] = \beta_k\ \mu_{k,p}(\tilde{c}_m)\ e^{\frac{L_{2p-1}(k)}{2}} e^{-\frac{L_{2p}(k)}{2}}. \quad (21)$$

Plugging these probabilities back into (15) and recurring to the identity $e^x + e^{-x} = 2\cosh(x)$, it can be shown that:

$$\begin{aligned} D_{\boldsymbol{\alpha}}(k) = 2\beta_k \sum_{\tilde{c}_m \in \tilde{\mathcal{C}}_p} & \exp\left\{-\frac{S^2|\tilde{c}_m|^2}{2\sigma^2}\right\}\mu_{k,p}(\tilde{c}_m) \times \\ & \Bigg[\cosh\left(\frac{\Re\{\tilde{c}_m\ y^*(k) S_{\phi,\vartheta}\}}{\sigma^2} + \frac{L_{2p-1}(k)}{2} + \frac{L_{2p}(k)}{2}\right) \\ & + \cosh\left(\frac{\Re\{\tilde{c}_m^*\ y^*(k) S_{\phi,\vartheta}\}}{\sigma^2} - \frac{L_{2p-1}(k)}{2} + \frac{L_{2p}(k)}{2}\right)\Bigg]. \end{aligned} \quad (22)$$

Furthermore, using the relationship $\cosh(x) + \cosh(y) = 2\cosh(\frac{x+y}{2})\cosh(\frac{x-y}{2})$ along with the two identities $\tilde{c}_m + \tilde{c}_m^* =$

$2\Re\{\tilde{c}_m\}$ and $\tilde{c}_m - \tilde{c}_m^* = 2j\Im\{\tilde{c}_m\}$, (22) is rewritten as follows:

$$D_{\boldsymbol{\alpha}}(k) = 4\beta_k \sum_{\tilde{c}_m \in \tilde{\mathcal{C}}_p} \Bigg[\exp\left\{-\frac{S^2|\tilde{c}_m|^2}{2\sigma^2}\right\}\mu_{k,p}(\tilde{c}_m)\times \cosh\left(\frac{S\,\Re\{\tilde{c}_m\}\Re\left\{y^*(k)e^{j(2\pi k\vartheta+\phi)}\right\}}{\sigma^2}+\frac{L_{2p}(k)}{2}\right)\times \cosh\left(\frac{S\,\Im\{\tilde{c}_m\}\Im\left\{y^*(k)e^{j(2\pi k\vartheta+\phi)}\right\}}{\sigma^2}-\frac{L_{2p-1}(k)}{2}\right)\Bigg]. \quad (23)$$

Recalling that $\tilde{\mathcal{C}}_p = \{(2i-1)d_p + j(2n-1)d_p\}_{i,n=1}^{2^{p-1}}$, the sum over $\tilde{c}_m \in \tilde{\mathcal{C}}_p$ in (23) can be written as a double sum over the counters i and n after replacing $\tilde{c}_m$ by $(2i-1)d_p + j(2n-1)d_p$. Therefore, in order to factorize $D_{\boldsymbol{\alpha}}(k)$, the term $\mu_{k,p}(\tilde{c}_m) = \mu_{k,p}\big([2i-1]d_p + j[2n-1]d_p\big)$ must be factorized into two terms, one depending only on i and the other only on n. Here, we are actually dealing with the first $2p-2$ MSBs, $\bar{b}_1^m\bar{b}_2^m\bar{b}_3^m\cdots\bar{b}_{2p-3}^m\bar{b}_{2p-2}^m$. This is because $\bar{b}_{2p-1}^m$ and $\bar{b}_{2p}^m$ are not involved in $\mu_k(\tilde{c}_m)$ and therefore they will be henceforth denoted as "$\times\times$". Furthermore, it will shortly prove very useful to represent the first $2p-4$ MSBs by the shorthand notation $\bar{\boldsymbol{b}}_p^m$, i.e., $\bar{\boldsymbol{b}}_p^m \triangleq \bar{b}_1^m\bar{b}_2^m\cdots\bar{b}_l^m\cdots\bar{b}_{2p-5}^m\bar{b}_{2p-4}^m$. Since $\tilde{c}_m = (2i-1)d_p + j(2n-1)d_p$, we will also index the bit sequence associated to $\tilde{c}_m$ by (i,n) instead of m, i.e., $\tilde{c}_m \longleftrightarrow \bar{\boldsymbol{b}}_p^{(i,n)}\bar{b}_{2p-3}^{(i,n)}\bar{b}_{2p-2}^{(i,n)}\times\times$. Now, each symbol $\tilde{c}_m$ in $\tilde{\mathcal{C}}_p$ which has current coordinates $\big([2i-1]d_p\ ,[2n-1]d_p\big)$ in the Cartesian coordinate system (CCS) of the 2^{2p}-QAM constellation already has some other old coordinates, $\big([2i'-1]d_p\ ,[2n'-1]d_p\big)$ (in the CCS of the original $2^{2(p-1)}$-QAM) associated with a symbol $c_{m'} = (2i'-1)d_p + j(2n'-1)d_p$ in $\mathcal{C}_{p-1}$ with $c_{m'} \longleftrightarrow \bar{\boldsymbol{b}}_p^{(i,n)}\bar{b}_{2p-3}^{(i,n)}\bar{b}_{2p-2}^{(i,n)}$. Moreover, $c_{m'}$ can be expressed in terms of (i,n) as follows:

$$c_{m'} \;=\; (2i-1-2^{p-1})d_p \;+\; j(2n-1-2^{p-1})d_p. \quad (24)$$

On the other hand, we recall the same decomposition $\mathcal{C}_{p-1} = \tilde{\mathcal{C}}_{p-1} \cup (-\tilde{\mathcal{C}}_{p-1}) \cup \tilde{\mathcal{C}}_{p-1}^* \cup (-\tilde{\mathcal{C}}_{p-1}^*)$ for the original $2^{2(p-1)}$-QAM constellation. Then, for some $\tilde{c}_{m'} \in \tilde{\mathcal{C}}_{p-1}$, we have $c_{m'} \in \{\tilde{c}_{m'}, -\tilde{c}_{m'}, \tilde{c}_{m'}^*, -\tilde{c}_{m'}^*\}$. In turn, the symbols $c_{m'}$ themselves are obtained from a previous Gray-coded $2^{2(p-2)}$-QAM constellation by applying the same recursive procedure. Therefore, due to the symmetries of "*step 2*", it follows that $\tilde{c}_{m'}$, $-\tilde{c}_{m'}$, $\tilde{c}_{m'}^*$, and $-\tilde{c}_{m'}^*$ have the same $2p-4$ MSBs (which are represented by $\bar{\boldsymbol{b}}_p^{(i,n)}$). Consequently, according to the definition in (16), we have

$$\mu_{k,p-1}(\tilde{c}_{m'}) = \prod_{l=1}^{2(p-1)-2} e^{(2\bar{b}_l^{(i,n)}-1)\frac{L_l(k)}{2}}, \qquad \forall\ \tilde{c}_{m'} \in \tilde{\mathcal{C}}_{p-1}$$

thereby yielding the following recursive property:

$$\mu_{k,p}(\tilde{c}_m) = \mu_{k,p-1}(\tilde{c}_{m'})\exp\left\{(2\bar{b}_{2p-3}^{(i,n)}-1)L_{2p-3}(k)/2\right\}\times \exp\left\{(2\bar{b}_{2p-2}^{(i,n)}-1)L_{2p-2}(k)/2\right\}. \quad (25)$$

Therefore, one needs to express the bits $\bar{b}_{2p-3}^{(i,n)}$ and $\bar{b}_{2p-2}^{(i,n)}$ explicitly as one function of i or n only and vice-versa, respectively, if $\mu_{k,p}(\tilde{c}_m)$ is to be factorized in terms of these two counters separately. Using $\lfloor x\rfloor$ to denote the floor function which returns the largest integer which is smaller than or equal to x, the following lemma finds this useful decomposition:

Lemma 1: $\forall\ i,n = 1,2,\cdots,2^{p-1}$, the two bits $\bar{b}_{2p-2}^{(i,n)}$ and $\bar{b}_{2p-3}^{(i,n)}$ are expressed as:

$$\bar{b}_{2p-2}^{(i,n)} = \left\lfloor\frac{i-1}{2^{p-2}}\right\rfloor \qquad \text{and} \qquad \bar{b}_{2p-3}^{(i,n)} = \left\lfloor\frac{n-1}{2^{p-2}}\right\rfloor. \quad (26)$$

Proof: See Appendix A of [25].

By revisiting (25) and considering the recursive construction of $\tilde{\mathcal{C}}_{p-1}$ from the $2^{2(p-2)}$-QAM constellation and following the same reasoning from (24) through (25), one can express $\mu_{k,p-1}(\tilde{c}_{m'})$ itself in the same recursive form of (25). We capitalize on this observation along with the result in (24) to show, by mathematical induction, the following decomposition:

$$\mu_{k,p}(\tilde{c}_m) = \theta_{k,2p}(i)\theta_{k,2p-1}(n), \quad (27)$$

where $\theta_{k,2p}(i)$ and $\theta_{k,2p-1}(n)$ can be computed recursively, for any $p \geq 2$ as follows:

$$\theta_{k,2p}(i) \;=\; \theta_{k,2p-2}\left(\frac{|2i-1-2^{p-1}|+1}{2}\right)\times \exp\left\{\left(2\left\lfloor\frac{i-1}{2^{p-2}}\right\rfloor-1\right)\frac{L_{2p-2}(k)}{2}\right\}, \quad (28)$$

$$\theta_{k,2p-1}(n) \;=\; \theta_{k,2p-3}\left(\frac{|2n-1-2^{p-1}|+1}{2}\right)\times \exp\left\{\left(2\left\lfloor\frac{n-1}{2^{p-2}}\right\rfloor-1\right)\frac{L_{2p-3}(k)}{2}\right\}, \quad (29)$$

with the initialization $\theta_{k,2}(1)=\theta_{k,1}(1)=1$ since we have extended the definition of $\mu_{k,p}(.)$ for $p=1$ (i.e., QPSK constellations) to be $\mu_{k,1}(c_m) = 1\ \forall\ c_m \in \mathcal{C}_1$. Plugging (27) in (23) and using the fact that $\tilde{\mathcal{C}}_p = \{(2i-1)d_p + j(2n-1)d_p\}_{i,n=1,2,\cdots,2^{p-1}}$, the term $D_{\boldsymbol{\alpha}}(k)$ is rewritten as follows:

$$D_{\boldsymbol{\alpha}}(k) \;=\; 4\beta_k\sum_{i=1}^{2^{p-1}}\sum_{n=1}^{2^{p-1}}\Bigg[\exp\left\{-\frac{S^2((2i-1)^2+(2n-1)^2)d_p^2}{2\sigma^2}\right\} \theta_{k,2p}(i)\cosh\left(\frac{S(2i-1)d_pu(k)}{\sigma^2}+\frac{L_{2p}(k)}{2}\right)\times \theta_{k,2p-1}(n)\cosh\left(\frac{S(2n-1)d_pv(k)}{\sigma^2}-\frac{L_{2p-1}(k)}{2}\right)\Bigg], \quad (30)$$

where $u(k)$ and $v(k)$ are defined as $u(k) = \Re\{y^*(k)e^{j(2\pi k\vartheta+\phi)}\}$ and $v(k) = \Im\{y^*(k)e^{j(2\pi k\vartheta+\phi)}\}$. Finally, splitting the two sums in (30), it can be shown that $D_{\boldsymbol{\alpha}}(k)$ factorizes as follows:

$$D_{\boldsymbol{\alpha}}(k) = 4\beta_k\ F_{2p,\boldsymbol{\alpha}}(u(k)) \times F_{2p-1,\boldsymbol{\alpha}}(v(k)), \quad (31)$$

where, by defining $\eta_{k,q}(i) = \theta_{k,q}(i)e^{-(2i-1)^2d_p^2\rho}$, the function $F_{q,\boldsymbol{\alpha}}(.)$ is given by:

$$F_{q,\boldsymbol{\alpha}}(x) \;\triangleq\; \sum_{i=1}^{2^{p-1}}\eta_{k,q}(i)\cosh\left(\frac{(2i-1)d_pSx}{\sigma^2}+\frac{(-1)^qL_q(k)}{2}\right),$$

and where, depending on the context, the counter q is used from now on to refer to $2p$ or $2p-1$. Finally, by injecting (31) into (12) and dropping the constant terms, the *useful* LLF for square-QAM constellations is linearized as follows:

$$L_{\boldsymbol{y}}(\boldsymbol{\alpha}) = \sum_{k=k_0}^{k_0+K-1}\ln\big(F_{2p,\boldsymbol{\alpha}}(u(k))\big) + \sum_{k=k_0}^{k_0+K-1}\ln\big(F_{2p-1,\boldsymbol{\alpha}}(v(k))\big), \quad (32)$$

involving thereby the sum of two analogous terms. Further, substituting (31) in (12) and using the fact that $I(k)^2 + Q(k)^2 = u(k)^2 + v(k)^2$, it can be shown that:

$$p[y(k);\boldsymbol{\alpha}] \;=\; p[u(k),v(k);\boldsymbol{\alpha}] = p[u(k);\boldsymbol{\alpha}]p[v(k);\boldsymbol{\alpha}], \quad (33)$$

where

$$p[u(k);\boldsymbol{\alpha}] = \frac{2\beta_{k,2p}}{\sqrt{2\pi\sigma^2}} \exp\left\{-\frac{u(k)^2}{2\sigma^2}\right\} F_{2p,\boldsymbol{\alpha}}(u(k)), \tag{34}$$

$$p[v(k);\boldsymbol{\alpha}] = \frac{2\beta_{k,2p-1}}{\sqrt{2\pi\sigma^2}} \exp\left\{-\frac{v(k)^2}{2\sigma^2}\right\} F_{2p-1,\boldsymbol{\alpha}}(v(k)), \tag{35}$$

with

$$\beta_{k,2p} = \prod_{l=1}^{p} \frac{1}{2\cosh\left(\frac{L_{2l}(k)}{2}\right)},\ \beta_{k,2p-1} = \prod_{l=2}^{p} \frac{1}{2\cosh\left(\frac{L_{2l-1}(k)}{2}\right)}.$$

This means that the two random variables (RVs), $u(k)$ and $v(k)$ are independent and *almost* identically distributed (i.e., their pdfs have the same structure, but are parameterized differently). These properties will prove extremely useful to the derivation of the different FIM elements in the next section.

IV. Derivation of the Closed-Form Expressions for the CRLBs

Our starting point is the expression for the FIM elements defined in (3). We will detail the derivation of the first diagonal FIM entry only since similar steps allow the derivation of the other ones. In fact, by defining $\gamma_{k,2p}(\rho) \triangleq \mathrm{E}\left\{\partial^2 \ln\left(F_{2p,\boldsymbol{\alpha}}\big(u(k)\big)\right)/\partial\phi^2\right\}$ and $\gamma_{k,2p-1}(\rho) \triangleq \mathrm{E}\left\{\partial^2 \ln\left(F_{2p-1,\boldsymbol{\alpha}}\big(v(k)\big)\right)/\partial\phi^2\right\}$, it can be readily shown using (3) and (32) that:

$$\left[\boldsymbol{I}(\boldsymbol{\alpha})\right]_{1,1} = \textstyle\sum_{k=k_0}^{k_0+K-1} \left[\gamma_{k,2p}(\rho) + \gamma_{k,2p-1}(\rho)\right]. \tag{36}$$

Due to the apparent symmetries between the pdfs of $u(k)$ and $v(k)$ in (34) and (35), we will derive the term $\gamma_{k,2p}(\rho)$ only and its equivalent term $\gamma_{k,2p-1}(\rho)$ can be easily deduced, at the very end, by simple identification. To do so, we establish the first and second derivatives of $F_{2p,\boldsymbol{\alpha}}(x)$ with respect to the working variable x as follows:

$$F'_{2p,\boldsymbol{\alpha}}(x) = \frac{Sd_p}{\sigma^2}\sum_{i=1}^{2^{p-1}}(2i-1)\eta_{k,2p}(i)\sinh\!\left(\frac{(2i-1)d_pSx}{\sigma^2}+\frac{L_{2p}(k)}{2}\right),$$

$$F''_{2p,\boldsymbol{\alpha}}(x) = \frac{S^2d_p^2}{\sigma^4}\sum_{i=1}^{2^{p-1}}(2i-1)^2\eta_{k,2p}(i)\cosh\!\left(\frac{(2i-1)d_pSx}{\sigma^2}+\frac{L_{2p}(k)}{2}\right).$$

Moreover, by recalling the expressions of $u(k)$ and $v(k)$ given after (30), we readily have:

$$u'(k) \triangleq \frac{\partial u(k)}{\partial\phi} = -v(k) \qquad \text{and} \qquad v'(k) \triangleq \frac{\partial v(k)}{\partial\phi} = u(k),$$

from which we obtain $u''(k) = -u(k)$. Using this result, and after some algebraic manipulations, it can be shown that:

$$\frac{\partial^2 \ln\left(F_{2p,\boldsymbol{\alpha}}\big(u(k)\big)\right)}{\partial\phi^2} = -u(k)\frac{F'_{2p,\boldsymbol{\alpha}}\big(u(k)\big)}{F_{2p,\boldsymbol{\alpha}}\big(u(k)\big)} + v(k)^2\left[\frac{F''_{2p,\boldsymbol{\alpha}}\big(u(k)\big)}{F_{2p,\boldsymbol{\alpha}}\big(u(k)\big)} - \left(\frac{F'_{2p,\boldsymbol{\alpha}}\big(u(k)\big)}{F_{2p,\boldsymbol{\alpha}}\big(u(k)\big)}\right)^2\right].$$

Then, since $u(k)$ and $v(k)$ are independent RVs, it follows that:

$$\gamma_{k,2p} = -\mathrm{E}\left\{u(k)\frac{F'_{2p,\boldsymbol{\alpha}}\big(u(k)\big)}{F_{2p,\boldsymbol{\alpha}}\big(u(k)\big)}\right\} + \mathrm{E}\left\{v(k)^2\right\} \times \left[\mathrm{E}\left\{\frac{F''_{2p,\boldsymbol{\alpha}}\big(u(k)\big)}{F_{2p,\boldsymbol{\alpha}}\big(u(k)\big)}\right\} - \mathrm{E}\left\{\left(\frac{F'_{2p,\boldsymbol{\alpha}}\big(u(k)\big)}{F_{2p,\boldsymbol{\alpha}}\big(u(k)\big)}\right)^2\right\}\right]. \tag{37}$$

Since the pdfs of these two RVs were already established in (34) and (35), the expectations involved above can be expressed in closed form. For instance, by integration over the pdf of $v(k)$, it follows that:

$$\mathrm{E}\left\{v(k)^2\right\} = \int_{-\infty}^{\infty} v(k)^2 p[v(k);\boldsymbol{\alpha}]\mathrm{d}v(k) = \frac{2\beta_{k,2p-1}}{\sqrt{2\pi\sigma^2}}\int_{-\infty}^{\infty} v(k)F_{2p-1,\boldsymbol{\alpha}}(v(k))e^{-v(k)^2/2\sigma^2}\mathrm{d}v(k).$$

After expanding the expression of $F_{2p-1}(x)$ in (32) using the identity $\cosh(x+y) = \sinh(x)\sinh(y) + \cos(x)\cos(x)$, inverting the sum and integral signs and then resorting to some algebraic manipulations, it can be shown that $A \triangleq \mathrm{E}\left\{v(k)^2\right\}$ is given by:

$$A = \sigma^2\!\left[\rho\ \omega_{k,2p-1} + 2\beta_{k,2p-1}\cosh\!\left(\frac{L_{2p-1}(k)}{2}\right)\sum_{n=1}^{2^{p-1}}\theta_{k,2p-1}(n)\right], \tag{38}$$

in which $\omega_{k,2p-1}$ along with $\omega_{k,2p}$ (that will appear shortly) are common coefficients to all the FIM elements defined as:

$$\omega_{k,q} \triangleq d_p^2\ \beta_{k,q}\cosh\left(L_q(k)/2\right)\textstyle\sum_{i=1}^{2^{p-1}}(2i-1)^2\theta_{k,q}(i), \tag{39}$$

where q is either $2p$ or $2p-1$. We further simplify (38) by showing via mathematical induction the following identity:

$$2\beta_{k,2p-1}\cosh\left(L_{2p-1}(k)/2\right)\textstyle\sum_{n=1}^{2^{p-1}}\theta_{k,2p-1}(n) = 1. \tag{40}$$

In fact, by plugging (40) in (38), it follows that:

$$\mathrm{E}\left\{v(k)^2\right\} = \sigma^2\left[1 + \rho\ \omega_{k,2p-1}\right]. \tag{41}$$

The closed-form expressions for the other expectations involved in (37) are obtained by integrating over the pdf of $u(k)$:

$$\mathrm{E}\left\{u(k)\frac{F'_{2p,\boldsymbol{\alpha}}\big(u(k)\big)}{F_{2p,\boldsymbol{\alpha}}\big(u(k)\big)}\right\} = \rho\ \omega_{k,2p}, \tag{42}$$

$$\mathrm{E}\left\{\frac{F''_{2p,\boldsymbol{\alpha}}\big(u(k)\big)}{F_{2p,\boldsymbol{\alpha}}\big(u(k)\big)}\right\} = \frac{\omega_{k,2p}}{\sigma^2}\rho, \tag{43}$$

$$\mathrm{E}\left\{\left(\frac{F'_{2p,\boldsymbol{\alpha}}\big(u(k)\big)}{F_{2p,\boldsymbol{\alpha}}\big(u(k)\big)}\right)^2\right\} = \frac{4\ d_p^2\ \beta_{k,2p}}{\sigma^2}\rho\Psi_{k,2p}(\rho), \tag{44}$$

where $\Psi_{k,2p}(.)$ in the last equality is given by:

$$\Psi_{k,2p}(\rho) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{+\infty}\frac{\lambda_{k,2p}^2(t,\rho)}{\delta_{k,2p}(t,\rho)}\ e^{-\frac{t^2}{2}}dt, \tag{45}$$

with

$$\lambda_{k,2p}(t,\rho) = \sum_{i=1}^{2^{p-1}}(2i-1)\eta_{k,2p}(i)\sinh\!\left(\sqrt{2\rho}(2i-1)d_pt + \frac{L_{2p}(k)}{2}\right),$$

$$\delta_{k,2p}(t,\rho) = \textstyle\sum_{i=1}^{2^{p-1}}\eta_{k,2p}(i)\cosh\left(\sqrt{2\rho}(2i-1)d_pt + L_{2p}(k)/2\right).$$

Therefore, by injecting the four expectations evaluated in (41) to (44) back into (37), the first term in (36) earlier denoted as $\gamma_{k,2p}(\rho) \triangleq \mathrm{E}\left\{\partial^2 \ln\left(F_{2p,\boldsymbol{\alpha}}\big(u(k)\big)\right)/\partial\phi^2\right\}$ is obtained as follows:

$$\gamma_{k,2p}(\rho) = \omega_{k,2p-1}\rho\left[\omega_{k,2p}\rho - 4d_p^2\beta_{k,2p}\Psi_{2p}(\rho)\left(\frac{1}{\omega_{k,2p-1}}+\rho\right)\right]. \tag{46}$$

As mentioned previously, the expression of the second term, $\gamma_{k,2p-1}(\rho) \triangleq \mathrm{E}\left\{\partial^2 \ln\left(F_{2p-1,\boldsymbol{\alpha}}\big(v(k)\big)\right)/\partial\phi^2\right\}$, involved in (36) can be easily deduced from the expression of $\gamma_{k,2p}(\rho)$ in (46). This is due to the apparent symmetries in the pdfs of the two RVs $u(k)$ and $v(k)$, as seen from (34) and (35), leading to:

$$\gamma_{k,2p-1}(\rho) = \omega_{k,2p}\rho\left[\omega_{k,2p-1}\rho - 4d_p^2\beta_{k,2p-1}\Psi_{2p-1}(\rho)\left(\frac{1}{\omega_{k,2p}}+\rho\right)\right].$$

The first FIM diagonal element is obtained by injecting $\gamma_{k,2p}(\rho)$ and $\gamma_{k,2p-1}(\rho)$ back into (36). After deriving the other elements using equivalent manipulations[4] and defining $\Omega_{p,k}(\rho) \triangleq -\gamma_{k,2p}(\rho) - \gamma_{k,2p-1}(\rho)$, we obtain an analytical expression for the FIM in CA estimation as follows:

$$\boldsymbol{I}(\boldsymbol{\alpha}) = \sum_{k=k_0}^{k_0+K-1} \Omega_{p,k}(\rho)\begin{pmatrix} 1 & 2\pi k \\ 2\pi k & (2\pi)^2 k^2 \end{pmatrix} = \sum_{k=k_0}^{k_0+K-1} \boldsymbol{I}_k(\boldsymbol{\alpha}), \quad (47)$$

where $\boldsymbol{I}_k(\boldsymbol{\alpha})$ is the FIM pertaining to the k^{th} received sample. Now, the obtained general FIM expression (47), in CA estimation, encloses the two traditional (extreme) scenarios of *completely NDA* and *completely DA* estimations as special cases. Indeed, in the former case, no *a priori* information about the bits is available at the receiver end and, therefore, $Pr[b_l^k = 1] = Pr[b_l^k = 0] = 1/2$ thereby yielding $L_l^{\text{NDA}}(k) = 0$ for all l and k. In the latter case, however, the bits are *a priori* perfectly known and therefore, at the receiver side, we have either $\{Pr[b_l^k = 1] = 1$ hence $Pr[b_l^k = 0] = 0\}$ or $\{Pr[b_l^k = 0] = 1$ hence $Pr[b_l^k = 1] = 0\}$ and consequently the LLRs verify $L_l^{\text{DA}}(k) = \pm\infty$. By injecting these two typical values, $L_l^{\text{NDA}}(k)$ and $L_l^{\text{DA}}(k)$, in all the quantities that are involved in the entries of $\boldsymbol{I}_k(\boldsymbol{\alpha})$ and by recurring to some easy simplifications, one obtains exactly the same expressions for the FIMs developed earlier in [15] and [28] in the traditional NDA and DA cases, respectively.

The CRLBs for the phase shift and the CFO are, respectively, the first and second diagonal elements of the FIM inverse $\boldsymbol{I}^{-1}(\boldsymbol{\alpha})$. As such, they depend on the first time index k_0 as seen from (47). Such dependencies on the observation window have previously been reported in the literature even in the NDA case [14-15]. In CA estimation as well, we obtain different loose (or excessively optimistic) bounds as k_0 varies. Our interest is focused on the tightest bound which is obtained when the square of the off-diagonal elements is negligible compared to the product of the diagonal ones:

$$0 \leq [\boldsymbol{I}(\boldsymbol{\alpha})]_{1,2}^2 \ll [\boldsymbol{I}(\boldsymbol{\alpha})]_{1,1}[I(\boldsymbol{\alpha})]_{2,2}. \quad (48)$$

We verify by computer simulations that the off-diagonal entries are almost equal to zero when the set of sampling indices is centred around zero, i.e., $k_0 = -\frac{K-1}{2}$. In this case, the CRLBs' expressions greatly simplify to:

$$\text{CRLB}_{\text{CA}}(\nu) = \frac{-1}{(2\pi)^2}\left(\sum_{k=-\frac{K-1}{2}}^{\frac{K-1}{2}} \Omega_{p,k}(\rho)k^2\right)^{-1} \quad (49)$$

$$\text{CRLB}_{\text{CA}}(\phi) = \left(-\sum_{k=\frac{K-1}{2}}^{\frac{K-1}{2}} \Omega_{p,k}(\rho)\right)^{-1}. \quad (50)$$

V. Simulation Results

In this section, we provide graphical representations for the analytical CRLBs in (49) and (50) for the joint estimation of the synchronization parameters, with different modulation orders and different coding rates. The encoder is composed of two identical RSCs of generator polynomials (1,0,1,1) and (1,1,0,1), with systematic rate $R_0 = \frac{1}{2}$ each. The output of the turbo encoder is punctured in order to achieve the desired code rate R. For the tailing bits, the size of the RSC encoders memory is fixed to 4. In order to evaluate the obtained CA CRLBs, the extrinsic information delivered by the SISO decoder is used to evaluate the bit LLRs, $L_l(k)$. Note that having the LLRs at hand, it is possible to evaluate all the quantities involved in the expressions of the considered bounds. Indeed, as pointed out in [6, 26, 27] (and references therein) and owing to the turbo principle, the extrinsic information accurately approximates the bit's a priori probabilities.

In Fig. 2, we begin by verifying that the new closed-form CRLBs coincide with their *empirical* counterparts obtained earlier in [23, 24]. This means that the new analytical expressions corroborate these previous attempts to evaluate the considered bounds, *empirically*, and they allow their immediate evaluation for any square-QAM turbo-coded signal.

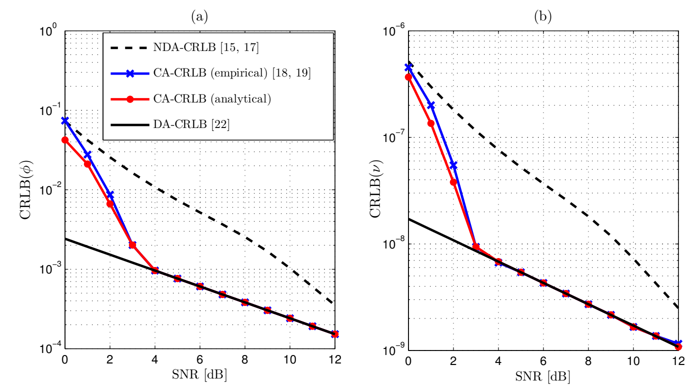

Fig. 2. NDA, DA, and CA (analytical and empirical) estimation CRLBs for: (a) the phase shift, and (b) the CFO (16-QAM; $K = 207$).

As expected, we also see from the same figure that the CA CRLBs are smaller than the NDA CRLBs which were earlier introduced in [13, 15]. This highlights the performance improvements that can be achieved by a coded system over an uncoded one. For example, at SNR = 4 dB, the CA CRLBs are about up to 10 times smaller than the NDA CRLBs. This figure underlines the huge potential performance gain that could be achieved at such low SNR level. Additionally and most prominently, the CA CRLBs decrease rapidly and reach the ideal DA bounds obtained by assuming all the transmitted symbols to be perfectly known to the receiver, and which are simply given by [28]:

$$\text{CRLB}_{\text{DA}}(\nu) = \frac{6}{(2\pi)^2 K(K^2-1)\rho}, \qquad \text{CRLB}_{\text{DA}}(\phi) = \frac{1}{2K\rho}.$$

In Fig. 3, we plot the CA CRLBs for different modulation orders. It is clear that the CRLBs increase with the modulation order at a given SNR value. This is a typical behavior that was observed for NDA CRLBs, as well, and actually for any parameter estimation problem involving linearly-modulated signals. Indeed, when the modulation order increases, the intersymbol distance decreases for normalized-energy constellations. As such, at the same SNR level, noise components have a relatively worse impact on symbol detection and parameter estimation in general. Furthermore, even in probability theory, when the ambient sample space of the *nuisance* parameters (here the constellation alphabet) gets larger, more uncertainty is introduced about each transmitted symbol thereby rendering estimation more difficult. Another interesting observation which can be drawn from Fig. 3 is that the CRLB for the frequency is much smaller than that for the phase. This is simply because the received signal depends much more on ν than on ϕ through the time index k in the argument of $e^{j(2\pi\nu k+\phi)}$. In other words, the received samples carry more information on the frequency than on the phase.

In Fig. 4, we show the effect of the coding rate on the synchronization performance. In fact, we plot the CA CRLBs for two different coding rates $R_1 = 0.3285 \approx \frac{1}{3}$ and $R_2 = 0.4892 \approx \frac{1}{2}$. Even though both CA CRLBs coincide at moderate SNRs, they exhibit a significant gap at lower SNR levels. In fact, with smaller

[4]Details were omitted due to lack of space.

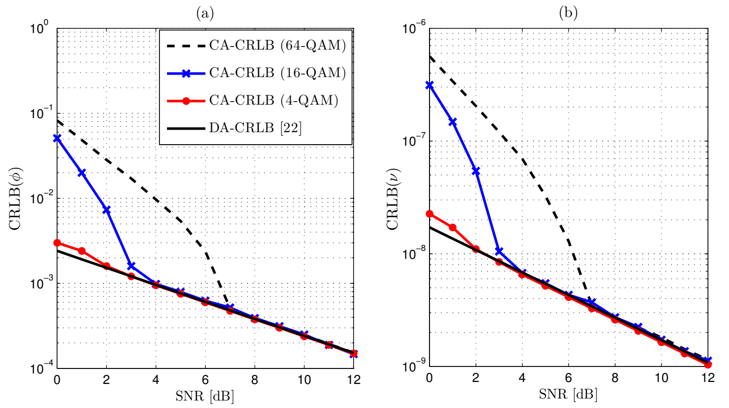

Fig. 3. CA estimation CRLBs (analytical) for: (a) the phase shift, and (b) the CFO (4-, 16-, and 64-QAM; $K = 207$).

coding rates, more redundancy is provided by the turbo encoder. Consequently, the decoder is more likely able to correctly detect the transmitted bits enhancing thereby the estimation performance.

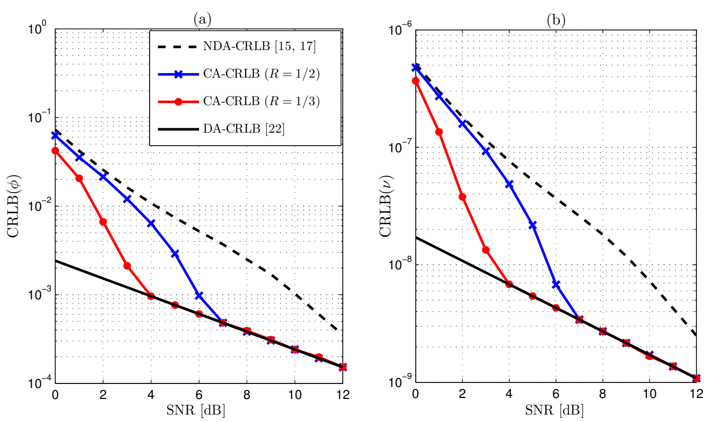

Fig. 4. CA estimation CRLBs (analytical) for: (a) the phase shift, and (b) the CFO, with two different rates (16-QAM, and $K = 207$).

VI. Conclusion

In this paper, we derived for the very first time analytical expressions for the CRLBs of joint CFO and carrier phase estimation from turbo-coded square-QAM transmissions. Our new analytical bounds coincide with their empirical counterparts earlier computed in [23, 24]. They are also remarkably smaller than the NDA CRLBs thereby suggesting enhanced synchronization capabilities if the *soft* information provided by the turbo decoder is exploited during the estimation process. Moreover, the CA CRLBs decay rapidly with the SNR and reach the DA CRLB at relatively low thresholds where all the transmitted symbols are assumed to be perfectly known. The effect of the coding rate is also more apparent in the low SNR regime where more redundancy implies more accurate decoding and therefore better synchronization.

References

[1] C. Berrou and A. Glavieux, "Near optimum error correcting coding and decoding: turbo codes," *IEEE Trans. Commun.,* vol. 44, no. 10, pp. 1261-1271, Oct. 1996.

[2] C. So-In, R. Jain, A. Al Tamimi, "Scheduling in IEEE 802.16e WiMAX Networks: Key Issues and a Survey," IEEE Journal on Select. Areas in Commun., vol. 27, no. 2, pp. 156-171, Feb. 2009,

[3] 3GPP TS 36.211: 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation.

[4] C. Herzet, N. Noels, V. Lottici, H. Wymeersch, M. Luise, M. Moeneclaey, and L. Vandendorpe "Code-aided turbo synchronization," in *Proc. of the IEEE,* vol. 95, no. 6, pp. 1255-1271, June 2007.

[5] V. Lottici and M. Luise, "Embedding carrier phase recovery into iterative decoding of turbo-coded linear modulations," *IEEE Trans. Commun.,* vol. 52, no. 4, pp. 661-669, Apr. 2004.

[6] K. Choi "Residual frequency offset compensation-embedded turbo decoder," *IEEE Trans. Veh. Technol.,* vol. 57, no. 5, pp. 3211-3217, May 2008.

[7] C. Morlet, I. Buret, and M.L. Boucheret, "A carrier phase estimator for multi-media satellite payloads suited to RSC coding schemes," in *Proc. IEEE Int. Conf. Commun. (ICC),* vol. 1, New Orleans, LA, June 2000, pp. 455-459.

[8] C. Langlais and M. Helard, "Phase carrier recovery for turbo codes over a satellite link with the help of tentative decisions," in *Proc. 2nd Int. Symp. Turbo Codes & Related Topics,* vol. 5, Sept. 2000, pp. 439-442.

[9] S. Cioni , G. E. Corazza, and A. Vanelli-Coralli "Turbo embedded estimation with imperfect phase/frequency recovery," in *Proc. IEEE Int. Conf. Commun.,* Anchorage, AK, Jun. 2003, pp. 2385-2389.

[10] W. Oh and K. Cheun, "Joint decoding and carrier phase recovery algorithm for turbo codes," *IEEE Commun. Lett.,* vol. 5, pp. 375-377, Sept. 2001.

[11] X. Wu, Y. Song, C. Zhao, and X. You: "Progressive frequency offset compensation in turbo receivers," *IEEE Trans. Wirel. Commun.,* vol. 10, no. 2, pp. 702-709, Fev. 2011.

[12] S. M. Kay, *Fundamentals of statistical signal processing, vol. 1: Estimation theory*. Englewood Cliffs, NJ: Prentice-Hall, 1998.

[13] B. Cowley, F. Rice, and M. Rice, "Cramér-Rao lower bound for QAM phase and frequency estimation," *IEEE Trans. Commun.,* vol. 49, no. 9, pp. 689-693, Sept. 2001.

[14] J. P. Delmas "Closed form-expressions of the exact Cramér-Rao bound for parameter estimation of BPSK, MSK, or QPSK waveforms," *IEEE Signal Process. Lett.*, vol. 15, pp. 405-408., 2008

[15] F. Bellili, N. Atitallah, S. Affes, and A. Stéphenne, "Cramér-Rao lower bounds for frequency and phase NDA estimation from arbitrary square QAM-modulated signals," *IEEE Trans. Signal Process.,* vol. 58, no. 9, pp. 4517-4525, Sept. 2010.

[16] F. Bellili, N. Atitallah, S. Affes, and A. Stéphenne, "Closed-form expressions for the exact Cramer-Rao bound for parameter estimation of arbitrary square QAM-modulated signals," in *Proc. IEEE Globecom,* Honolulu, HI, Nov./Dec. 2009.

[17] F. Bellili , A. Stéphenne, and S. Affes, "Cramér-Rao lower bounds for NDA SNR estimates of square QAM modulated transmissions," *IEEE Trans. Commun.,* vol. 58, no. 11, pp. 3211-3218, Nov. 2010.

[18] F. Bellili, A. Stéphenne, and S. Affes, "Cramér-Rao bounds for NDA SNR estimates of square QAM modulated signals," presented at the IEEE WCNC, Budapest, Hungary, Apr. 2009.

[19] A. Masmoudi, F. Bellili, S. Affes, and A. Stéphenne, "Closed-form expressions for the exact Cramér-Rao bounds of timing tecovery estimators from BPSK, MSK and square-QAM transmissions," *IEEE Trans. Signal Process.*, vol. 59, pp. 2474-2484, Jan. 2011.

[20] A. Masmoudi, F. Bellili, S. Affes, and A. Stephenne, "Closed-form expressions for the exact Cramér-Rao bounds of timing recovery estimators from BPSK and square-QAM transmissions," in *Proc. Int. Conf. on Commun.*, Kyoto, Japan, June 2011, pp. 1-6.

[21] F. Bellili, S. B. Hassen, S. Affes, and A. Stephenne, "Cramer-Rao lower bounds of DOA estimates from square QAM-modulated signals," *IEEE Trans. Signal Process.*, vol. 59, pp. 1675-1685, June 2011.

[22] F. Bellili, S. Ben Hassen, S. Affes, and A. Stéhpenne, "Cramér-Rao bound for NDA DOA estimates of square QAM-modulated signals," in*Proc. IEEE GLOBECOM,* Honolulu, HI, Nov/Dec. 2009.

[23] N. Noels, H. Steendam, and M. Moeneclaey, "Carrier and clock recovery in (turbo) coded systems: Cramér-Rao bound and synchronizer performance," *EURASIP Journal on App. Signal process., Special Issue on Turbo Processing,* vol 2005, no. 6, pp. 972-980, May 2005.

[24] N. Noels, H. Steendam, and M. Moeneclaey, "The Cramér-Rao bound for phase estimation from coded linearly modulated signals," *IEEE Commun. Lett.,* vol. 7, no. 5, pp. 207-209, May 2003.

[25] F. Bellili, A. Methenni, and S. Affes, "Closed-form CRLBs for CFO and phase estimation from Turbo coded square-QAM-modulated transmissions," submitted to *IEEE Trans on Wireless Commun.*, Jan. 2014, revised, June 2014, accepted for publication, Aug. 2014, pending mninor revisions, to appear.

[26] G. Colavolpe, G. Ferrari, and R. Raheli, "Extrinsic information in iterative decoding: A unified view," *IEEE Trans. Commun.,* vol. 49, no. 12, pp. 2088-2094, Dec. 2001.

[27] Stéphane Y. Le Goff, B. K. Khoo, and C. C. Tsimenidis, "Constellation shaping for bandwidth-efficient turbo-coded modulation with iterative receiver," *IEEE Trans. Wireless Comm.,* vol. 6, no. 6, pp. 2223-2233, June 2007.

[28] A. N. D'Andrea, U. Mengali, and R. Reggiannini, "The modified Cramér-Rao bound and its application to synchronization parameters," *IEEE J. Select. Areas Commun.,* vol. 42, no. 2/3/4, pp. 1391-1399, Apr. 1994.

[29] F. Bellili, A. Methenni, and S. Affes, "Closed-Form CRLBs for SNR estimation from Turbo-coded BPSK-, MSK-, and square-QAM-modulated signals," *IEEE Trans. Signal Process.,* vol. 58, no. 15, pp. 4018-4033, Aug. 2014.