Digital Signal Processing 87 (2019) 60–74

Contents lists available at ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

M-estimator based Chinese Remainder Theorem with few remainders using a Kroenecker product based mapping vector

Jayme Milanezi Junior [a,b,c,*], João Paulo C.L. da Costa [a], Florian Römer [b,d], Ricardo K. Miranda [a], Marco A.M. Marinho [a], Giovanni Del Galdo [b,e]

[a] Department of Electrical Engineering, Universidade de Brasília, Brasília-DF, Brazil
[b] Institute for Information Technology, Technische Universität Ilmenau, Ilmenau, Germany
[c] Brazilian Electricity Regulatory Agency, ANEEL, Brasília-DF, Brazil
[d] Fraunhofer Institute for Nondestructive Testing IZFP, Saarbrücken, Germany
[e] Fraunhofer Institute for Integrated Circuits IIS, Erlangen, Germany

ARTICLE INFO

Article history:
Available online 29 January 2019

Keywords:
Chinese Remainder Theorem (CRT)
Remainder error bound
Tensorial products
M-estimation
Kroenecker product

ABSTRACT

The Chinese Remainder Theorem (CRT) explains how to estimate an integer-valued number from the knowledge of the remainders obtained by dividing such unknown integer by co-prime integers. As an algebraic theorem, CRT is the basis for several techniques concerning data processing. For instance, considering a single-tone signal whose frequency value is above the sampling rate, the respective peak in the DFT informs the impinging frequency value modulo the sampling rate. CRT is nevertheless sensitive to errors in the remainders, and many efforts have been developed in order to improve its robustness. In this paper, we propose a technique to estimate real-valued numbers by means of CRT, employing for this goal a Kroenecker based M-Estimation (ME), specially suitable for CRT systems with low number of remainders. Since ME schemes are in general computationally expensive, we propose a mapping vector obtained via Kroenecker products which considerably reduces the computational complexity. Furthermore, our proposed technique enhances the probability of estimating an unknown number accurately even when the errors in the remainders surpass 1/4 of the greatest common divisor of all moduli. We also provide a version of the mapping vectors based on tensorial n-mode products, delivering in the end the same information of the original method. Our approach outperforms the state-of-the-art CRT methods not only in terms of percentage of successful estimations but also in terms of smaller average error.

1. Introduction

The Chinese Remainder Theorem (CRT) explains how to solve an algebra problem in which an integer-valued N is determined from its remainders, as in

$$\begin{cases} N \bmod M_1 = r_1, \\ N \bmod M_2 = r_2, \\ \quad \vdots \quad \vdots \quad \vdots \\ N \bmod M_L = r_L, \end{cases} \tag{1}$$

where mod stands for the modulus operator, M is the greatest common divisor (GCD) of all moduli M_i, for $M_i \in \{M_1, M_2, \ldots, M_L\}$, and $M_i = M\Gamma_i$, where $\Gamma_1 < \Gamma_2 < \cdots < \Gamma_L$, are assumed relatively co-prime, i.e., for $i \neq j$, $\mathrm{GCD}(\Gamma_i, \Gamma_j) = 1$. This data model, where all possible pairs of moduli M_i have the same GCD, is also adopted in [1–5]. From a general standpoint, the theoretical interval in which the number N is uniquely determinable is the dynamic range $D = \mathrm{LCM}(M_1, M_2, \ldots, M_L)$, i.e., $0 \leq N < D$, where LCM denotes the least common multiple of a set of numbers [2,6].

The remainders are r_i, for $i \in \{1, 2, \ldots, L\}$. All remainders respect $0 \leq r_i < M_i$ for $i \in \{1, 2, \ldots, L\}$. Given any i-th row of (1), an equivalent expression is

$$n_i M_i + r_i = N, \tag{2}$$

where the n_i, for $i \in \{1, 2, \ldots, L\}$ are the folding integers, also unknown. From the knowledge of M_i and r_i, the CRT offers the

* Corresponding author at: Department of Electrical Engineering, Universidade de Brasília, Brasília-DF, Brazil.
E-mail addresses: jayme@aneel.gov.br (J. Milanezi Junior), joaopaulo.dacosta@ene.unb.br (J.P.C.L. da Costa), florian.roemer@tu-ilmenau.de (F. Römer), rickehrle@unb.br (R.K. Miranda), marco.marinho@ieee.org (M.A.M. Marinho), giovanni.delgaldo@iis.fraunhofer.de (G. Del Galdo).

https://doi.org/10.1016/j.dsp.2019.01.009
1051-2004/

straightforward calculation integer-valued N when the remainders are free of errors [7–9].

Particularly in signal processing, the CRT can be used to solve the problem of estimating the frequency of a desired signal in undersampling systems [10–13], i.e., systems whose sampling rates are co-prime and all below the Nyquist limit [14–18]. The frequency is estimated in terms of their remainders given the sampling rates. For illustration, consider that a single-tone signal whose frequency value is $f = 2177$ MHz is sampled by four distinct synchronized sensors, whose sampling rates are respectively $F_{s,1} = 11$ MHz, $F_{s,2} = 13$ MHz, $F_{s,3} = 15$ MHz and $F_{s,4} = 17$ MHz. The four sampling rates form a co-prime system since the GCD of any pair $\text{GCD}\{F_{s,i}, F_{s,j}\} = 1$, for $i \neq j$. Hence, the peaks in the DFT taken by every sensor are respectively $\{10, 6, 2, 1\}$, which are the remainders in

$$\begin{cases} f \bmod 11 = 10, \\ f \bmod 13 = 6, \\ f \bmod 15 = 2, \\ f \bmod 17 = 1, \end{cases} \tag{3}$$

where the moduli M_i are the sampling rates. For instance, in the undersampling system whose CRT scheme is given by (3), the sensor of 15 MHz reads exactly the same sequence of snapshots of a hypothetical impinging waveform of 2 MHz, since the same vector of snapshots is obtained with the frequency value of $f = 2177$ MHz or $f = 2$ MHz when sampled at $F_{s,3} = 15$ MHz. The main goal of undersampling schemes is reducing the necessary sampling rates for achieving the values of frequency. Theoretically, only three samples are sufficient for featuring frequency, phase and amplitude of a wavelength, provided that such samples are close enough. This closeness implies that the sampling rate must be sufficiently high. Undersampling systems, on the other hand, are suitable for the acquisition of high-frequency signal components that are sparse in the frequency domain when it is not possible to sample such high-frequency components at the Nyquist rate because of limitations of the sampling rate in the hardware in use [19]. For instance, in [20], with a monostatic synthetic aperture radar (SAR) for terahertz (THz), the wavelength is in the order of millimeter or submillimeter, and hence the requirement on subwavelength interval of spatial sampling by the Nyquist theory aggravates the measurement difficulty.

Clearly, measurements in the realm of digital signal processing are liable to jitter and phase noise as part of real applications. These errors affect the remainders in a CRT originated by an undersampling system. It is important to notice that any deviations in the remainders cannot be reduced or improved by the CRT system itself. A better CRT technique can, however, estimate the unknown number – in the case of undersampling systems, the frequency – with better approximation given the mentioned pre-existing errors.

In engineering applications, either the unknown is an integer or a real-number, and errors may exist or not. In the latter, we have deterministic applications, related for instance to cryptography [21,22], Digital Signature Standard (DSS) [23], image processing and security [24,25], secret sharing schemes [26,27] and E-Voting systems [28]. However, not only the remainders have errors, but also the unknown value is a real-valued number. Hence, beyond undersampling systems, CRT is also employed to estimate unknown numbers in the presence of errors such as in cognitive radio networks (CRN) [29], polynomial reconstruction [30–32], electric encoders (EE) for motion control [33], and radio interferometric positioning system [34]. Another signal processing application of CRT is related to phase unwrapping based systems for distance estimation [7,8]. In such application, the remainders are the phase of arrival in terms of wavelength, and the moduli are the wavelengths of each spectral component.

The state-of-the-art approaches for CRT estimation includes the traditional CRT [1,9], the robust CRT [1,2,6,35], the closed-form robust CRT [1,7] and the maximum likelihood based robust CRT [3,4]. In the latter, an optimization of the search routine for a real-valued number is proposed assuming Gaussian distributed errors with different variances, whereas in the closed-form robust CRT the variances are presumed constant. There is still the Multi-Stage Robust CRT, which is proposed in [8] and consists in splitting the moduli of a CRT system over different moduli groups in accordance with the GCD of each set. The number of resulting groups is the number of stages. In [13], a generalization of the two-stage robust CRT algorithm to a multi-stage system is also presented. Splitting the moduli in groups with different GCD by group can improve the remainder error bound for a given set of moduli in terms of the remainder error bound of the entire CRT system. However, such a split is based on adopting for each moduli set the same concepts of the CFR-CRT. When all moduli share the same pairwise GCD as presumed in (1), applying the Multi-Stage Robust CRT does not yield improvements for the estimation of N in terms of the maximum tolerable error.

In this paper, we propose a Kroenecker based M-Estimation (ME) approach (KME-CRT). By exploiting the Kroenecker product that yields a mapping vector, we drastically reduce the computational complexity of the ME approach allowing its practical application. Due to its routines, the here presented method is specially suitable for CRT systems with few remainders, which is equivalent to networks with few sensors. Furthermore, our proposed technique enhances the probability of estimating an unknown number accurately even when the errors in the remainders surpass 1/4 of the greatest common divisor of all moduli. We also provide a version of the mapping vectors based on tensorial n-mode products, delivering in the end the same information of the original method.

The remainder of this paper is organized as follows. The CRT systems and the state-of-the-art Closed-Form Robust CRT (CFR-CRT) and Maximum Likelihood Estimator Based Robust CRT (MLE-CRT) are reviewed in Section 2. Section 3 presents the proposed KME-CRT for assembling the mapping vector, along with its tensorial versions. Simulations and results are presented in Section 4, and Section 5 concludes the paper.

In this paper, bold calligraphic letters denote tensors, as for example in $\boldsymbol{\mathcal{T}}$. Bold upper case letters are used to denote matrices, whereas bold lower case letters are used for vectors. Scalars are denoted by non-bold letters, either upper, lower case or Greek letters. Estimated numbers are written as in $\hat{N}$, whereas values with errors are notated as in $\tilde{r}$. Vectors of estimations and values with errors are notated respectively as in $\hat{\mathbf{n}}$ and $\tilde{\mathbf{r}}$. We assume that non-integer values have the modulus operation applicable only on its integer part. Thus, when a real-valued $N = N_{\text{int}} + N_{\text{dec}}$, where $N_{\text{int}} \in \mathbb{Z}$ and $N_{\text{dec}} \in \mathbb{R}$, with $0 \leq N_{\text{dec}} < 1$, hence with the parcels referring respectively to the integer and decimal parts of N, we assume that

$$N \bmod M_i = (N_{\text{int}} \bmod M_i) + N_{\text{dec}}. \tag{4}$$

We introduce the Kroenecker product based on [36]. Let $\mathbb{S}^{p\times q}$ denote the space of real or complex matrices. The (i, j)-th entry of a matrix $\mathbf{A} \in \mathbb{S}^{p\times q}$ is a_{ij}. The Kroenecker product is defined for two matrices of arbitrary sizes over any ring. For instance, consider matrices $\mathbf{A} \in \mathbb{S}^{p\times q}$ and $\mathbf{B} \in \mathbb{S}^{u\times v}$. Their Kroenecker product is defined as

$$\mathbf{A} \otimes \mathbf{B} = \begin{bmatrix} a_{11}\mathbf{B} & \dots & a_{1q}\mathbf{B} \\ \vdots & & \vdots \\ a_{p1}\mathbf{B} & \dots & a_{pq}\mathbf{B} \end{bmatrix} \in \mathbb{S}^{pu\times qv}, \tag{5}$$

where the symbol "$\otimes$" stands for the defined Kroenecker product.

2. The state-of-the-art CRT based techniques

In practical applications, differently from solving (1), CRT problems consist in estimating a real-valued N with erroneous remainders as in

$$\begin{cases} N \bmod M_1 + \Delta_1 = \tilde{r}_1, \\ N \bmod M_2 + \Delta_2 = \tilde{r}_2, \\ \quad \vdots \quad \vdots \quad \vdots \\ N \bmod M_L + \Delta_L = \tilde{r}_L, \end{cases} \tag{6}$$

where $\tilde{r}_i = r_i + \Delta_i$, for $i \in \{1, 2, \ldots, L\}$, with Δ_i denoting the deviation or error in the i-th remainder originated from noise or inaccuracy in measurement. All remainders respect $0 \leq r_i < M_i$ for $i \in \{1, 2, \ldots, L\}$. Solving (6) is generally far more complex than (1). CRT is not a robust system due to the fact that small errors in any remainder may cause a large reconstruction error [1]. Note that, given (2), we can also write

$$n_i\, M_i + \tilde{r}_i - \Delta_i = N. \tag{7}$$

A variable τ is defined as the remainder error bound, or the maximum absolute value for every existing error Δ_i, hence $\tau = \max_{i \in \{1,\ldots,L\}} |\Delta_i|$. Assuming M as the GCD of all moduli M_i, if

$$\tau < \frac{M}{4}, \tag{8}$$

the calculation of the folding integers n_i is guaranteed [1,37]. The estimated values of n_i in CFR-CRT are designed as $\hat{n}_i$ and $\hat{N}$ is the estimation for N.

The dynamic range D of a CRT system delimits the value until which N can be uniquely determined [38,39]. As a consequence, the search for the value of N is performed only in the range of D. If all moduli M_i are co-prime such that $M = 1$, $D = \prod_{i=1}^{L} M_i$. Otherwise, if $M > 1$, let

$$\Gamma_i = \frac{M_i}{M}, \qquad i \in \{1, 2, \ldots, L\}, \tag{9}$$

so that all Γ_i, for $i \in \{1, 2, \ldots, L\}$, are co-prime, and the dynamic range D is given by

$$D = M\Gamma, \tag{10}$$

where $\Gamma = \prod_{i=1}^{L} \Gamma_i$.

In this paper, the goal is to estimate a desired real-valued N given the information about M_i and $\tilde{r}_i$, for $i \in \{1, \ldots, L\}$. One of the state-of-the-art CRT techniques is the Robust CRT [2,6], whose main disadvantage is that the order of $2(L-1)\Gamma_i$ searches is necessary even in the 1-D searching scheme. As a consequence, when L or Γ_i gets large, the searching complexity is still high [1,8]. Therefore, we consider the CFR-CRT and the MLE-CRT in terms of benchmark to compare with our proposed approach. In the CFR-CRT, the variances of the errors are presumed equal, whereas MLE-CRT addresses scenarios in which the variances of errors are different and known at prior.

Note that CRT is a deterministic problem and that, given a remainder error bound τ, all errors are confined to a fixed interval $[N - \tau, N + \tau]$. Nevertheless, probabilistic examples of CRT solutions have also been proposed, as for instance in [40]. In the following state-of-the-art methods, the errors are presumed to have Gaussian distribution. In a Gaussian distribution, any error that surpasses τ can be arbitrarily high with non-zero probability, thus violating the assumption of the existence of τ. In order to keep the Gaussian distribution yet with reasonable error profile, we assume that $\tau \approx 3\sigma$, hence assuring that more than 99% of the values of Δ_i lie in the interval $[-\tau, +\tau]$. In doing so, we also preserve the possibility of changing the variances of errors by modifying the value of τ.

Algorithm 1 State-of-the-art technique: CFR-CRT.

procedure CFR-CRT $(M_i, \tilde{r}_i)$
  for $i = 1 : L, i \neq z$ **do**
    $\hat{q}_{i,z} \leftarrow \left\lfloor \frac{\tilde{r}_i - \tilde{r}_z}{M} \right\rfloor$ % The reference remainder $\tilde{r}_z$ is chosen by means of
    % (17)–(19), and $\hat{q}_{i,z}$ follows the definition of (16)
    $\overline{\Gamma}_{i,z} \leftarrow \overline{\Gamma_z \bmod \Gamma_i}$ % MMI operation as specified in (12).
    % Note that all Γ_i are defined in (9)
    $\hat{\xi}_{i,z} \leftarrow (\hat{q}_{i,z}\overline{\Gamma}_{i,z}) \bmod \Gamma_i$
    $b_{i,z} \leftarrow \gamma_z/\Gamma_i \bmod \Gamma_i$ % Recall that all γ_i are computed as in (11)
  $\hat{n}_z \leftarrow \sum_{i=1, i\neq z}^{L} (\hat{\xi}_{i,z} b_{i,z} \frac{\gamma_z}{\Gamma_i}) \bmod \gamma_z$
  for $i = 1 : L, i \neq z$ **do**
    $\hat{n}_i \leftarrow \frac{\hat{n}_z \Gamma_z - \hat{q}_{z,1}}{\Gamma_i}$
  $\hat{N} \leftarrow \frac{1}{L} \sum_{i=1}^{L} (\hat{n}_i M_i + r_i)$

2.1. Closed-form robust CRT

According to [1,7,13], the CFR-CRT is summarized in (11)–(19) and Algorithm 1. First an auxiliary variable γ_i is defined using Γ_i from (9) and Γ from (10) as follows,

$$\gamma_i = \frac{\Gamma}{\Gamma_i}, \qquad 1 \leq i \leq L. \tag{11}$$

Note that all possible pairs $\{\gamma_i, \Gamma_i\}$ are co-prime. The modular multiplicative inverse (MMI) of a number γ_i modulo Γ_i is the smallest number $\overline{\gamma}_i$ that satisfies $\gamma_i \overline{\gamma}_i = k\Gamma_i + 1$, for some $k \in \mathbb{Z}$. In [37], the Qin's Algorithm for the calculation of the MMI by means of a fast matrix based technique is presented. We notate the MMI function as

$$\overline{\gamma}_i = \overline{\gamma_i \bmod \Gamma_i}. \tag{12}$$

According to [1], the co-primality between $\{\gamma_i, \Gamma_i\}$ assures the existence of a MMI $\overline{\gamma}_i$. Next, we define q_i,

$$q_i = \left\lfloor \frac{\tilde{r}_i}{M} \right\rfloor, \tag{13}$$

where $\lfloor . \rfloor$ stands for the flooring operation. N_0 is defined as

$$N_0 = \sum_{i=1}^{L} (\overline{\gamma}_i \gamma_i q_i) \bmod \Gamma_i. \tag{14}$$

In fact, the sequence (11)–(14) is used to calculate integer-valued N when the remainders are free of errors and receives different names in the literature, such as Conventional CRT [1,2,5,38], Gauss's Algorithm [41,42], CRT Standard version [28] and Classical CRT formula [3,4]. In [9], it is called Traditional CRT, as well as in [1,3,4]. We adopt the latter terminology. The Traditional CRT is based on the extended Euclidean algorithm [37] and is incorporated as part of the CFR-CRT in [1].

It is still worth noting that, according to the CRT theory,

$$N_0 = n_i \Gamma_i + q_i, \tag{15}$$

for $i \in \{1, 2, \ldots, L\}$, i.e., N_0 is an integer-valued number whose value is obtained by means of (15) independently of the chosen i. The CFR-CRT is developed with sequential subtractions of $(n_i\Gamma_i + q_i)$ from a reference remainder whose row is z, yielding $L - 1$ results that are generated by applying

$$n_z \Gamma_z - n_i \Gamma_i = q_{i,z} \tag{16}$$

where $q_{i,z} = q_i - q_z$, for $i \in \{1, 2, \ldots, z-1, z+1, \ldots L\}$. In order to choose the reference remainder, first we define the circular distance of two real numbers x and y for a non-zero positive number C as

$$d_C(x, y) \triangleq x - y - \left\lceil \frac{x-y}{C} \right\rfloor C. \tag{17}$$

In [1], the z-th row, which is the row of the reference remainder, is obtained via

$$\hat{r}^c \triangleq \underset{0 \le m \le M-1}{\arg\min} \sum_{i=1}^{L} d_M^2(\tilde{r}_i^c, m) \tag{18}$$

where $\tilde{r}_i^c = \tilde{r}_i \mod M$, for $i \in \{1, 2, \ldots, L\}$, and

$$z = \underset{j \in \{1,2,\ldots,L\}}{\arg\min} d_M^2(\tilde{r}_j^c, \hat{r}_c). \tag{19}$$

The estimation of $\hat{N}$ obtained from CFR-CRT according to [1] is summarized in Algorithm 1, where the results of (9)–(19) are presumed available. In line 3 of Algorithm 1, [.] stands for the rounding operator.

The selection of the optimal reference remainder $\tilde{r}_z$ is based on the reference common remainder $\tilde{r}_i^c$, which can only be appropriately determined when $\sigma_1^2 = \sigma_2^2 = \cdots = \sigma_L^2$. When σ_i^2 are different for each Δ_i, for $i \in \{1, 2, \ldots, L\}$, the calculations based on $\tilde{r}_z$ as in (18) and (19) may be ineffective [3].

Note that, although the Traditional CRT is part of the CFR-CRT, the latter is the method that makes the estimation of N achievable when the remainders have errors. CFR-CRT can be used for integer-valued N free of errors; however, in this case, it consists in a simple application of the above commented Traditional CRT.

2.2. Maximum likelihood based robust CRT

Aiming to solve the case of different variances in the errors, a Maximum Likelihood based CRT is proposed in [3,4]. MLE-CRT is basically a method for determining the best $\hat{r}^c$, the estimation of the common remainder r^c.

In [3,4], the standard deviations are $\sigma_i = \mu M_i$, for $i \in \{1, 2, \ldots, L\}$, where μ is a small arbitrary positive factor. A set Ω is then assembled as

$$\Omega = \left\{ \left(\sum_{i=1}^{L} w_i \tilde{r}_i^c + M \sum_{i=1}^{t} w_{\rho(i)} \right) \mod M \right\}, \text{ for } t \in \{1, 2, \ldots, L\}, \tag{20}$$

where ρ is a permutation of the set $\{1, 2, \ldots, L\}$ such that $\tilde{r}_{\rho(1)}^c \le \cdots \le \tilde{r}_{\rho(L)}^c$, and

$$w_i = \frac{1/\sigma_i^2}{\sum_{i=1}^{L} 1/\sigma_i^2}. \tag{21}$$

The estimated common remainder $\hat{r}^c$ is then achieved by

$$\hat{r}^c \triangleq \underset{x \in \Omega}{\arg\min} \sum_{i=1}^{L} w_i d_M^2(\tilde{r}_i^c, x) \tag{22}$$

Algorithm 2 shows the MLE-CRT, whose input arguments are M_i, $\tilde{r}_i$ and μ.

Algorithm 2 State-of-the-art technique: MLE-CRT.

procedure MLE-CRT($M_i, \tilde{r}_i, \mu$)
  for $i = 1 : L$ **do**
    $\tilde{r}_i^c \leftarrow \tilde{r}_i \mod M$
    $\sigma_i \leftarrow \mu M_i$
  for $i = 1 : L$ **do**
    $w_i \leftarrow \frac{1/\sigma_i^2}{\sum_{i=1}^{L} 1/\sigma_i^2}$
  $\tilde{\mathbf{r}}' \leftarrow [\tilde{r}_1 \ \ \tilde{r}_2 \ \ \ldots \ \ \tilde{r}_L]$
  $\mathbf{w}' \leftarrow [w_1 \ \ w_2 \ \ \ldots \ \ w_L]$
  $\mathbf{R_W} \leftarrow [\tilde{\mathbf{r}} \ \ \mathbf{w}]$
  $\mathbf{R_W} \leftarrow$ sortrows($\mathbf{R_W}$)
  for $i = 1 : L$ **do**
    for $t = 1 : i$ **do**
      $\Omega(i) \leftarrow \left\{ \left(\sum_{j=1}^{L} w_j \tilde{r}_j^c + M \sum_{j=1}^{t} \mathbf{R_W}(j, 2) \right) \mod M \right\}$
  $\hat{\mathbf{r}} \leftarrow$ zeros[$L \times 1$]
  for $i = 1 : L$ **do**
    $x \leftarrow \Omega(i)$
    $\hat{\mathbf{r}}(i) \leftarrow \sum_{j=1}^{L} w_j d_M^2(\tilde{r}_i^c, x)$
  [$\sim$, index] $\leftarrow \min(\hat{\mathbf{r}})$
  $\hat{r}^c = \Omega$(index)
  for $i = 1 : L$ **do**
    $\hat{q}_i \leftarrow \left\lceil \frac{\tilde{r}_i - \hat{r}^c}{M} \right\rfloor$
  $\hat{N}_0 \leftarrow \sum_{i=1}^{L} \overline{\gamma_i} \gamma_i \hat{q}_i \mod \Gamma$
  $\hat{N} \leftarrow M\hat{N}_0 + \hat{r}^c$

3. Kroenecker product based mapping vector

In Subsection 3.1, we exploit the CRT system with error-free remainders, with $N \in \mathbb{Z}$ and $\Delta_i = 0$, for $i \in \{1, 2, \ldots, L\}$, in which N is not estimated but rather calculated in a deterministic way. Next, Subsection 3.2 handles the case of remainders with errors, when $\hat{N}$, the estimated N, is obtained. In Subsection 3.3, we provide a tensorial model based on n-mode products for delivering the same information of the mapping vector with regards to the error-free case of Subsection 3.1 and the remainders with errors of Subsection 3.2. Subsection 3.4 presents the study of how the proposed mapping vector enables correct estimations $\hat{N}$ even when $M/4 \le \tau < M/2$. Recall that, when any error surpasses $M/4$, the reconstruction of the folding integers $\hat{n}_i$ is not guaranteed in accordance with the literature.

If an ME routine is performed over the entire dynamic range D in order to find the most appropriate value of $\hat{N}$ that minimizes all deviations with regards to the remainders, the result is a computationally expensive task. In order to mitigate this hindrance, we propose a mapping vector $\mathbf{v}$ that indicates on which parts of D the search for N should be made. From the knowledge of the values M_i and $\tilde{r}_i$, L auxiliary vectors $\mathbf{c}_i$, for $i \in \{1, 2, \ldots, L\}$ are assembled, which jointly yield $\mathbf{v}$.

As it will be shown in Algorithm 3 of Subsection 3.2, our M-Estimator for a given $\hat{N}$ is based on the minimization of θ in (23). Using the circular distances of (17), for the case of all variances with the same value, the estimator is given by

$$\theta = \underset{\hat{N}}{\arg\min} \sum_{i=1}^{L} (d_{M_i}(\hat{N} \bmod M_i, \tilde{r}_i))^2, \tag{23}$$

whereas if the variances are a function of the respective modulus M_i,

$$\theta = \underset{\hat{N}}{\arg\min} \sum_{i=1}^{L} \left(\frac{d_{M_i}(\hat{N} \bmod M_i, \tilde{r}_i)}{M_i} \right)^2, \tag{24}$$

where the values of $\hat{N}$ are to be selected according to the content of the mapping vector $\mathbf{v}$. Note that either in (23) and (24) the intermediate estimation of the folding integers $\hat{n}_i$ is avoided, differently of the state-of-the-art CFR-CRT and MLE-CRT.

3.1. Data structure for remainders without errors

In this Subsection, we address the problem of calculating $N \in \mathbb{Z}$ and $\Delta_i = 0$, for $i \in \{1, 2, \ldots, L\}$. Prior to the CRT system itself, we explain how N can be determined by the remainders and moduli under the perspective of group theory as a way of featuring the proposed method. In any CRT system, each of the L rows informs the possible values for N over the dynamic range D. We then assemble the sets S_i, for $i \in \{1, 2, \ldots, L\}$, where the k-th component is of the form

$$r_i + (k-1)M_i, \tag{25}$$

for $k \in \{1, 2, \ldots, \gamma_i\}$. Therefore, the values in each set S_i represent the sufficient and necessary set of possibilities for N in the dynamic range respecting the condition $N \bmod M_i = r_i$. Hence,

$$S_i = \{r_i,\ (r_i + M_i),\ (r_i + 2M_i),\ \ldots,\ (r_i + (\gamma_i - 1)M_i)\}, \tag{26}$$

and we can write

$$\cap_{i=1}^{L} S_i = \{N\}, \tag{27}$$

which is equivalent to stating that N is the unique number that figures simultaneously in all sets S_i, for $i \in \{1, 2, \ldots, L\}$.

Proposition 1. *The set of values in each S_i specified as in (26) not only cover all the possibilities of values for the unknown N, given M_i and r_i over D, but also N cannot be excluded from any set S_i.*

Proof of sufficiency. In case of Proposition 1, sufficiency is proven if and only if any additional insertions of $(r_i + kM_i)$ terms beyond the limit shown in (26), i.e., $(r_i + (\gamma_i - 1)M_i)$, lead to repetition of terms in the set S_i. Let $(r_i + kM_i)$, $k \in \{0, 1, \ldots, (\gamma_i - 1)\}$ be the $(k+1)$-th possible value for N in the set S_i. We show that extending the content of S_i by inserting a k'-th entry, where

$$k' = q_1\gamma_i + q_2, \tag{28}$$

where $q_1 \in \mathbb{Z}^+$ and $q_2 \in \mathbb{Z}$, entails repetition of values in S_i, since the inserted values are of the form

$$r_i + (q_1\gamma_i + q_2)M_i = r_i + q_1 D + q_2 M_i, \tag{29}$$

as $M\gamma_i\Gamma_i = D$. Given the definition of the dynamic range, $(r_i + D + q_2M_i) \bmod D = r_i + q_2M_i$, if $q_2 < D/M_i$. If, otherwise, $q_2 \geq D/M_i$ in (29), then

$$\begin{aligned} \bmod (k'M_i, D) &= \bmod (q_2M_i, D) = \bmod (D + q_2'M_i, D) \\ &= \bmod (q_2'M_i, D), \end{aligned} \tag{30}$$

so that it is possible to substitute $q_2'M_i = k'$ and recalculate (28) until $q_2 < D/M_i$ in (29). Note that, since $q_2 \in \mathbb{Z}$, D/M_i is also an integer, it is equivalent to state that $q_2 \leq \gamma_i - 1$, as $D/M_i = \gamma_i$. Therefore, the dynamic range is surpassed given a set of values for S_i if any arbitrary value $(r_i + k'M_i)$, with $k' \in \{\gamma_i, \gamma_i + 1, \ldots\}$, is included in S_i. Due to the minimum values that q_1 and q_2 can assume in (28), namely $q_1 = 1$ and $q_2 = 0$, no further elements are to be included in (26), proving the limit $k' = \gamma_i$. As a consequence, each set S_i has γ_i terms. The smallest value for S_i cannot be lower than r_i due to the non-admission of negative numbers. Hence, the analysis of the boundary to the left is dismissed.

Proof of necessity is the requirement that no possible value of N can be excluded from at least one set S_i, $i \in \{1, 2, \ldots, L\}$. This proof is straightforward, since $N \bmod M_i = r_i$, $k \in \{0, 1, \ldots, \gamma_i - 1\}$. □

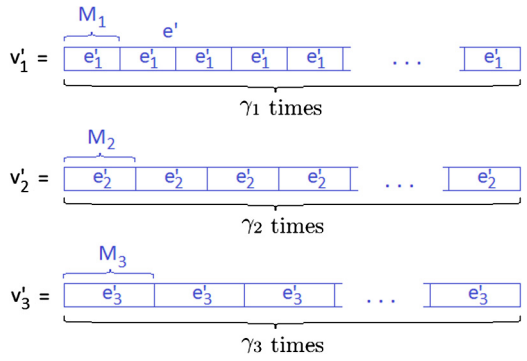

Fig. 1. Visual equivalent description of (33) with $L = 3$ as example.

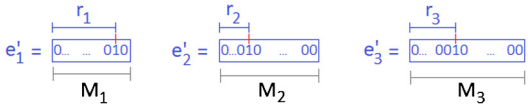

Fig. 2. Visual equivalent description of $\mathbf{e}_i$ as specified in (31).

Defining $\mathbf{e}_i \in \mathbb{Z}^{M_i}$ as

$$\begin{cases} \mathbf{e}_i(p) = 1, & \text{if } p = r_i \text{ and } r_i \neq 0, \\ \mathbf{e}_i(p) = 1, & \text{if } p = M_i \text{ and } r_i = 0, \\ \mathbf{e}_i(p) = 0, & \text{otherwise,} \end{cases} \tag{31}$$

and the vector $\mathbf{u}_k$ as

$$\mathbf{u}_k \in \mathbb{Z}^k,\ \mathbf{u}_k(j) = 1 \text{ for } j \in \{1, 2, \ldots, k\}, \tag{32}$$

each column-vector $\mathbf{c}_i \in \mathbb{Z}^D$ is obtained via Kroenecker product as

$$\mathbf{c}_i = \mathbf{w}_i \otimes \mathbf{e}_i, \tag{33}$$

where, defining the auxiliary set $\mathcal{Y}_i \in \{1, \ldots, i-1, i+1, \ldots, L\}$,

$$\mathbf{w}_i = \mathbf{u}_{\Gamma_{\mathcal{Y}_i(1)}} \otimes \mathbf{u}_{\Gamma_{\mathcal{Y}_i(2)}} \otimes \cdots \otimes \mathbf{u}_{\Gamma_{\mathcal{Y}_i(L-1)}}, \tag{34}$$

which is the same as writing

$$\mathbf{w}_i = \mathbf{u}_{\gamma_i}. \tag{35}$$

Carrying out the product in (33) is the same as assembling a vector which is formed by γ_i stacked vectors $\mathbf{e}_i$. Fig. 1 shows the concept for visualization with an example where $L = 3$. Note that the length of the resultant $\mathbf{c}_i$ is $M_i\gamma_i = M\Gamma = D$, for $i \in \{1, 2, \ldots, L\}$, in accordance with (10).

Every vector $\mathbf{e}_i \in \mathbb{Z}^{M_i}$ in Fig. 1 has zeros in all entries, except in entry $\mathbf{e}_i(r_i) = 1$ according to (31). A generic representation of $\mathbf{e}_i$ in a system with $L = 3$ is shown in Fig. 2.

In the context of undersampling systems, Fig. 1 combined with Fig. 2 has the representation of Fig. 3 for $L = 3$. The sampling rates $F_{s,i}$ are the length of the i-th DFT window and numerically correspond to M_i, for $i \in \{1, 2, 3\}$. The r_i-th entry of each $\mathbf{e}_i$ is 1 due to (31) as in Fig. 2. Here, r_i indicates the frequency f undersampled at the rate $M_i = F_{s,i}$, as $f \bmod M_i = r_i$, in accordance with (3). Note that the value of N is achieved only when $\mathbf{v}_1(N) = \mathbf{v}_2(N) = \mathbf{v}_3(N) = 1$, and that over the dynamic range D only one value of N fits in this definition. This simultaneousness derives from (27). Since all peaks in Fig. 3 are of the form $r_i + kM_i$, for $k \in \{0, 1, 2, \ldots, \gamma_i - 1\}$, they obey the rule of (25).

Each vector $\mathbf{c}_i \in \mathbb{Z}^D$ is obtained by means of (33). Gathering all $\mathbf{c}_i$ together, the mapping vector $\mathbf{v} \in \mathbb{Z}^D$ is given by

$$\begin{cases} \mathbf{v}(p) = 1, & \text{if } \prod_{i=1}^{L} \mathbf{c}_i(p) = 1, \\ \mathbf{v}(p) = 0, & \text{otherwise.} \end{cases} \tag{36}$$

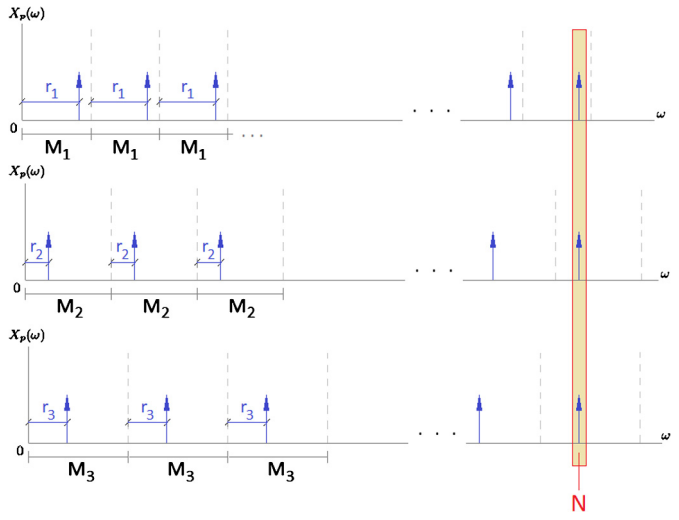

Fig. 3. Visual equivalent description of CRT for an undersampling system with $L = 3$. Each graphic reproduces the values in $\mathbf{c}_i$ through repetitions of the DFT window, and the value of N is achieved when all the peaks occur simultaneously, due to (27).

Note that each vector $\mathbf{c}_i$ contains a sequence of entries whose values are either 0 or 1. The relevant information is the cardinality of the entries 1 throughout the vector $\mathbf{c}_i$, which indicate the possible values of N according to the content of each set S_i, for $i \in \{1, 2, \ldots, L\}$, as in (26). Hence, (36) aims at obtaining the set intersection specified in (27), which returns N.

3.2. Data structure for remainders with errors

If $N \in \mathbb{Z}$ and $\Delta_i = 0$, for $i \in \{1, 2, \ldots, L\}$, the data structure explained in (31)–(36) suffices for determining the value of N. However, if $\Delta_i \neq 0$ for any $i \in \{1, 2, \ldots, L\}$, the entries of the unitary vectors $\mathbf{e}_i$ must inform not the integer remainders, but the interval in which the remainders lie given that the errors are continuous variables. Fig. 4 illustrates the assemblage of vectors $\mathbf{e_i}$, for $i \in \{1, 2, \ldots, L\}$, in terms of subsections 3.1 and 3.2. Hereafter, each entry in $\mathbf{e_i}$ is determined in accordance with the model of Fig. 4(b), i.e., the entry that satisfies the criterion in terms of r_i assumes the value 1, while the others remain with value zero. In this paper, the interval is 1/4 for each entry. Hence, while in subsection 3.1 all vectors $\mathbf{c}_i \in Z^D$, now $\mathbf{c}_i \in Z^{4D}$ due to the fact that the vector $\mathbf{e}_i \in \mathbb{Z}^{4M_i}$. The length 1/4 is chosen as an example, so that other implementations of the here proposed method can have different values for this length. Note that in (a) the r_i stand for a discrete variable, whereas in (b) the r_i are continuous variables due to the fact that N is also a continuous number.

In the proposed KME-CRT with errors in the remainders, all $\tilde{r}_i$ and M_i are normalized to the case $M = 1$, so that $M_i = \Gamma_i$, for $i \in \{1, 2, \ldots, L\}$. This is achieved by dividing all rows in (6) by M as in (37),

Algorithm 3 Proposed Kroenecker Based Mapping Vector for ME-CRT.

procedure PROPOSED KME-CRT $(M_i, \tilde{r}_i, s_i, H)$
  $\mathbf{v} \leftarrow$ zeros$[4D \times 1]$ % **v** is the mapping vector to be obtained
  for $i = 1 : L$ **do**
    $\mathbf{e}_i \leftarrow$ zeros$[4\Gamma_i \times 1]$
    $\mathbf{e}_i(j_i) \leftarrow 1$, where $j_i = \lceil 4r_i \rceil$
    for $k \in \{-2, -1, 1, 2\}$ **do**
      if $j_i + k \neq 4\Gamma_i$ **then**
        $\mathbf{e}_i((j_i + k) \bmod 4\Gamma_i) \leftarrow 1$
      else $j_i + k = 4\Gamma_i$
        $\mathbf{e}_i(4\Gamma_i) \leftarrow 1$
    $\mathcal{Y}_i \leftarrow \{1, 2, \ldots, i-1, i+1, \ldots, L\}$
    $\mathbf{w}_i = \mathbf{u}_{\Gamma_{\mathcal{Y}_i(1)}} \otimes \mathbf{u}_{\Gamma_{\mathcal{Y}_i(2)}} \otimes \cdots \otimes \mathbf{u}_{\Gamma_{\mathcal{Y}_i(L-1)}}$ % Eq. (34)
    $\mathbf{c}_i \leftarrow \mathbf{w}_i \otimes \mathbf{e}_i$ % Eq. (33)
  for $p = 1 : 4D$ **do**
    if $\prod_{i=1}^{L} \mathbf{c}_i(p) = 1$ **then** % Conditions stated in (36)
      $\mathbf{v}(p) \leftarrow 1$
  $\mathbf{p} \leftarrow$ find$(\mathbf{v}(p))$ % **p** informs which rows of **v** have all elements 1
  $L_p \leftarrow$ length$(\mathbf{p})$
  $\mathbf{p} \leftarrow \mathbf{p}/4 - 1/4$ % As each row of **v** in fact spans 1/4.
  $L_q \leftarrow \lceil 1/4s_i \rceil$
  $\mathbf{Q} \leftarrow$ zeros$[L_q \times L_p]$
  $\mathbf{W} \leftarrow$ zeros$[L_q \times L_p]$
  for $j_1 = 1 : L_q$ **do**
    for $j_2 = 1 : L_p$ **do**
      $\mathbf{Q}(j_1, j_2) \leftarrow \mathbf{p}(j_2) + (j_1 - 1)s_i$
      for $i = 1 : L$ **do**
        if $H = 1$ **then** % Hypothesis of constant variances
          $\mathbf{W}(j_1, j_2) \leftarrow \mathbf{W}(j_1, j_2) + (d_{\Gamma_i}(\mathbf{Q}(j_1, j_2) \bmod \Gamma_i), \tilde{r}/M)^2$
        else $H = 2$ % Hypothesis of σ_i^2 as a function of M_i
          $\mathbf{W}(j_1, j_2) \leftarrow \mathbf{W}(j_1, j_2) + (d_{\Gamma_i}((\mathbf{Q}(j_1, j_2) \bmod \Gamma_i), \tilde{r}/M)/\Gamma_i)^2$
  $[x_1, x_2] \leftarrow \min(\mathbf{W})$
  $[\sim, x_3] \leftarrow \min(x_1)$ % $\mathbf{W}(x_2(x_3))$ is the minimal deviation in the ME algorithm
  $\hat{N} = M\mathbf{Q}(x_2(x_3), x_3)$ % Hence, $\mathbf{Q}(x_2(x_3))$ is the optimal value of N/M.

$$\begin{cases} N_m \bmod \Gamma_1 = \tilde{r}_1/M, \\ N_m \bmod \Gamma_2 = \tilde{r}_2/M, \\ \quad \vdots \quad \vdots \quad \vdots \\ N_m \bmod \Gamma_L = \tilde{r}_L/M, \end{cases} \tag{37}$$

where $N_m = N/M$. The assemblage of $\mathbf{e}_i \in \mathbb{Z}^{4M_i}$, for $i \in \{1, 2, \ldots, L\}$, is modified to

$$\begin{cases} \mathbf{e}_i(p) = 1, \quad \text{if } p = \lceil 4r_i \rceil \\ \text{For } k \in \{-2, -1, 1, 2\} \text{ do} \\ \quad \mathbf{e}_i(p) = 1, \quad \text{if } p = (\lceil 4r_i \rceil + k) \bmod 4\Gamma_i \text{ and } \lceil 4r_i \rceil + k \neq 4\Gamma_i, \\ \quad \mathbf{e}_i(p) = 1, \quad \text{if } p = 4\Gamma_i \text{ and } \lceil 4r_i \rceil + k = 4\Gamma_i, \\ \text{End For} \\ \mathbf{e}_i(p) = 0, \quad \text{otherwise}, \end{cases} \tag{38}$$

where $\lceil . \rceil$ stands for the ceil operator, which turns the input number to next integer towards plus infinity. Eq. (38) adapts (31) for the case of errors in the remainders.

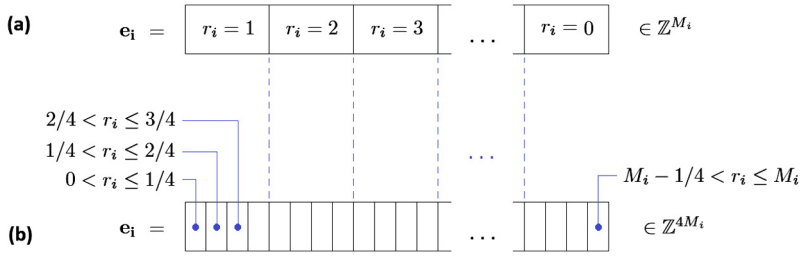

Fig. 4. Assemblage of vectors $\mathbf{e_i}$, for $i \in \{1, 2, \ldots, L\}$, (a) in terms of subsection 3.1 and (b) in terms of subsection 3.2, where the value 1 is inserted in the entry that can contain the true r_i. In (a), the r_i stand for discrete values, whereas in (b) the entries refer to the interval of r_i, which are now continuous variables.

Algorithm 3 specifies the routine for the estimation of $\hat{N}$ in the proposed method for remainders with errors. The set $\Gamma \in \{\Gamma_1, \Gamma_2, \ldots, \Gamma_L\}$ has its values selected with aid of the same auxiliary set $\mathcal{Y}$ used in (34). The input arguments are $M_i, \tilde{r}_i, s_i, H$, where s_i is the incremental step of the ME iterations and H is the hypothesis of error variances, i.e., $H = 1$ for $\sigma_i = \tau/3$, and $H = 2$ for $\sigma_i = (M_i\tau)/(3M_1)$, for $i \in \{1, 2, \ldots, L\}$. The corresponding adjustment is between lines 33 and 37 of the Algorithm, following the stated in (23) and (24) respectively.

Note that, according to the commands in lines 32, 33 and 34 of the Algorithm 3, the proposed method evaluates the minimal squared errors in terms of the M-Estimators in (23) and (24). A set of numbers is tested in intervals in accordance with the incremental step s_i, which is the resolution of test. It is indeed a test made over discrete values, however, any real number can be sufficiently approximated with a properly chosen small incremental step s_i.

3.3. Tensorial models for the proposed mapping vector

In this Subsection, we present equivalent approaches to the set of Eqs. (31)–(36) involving tensorial operations as a way of enriching the proposed technique. In Subsection 3.3.1, we explain the sequence of operations for the error-free case of Subsection 3.1, and in Subsection 3.3.2, for the case of a system with erroneous remainders of Subsection 3.2.

According to [43], the n-mode product between a tensor $\mathcal{A} \in \mathbb{R}^{x_1 \times x_2 \times \cdots \times x_N}$ with a matrix $\mathbf{E} \in \mathbb{R}^{J \times x_n}$ over the n-th dimension of $\mathcal{A}$ is denoted by

$$\mathcal{B} = \mathcal{A} \times_n \mathbf{E}, \tag{39}$$

where $\mathcal{B} \in \mathbb{R}^{x_1 \times x_2 \times \cdots \times x_{n-1} \times J \times x_{n+1} \times \cdots \times x_N}$. Note that, in terms of matrix based expressions, we have

$$\mathcal{B}_{(n)} = \mathbf{E}\mathcal{A}_{(n)}, \tag{40}$$

where the subscript in tensor $\mathcal{B}_{(n)}$ denotes that it is unfolded over its n-th dimensional fibers [43]. Hence, $\mathcal{A}_{(n)}$ and $\mathcal{B}_{(n)}$ are matrices, so that the first size of $\mathcal{A}_{(n)}$ is x_n, while in $\mathcal{B}_{(n)}$ the first size is J. The second size of $\mathcal{A}_{(n)}$ and $\mathcal{B}_{(n)}$ is the product of all remaining dimensions of the original tensor, i.e., $(x_1 x_2 \ldots x_{n-1} x_{n+1} \ldots x_N)$.

One of the properties of the n-mode product shown in (39) is that one can select the entries of a tensor over one of its dimensions by means of a diagonal matrix whose elements are properly chosen. If the matrix used in (39) is $\mathbf{E} \in \mathbb{R}^{x_n \times x_n}$ where $\mathbf{E}(l, l) = 1$, for $1 \le l \le x_n$, and all other entries are zero, then the resulting tensor $\mathcal{B}_{(n)}$ is

$$\begin{cases} \mathcal{B}(x_1, x_2, \ldots, x_n, \ldots, x_N) = \mathcal{A}(x_1, x_2, \ldots, x_n, \ldots, x_N), \text{ if } x_n = l, \\ \mathcal{B}(x_1, x_2, \ldots, x_n, \ldots, x_N) = 0, \text{ otherwise.} \end{cases} \tag{41}$$

As an example, let the tensor $\mathcal{A} \in \mathbb{R}^{5\times6\times4}$ and the matrix $\mathbf{E} \in \mathbb{R}^{5\times5}$ have an n-mode product. If $\mathbf{E}(i, j) = 0$ for $i \neq j$ and the main diagonal of $\mathbf{E}$ is the vector

$$\mathbf{e} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \tag{42}$$

then

$$\mathbf{E} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{43}$$

and the n-mode product of (39) is written as $\mathcal{B} = \mathcal{A} \times_1 \mathbf{E}$. Fig. 5 provides a visual interpretation of this tensorial operation, with the original entries in gray and zero values in white. The diagonal of $\mathbf{E}$ is applied over the first dimensions, i.e., column-wise. Tensor $\mathcal{A}$ has its entries in the fourth slice of the first dimension preserved, while all other entries are set to zero, yielding thereby tensor $\mathcal{B}$.

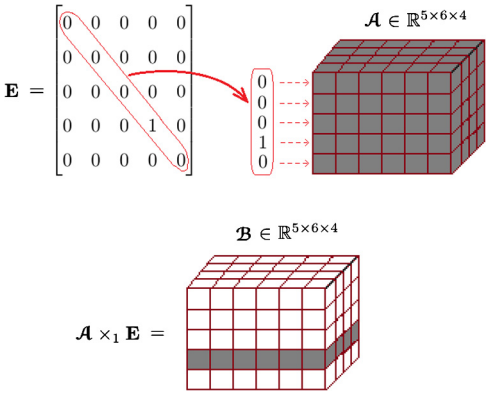

Fig. 5. Visual interpretation of the tensorial n-mode product $\mathcal{B} = \mathcal{A} \times_1 \mathbf{E}$. By convention, original entries are in gray and zero values in white.

Algorithm 4 Proposed Tensorial KME-CRT for remainders free of errors.

```
1: procedure TENSORIAL KME-CRT 1 (M_i, r_i)
2:     T ← ones([M_i])
3:     for i = 1 : L do
4:         E_i ← diag{e_i}                    % Vectors e_i defined in (31)
5:     T^(1) ← T ×_1 E_1
6:     M'_i ← M_i
7:     for i = 2 : L do
8:         M'_i ← circshift{M'_i, (L − 1)}
9:         v ← T^(i−1)_(L+1)
10:        Reshape the vector v into a tensor T^(i) ∈ ℕ^[M'_i]
11:        T^(i) ← T^(i) ×_1 E_i
12:    v ← T^(L)_(L+1)
13:    N ← find{v}
```

3.3.1. Tensorial model for the error-free case

The tensorial algorithm for the proposed KME-CRT starts with the moduli M_i and the remainders r_i. Initially, we set up a tensor $\mathcal{T} \in \mathbb{Z}^{M_1 \times M_2 \times \cdots \times M_L}$, with $\mathcal{T}(j_1, j_2, \ldots, j_L) = 1$, for all $i \in \{1, 2, \ldots, L\}$ and $j_i \in \{1, 2, \ldots, M_i\}$, i.e., the value 1 in all entries. Now define matrices $\mathbf{E}_i \in \mathbb{Z}^{M_i \times M_i}$ following

$$\mathbf{E}_i = \text{diag}\{\mathbf{e}_i\}, \tag{44}$$

using the vectors $\mathbf{e}_i$ defined in (31). Algorithm 4 shows the sequence of steps in order to accomplish the calculation of N. Note that, in line 8, the circshift$(\mathbf{a}, j)$ command makes a circular shift over a vector $\mathbf{a} \in \mathbb{R}^L$ as in

$$\text{circshift}(\mathbf{a}, j) = \begin{bmatrix} \mathbf{a}(L - j + 1 : L) & \mathbf{a}(1 : L - j) \end{bmatrix}, \tag{45}$$

while, in line 9, $\mathcal{T}$ is unfolded in its $(L+1)$-th dimension, yielding vector $\mathbf{v}$.

As visual example of application for Algorithm 4, let a CRT system with $L = 3$ and M_1, M_2, M_3 be generic moduli. The tensor $\mathcal{T} \in \mathbb{Z}^{M_1 \times M_2 \times M_3}$ is set up with all entries 1. Fig. 6 shows the sequence of steps in this specific case. Note that, along the three steps (a), (b) and (c), the tensor $\mathcal{T}^{(i)}$, $i \in \{1, 2, 3\}$, is the reshape of vector $\mathbf{v}$ as stated in line 10 of Algorithm 4. The n-mode products along the first dimension successively filter the elements of the reshaped tensor $\mathcal{T}^{(i)}(x_1, x_2, x_3)$ which are located at the slice $x_1 = r_i$ at each step i.

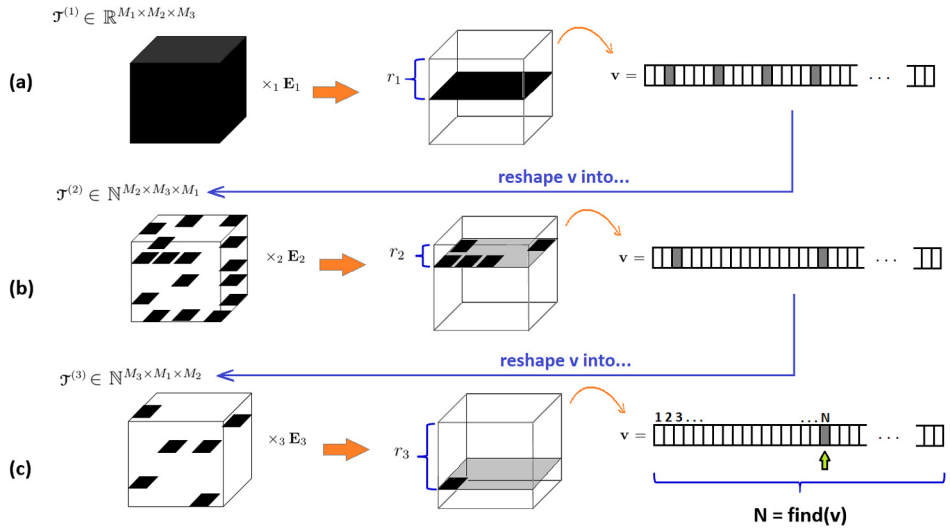

Fig. 6. Example of application of Algorithm 4 with $L = 3$. The tensor $\mathcal{T}^{(i)}$, $i \in \{1, 2, 3\}$, is at each step i the reshape of vector $\mathbf{v}$ as stated in line 10. The n-mode products along the first dimension filter the elements of the reshaped tensor $\mathcal{T}^{(i)}(x_1, x_2, x_3)$ where $x_1 = r_i$.

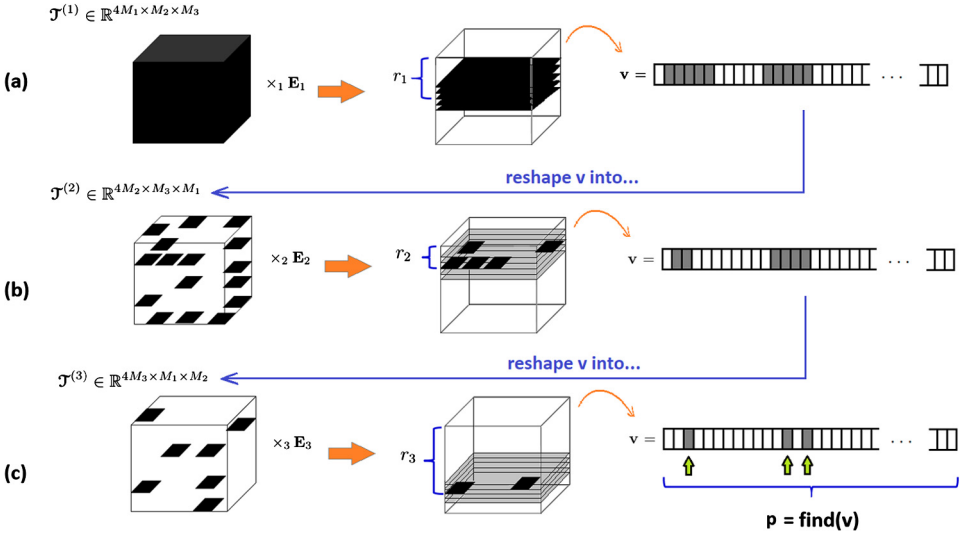

Fig. 7. Example of application of Algorithm 5 with $L = 3$, providing a version of Fig. 6 for the case of remainders with errors as described in Algorithm 5. Note that the final vector is $\mathbf{p}$ which, differently of vector $\mathbf{v}$ in Fig. 6, has several intervals of possible locations of $\hat{N}$.

3.3.2. *Tensorial model for the case of remainders with errors*

In order to adapt the Algorithm 3 for the case when there are errors in the remainders, we rewrite matrices $\mathbf{E}_i \in \mathbb{Z}^{4M_i \times 4M_i}$ as in (44), however now using vectors $\mathbf{e}_i \in \mathbb{Z}^{4M_i}$ defined as in (38). Algorithm 5 gives the pathway for the best estimation of $\hat{N}$. Note that, by the end of Algorithm 5, the last steps of Algorithm 3 are needed to achieve the definitive estimation.

The routine in Algorithm 5 is shown in Fig. 7, where the scheme in Fig. 6 is adapted in order to provide the estimation of $\hat{N}$ when at least one of the errors is not equal to zero. Note that the final vector is $\mathbf{p}$ which, differently of vector $\mathbf{v}$ in Fig. 6, has several intervals of possible locations of $\hat{N}$, and that the first dimension of the reshaping tensor $\mathcal{T}^{(i)}$ at each stage i is $4M_i$.

Algorithm 5 Proposed Tensorial KME-CRT for remainders with errors.

1: **procedure** PROPOSED TENSORIAL KME-CRT 2 $(M_i, \tilde{r}_i)$
2: $M_i(1) = 4M_i(1)$
3: $\mathcal{T} \leftarrow \text{ones}([M_i])$
4: **for** $i = 1 : L$ **do**
5: $\mathbf{E}_i \leftarrow \text{diag}\{\mathbf{e}_i\}$ % Vectors $\mathbf{e}_i$ defined in (38)
6: $\mathcal{T} \leftarrow \mathcal{T} \times_1 \mathbf{E}_1$
7: $M'_i \leftarrow M_i$
8: **for** $i = 2 : L$ **do**
9: $M'_i(1) \leftarrow M'_i(1)/4$
10: $M'_i \leftarrow \text{circshift}\{M'_i, (L-1)\}$
11: $M'_i(1) \leftarrow 4M'_i(1)$
12: $\mathbf{v} \leftarrow \mathcal{T}_{(L+1)}$
13: Reshape the vector $\mathbf{v}$ into a tensor $\mathcal{T}^{(i)} \in \mathbb{N}^{M'_i}$
14: $\mathcal{T}^{(i)} \leftarrow \mathcal{T}^{(i)} \times_1 \mathbf{E}_i$
15: $\mathbf{p} \leftarrow \text{find}\{\mathcal{T}^{(L)}_{(L+1)}\}$
16: Resume Algorithm 3 at line 24

3.4. *Possibility of correct estimation when $M/4 \leq \tau < M/2$ by means of the proposed mapping vector*

In accordance with [13,44], CRT is a robust method when the remainders have an error bound τ and the reconstruction error is also bounded to $|N - \hat{N}| \leq \tau$. Note that, as extensively studied in the literature, the maximum value for τ is $\tau < M/4$ as given in (8). In [37], the sharpness of the boundary in (8) is illustrated by means of an example. The boundary in (8) is indeed the sufficient one in order to ensure that all folding integers n_i are

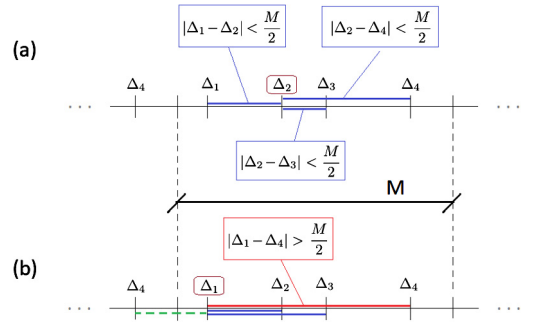

Fig. 8. Magnitudes of the errors Δ_i along the distance M, where (a) the chosen reference remainder is r_2, when all distances respect the limit $|\Delta_2 - \Delta_i| < M/2$, whereas in (b) r_1 is erroneously selected as the reference remainder, yielding $|\Delta_1 - \Delta_4| > M/2$, which violates the criterion in (46), that is a necessary and sufficient condition for solving the CRT system. (For interpretation of the colors in the figure(s), the reader is referred to the web version of this article.)

correctly reconstructed. However, the actual boundary from a theoretical standpoint is given by

$$-\frac{M}{2} \leq \Delta_1 - \Delta_i < \frac{M}{2}, \tag{46}$$

so that (46) is automatically guaranteed when $\tau < M/4$, as extensively proven in [1,8,13,44]. Thus, while (8) is a sufficient condition for the uniqueness of the solution of the folding numbers n_i, (46) is the necessary and sufficient one, constituting the general boundary for a robust CRT.

The main drawback in working with (46), in accordance with [1,8], is that it involves two remainder errors, which are in practice hard to check. That is the reason why the limit of (8) is largely adopted in the literature instead of (46). On the other hand, a consequence of using (8) is that selecting the remainder of least variance is crucial for the success of the CRT methods based on a reference remainder [1,13]. In order to illustrate this aspect, Fig. 8 shows an example with the remainders errors of a CRT system of $L = 4$, $\Delta_i \in \mathbb{R}$, for $i \in \{1, 2, 3, 4\}$, normalized at each length M. In this example, we assume $M/4 < |\Delta_3| < M/2$ and $M/4 < |\Delta_4| < M/2$. In Fig. 8(a), the chosen reference remainder is r_2, so that $|\Delta_2 - \Delta_i| < M/2$, with $i \in \{1, 3, 4\}$. In Fig. 8(b), an alternative case is shown where r_1 is erroneously selected as the reference remainder. Suppose, as suggested by the figure, that $|\Delta_1 - \Delta_4| > M/2$ through the continuous red line, i.e., inside the length M. In order to obtain $|\Delta_1 - \Delta_4| < M/2$, the resulting minimal distance $|\Delta_1 - \Delta_4|$ must be calculated through the green dashed line to the left. However, computing the distance $|\Delta_1 - \Delta_4|$ in this way corresponds to changing the remainder error Δ_4, yielding $\Delta'_4 = \Delta_4 - M$, whereas Δ_4 is the true deviation. Since originally $\tilde{r}_4 = r_4 + \Delta_4$, the change in the pathway entails $r_4 + \Delta'_4 + M = r'_4 + \Delta'_4$, where $r'_4 = r_4 + M$, thus erroneously changing the value of the remainder r_4. As a consequence, the choice of r_1 as the reference remainder in this example leads to the violation of the rule in (46).

We now explain how the proposed mapping vector addresses this problem. Lines 5 to 11 of Algorithm 3 are dedicated to set up vectors $\mathbf{e}_i \in \mathbb{Z}^{4M_i}$, for $i \in \{1, 2, \ldots, L\}$, while lines 13 and 14 provide their successive concatenations until the vectors $\mathbf{c}_i$ are assembled. As explained with Fig. 4, each vector $\mathbf{e}_i$ contains entries (or slots) that inform the occurrence of the $\tilde{r}_i$ value in terms of slots whose length is 1/4. In accordance with (38), two slots on each side of the original entry in $\mathbf{e}_i$ are also filled with 1. As a consequence, any possible slot corresponding to the correct r_i has 1 as its entry in $\mathbf{e}_i$, since two slots cover 1/2 on each side of the entry related to $\tilde{r}_i$. Fig. 9 shows how the criterion in (46) is maintained. Independently of how near to the border of the original slot the value $\tilde{r}_i$ is, the values within the distance $\pm M/2$ have also entries 1. Points a and b in Fig. 9 illustrate two hypotheses for the

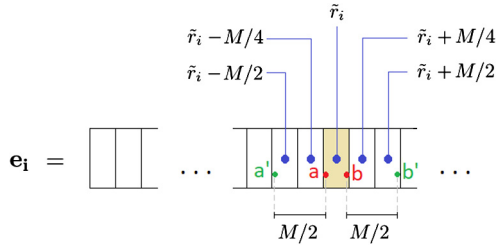

Fig. 9. Assemblage of vector $\mathbf{e}_i$ in terms of $\tilde{r}_i$ value, with two entries on each side of the original entry also filled with 1. Points a and b are examples of near border points, and the points a' and b' are in any case within a slot of value 1.

location of the value r_i near border points. Points a' and b', which show the spatial boundary for the value of $\tilde{r}_i$ in each case, with a maximum deviation of $M/2$ or two slots, are also within a slot of value 1, and their interval are then included in the M-Estimator test of either (23) or (24) due to (38).

After assembling all vectors $\mathbf{e}_i \in \mathbb{Z}^{4M_i}$ and $\mathbf{c}_i \in \mathbb{Z}^{4D}$, commands in lines 16 and 17 of Algorithm 3 yield the scheme in Fig. 10, where each vector $\mathbf{c}_i$ is set up according lines 13 and 14 of the same algorithm. As a consequence, only a restricted set of entries in the resulting vector $\mathbf{v} \in \mathbb{Z}^{4D}$ is obtained. Since $\mathbf{v}$ contains solely the intersection of all 1 entries from the vectors $\mathbf{c}_i$, for $i \in \{1, 2, \ldots, L\}$, the cardinality of these entries indicate in which points of the dynamic range the application of the M-Estimator is to be made, thus constituting the mapping vector $\mathbf{v}$ over the dynamic range D. Note that there are many intersections of this type throughout the vector $\mathbf{v}$, such that in Fig. 10 only one intersection, p_1, is shown due to practical reasons.

As a result of schemes in Figs. 9 and 10, every value r_i that follows $|r_i - \tilde{r}_i| \leq M/2$ is considered for the analysis of the M-Estimator. Therefore, the criterion in (46) is fully preserved, and the reconstruction of N is possible without necessarily choosing the best reference remainder. Note that there is no guarantee the value of $\hat{N}$ that minimizes (23) or (24) reproduces the real value of N. However, the value of N is necessarily in the vicinity of at least one entry of the vector $\mathbf{p}$, which informs the cardinalities of the mapping vector $\mathbf{v}$ in accordance with the line 18 in Algorithm 3.

4. Experiments and results

In this section, we first develop an example with an undersampling system in subsection 4.1. In subsection 4.2, results of general simulations are presented for the case of $\sigma_1 = \sigma_2 = \cdots = \sigma_L$ and, in sequel, for the case of $\sigma_i = \mu\Gamma_i$, for $i \in \{1, 2, \ldots, L\}$. In subsection 4.3, we present a comparison of the computational cost of CFR-CRT, MLE-CRT and the proposed KME-CRT.

4.1. System validation – example

In a system with $L = 3$ sensors, the sampling frequencies are $M_i \in \{55\text{ kHz}, 65\text{ kHz}, 85\text{ kHz}\}$. The impinging frequency value N is any real number within the dynamic range, $0 < N < 12.1550$ MHz, and must be estimated. Each sensor reads the peaks in the DFT of the frequency N, whose values are $r_i \in \{17.81\text{ kHz}, 15.45\text{ kHz}, 13.24\text{ kHz}\}$, yielding the system

$$\begin{cases} N \bmod 55 = 17.81, \\ N \bmod 65 = 15.45, \\ N \bmod 85 = 13.24. \end{cases} \tag{47}$$

Prior to further steps, proceed to the division of the original system as in (47) by M, the GCD of all moduli M_i. In (47), $M = 5$, yielding

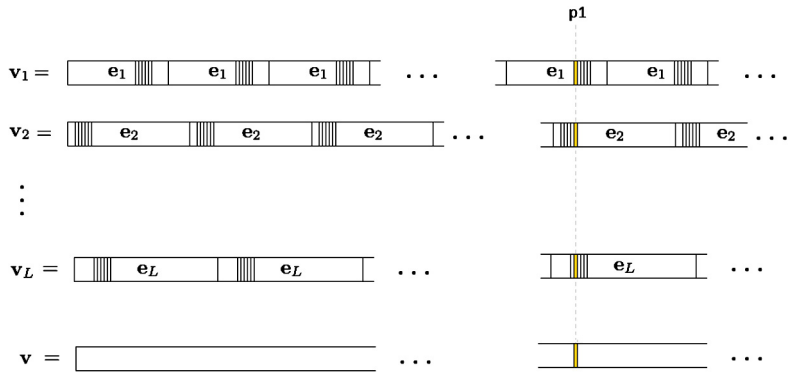

Fig. 10. Assemblage of vectors $\mathbf{c}_i$. Only a restricted set of entries in $\mathbf{v}$ are to be tested with the M-Estimator. In this example, the intersection of all entries of the same cardinality with value 1 is indicated in yellow. Note that there are many intersections of this type throughout the vector $\mathbf{v}$, while in this Figure only the first one, p_1, is shown.

$$\begin{cases} N_m \bmod 11 = 3.562, \\ N_m \bmod 13 = 3.09, \\ N_m \bmod 17 = 2.648, \end{cases} \tag{48}$$

where $N_m = N/M$. Note that in (48) $M = 1$, and thus $M_i = \Gamma_i$, for $i \in \{1, 2, 3\}$.

We assemble vectors $e_1 \in \mathbb{Z}^{44}$, $e_2 \in \mathbb{Z}^{52}$ and $e_3 \in \mathbb{Z}^{68}$ with zeros in all entries. In sequel, we make $e_1(15) = 1$, $e_2(13) = 1$ and $e_3(11) = 1$, filling with value 1 also the following entries: $e_1(13) = e_1(14) = e_1(16) = e_1(17) = 1$, $e_2(11) = e_2(12) = e_2(14) = e_2(15) = 1$ and $e_3(9) = e_3(10) = e_3(12) = e_3(13) = 1$. Such steps correspond to lines 4–13 of Algorithm 3. By this moment, we have the definitive e_i, for $i \in \{1, 2, 3\}$.

We set up the mapping vector $\mathbf{v} \in \mathbb{Z}^{9724}$ with zero in all entries. For $i \in \{1, 2, 3\}$, we organize the vectors $\mathbf{v}_1$ in (49), $\mathbf{v}_2$ in (50) and $\mathbf{v}_3$ in (51),

$$\mathbf{v}_1 = \mathbf{u}_{13} \otimes \mathbf{u}_{17} \otimes \mathbf{e}_1, \tag{49}$$

$$\mathbf{v}_2 = \mathbf{u}_{11} \otimes \mathbf{u}_{17} \otimes \mathbf{e}_2, \tag{50}$$

$$\mathbf{v}_3 = \mathbf{u}_{11} \otimes \mathbf{u}_{13} \otimes \mathbf{e}_3, \tag{51}$$

where $\mathbf{u}_k$ is defined as in (32).

We now apply (36) in order to obtain mapping vector $\mathbf{v}$ in accordance with the lines 18–22 of Algorithm 3. With line 23, we extract the cardinality of such entries in $\mathbf{v}$, which returns the following vector $\mathbf{p} \in \mathbb{Z}^8$ in (52),

$$\mathbf{p}' = \begin{bmatrix} 13 & 895 & 896 & 897 & 6877 & 6878 & 6879 & 7761 \end{bmatrix}. \tag{52}$$

Line 25 of Algorithm 3 converts $\mathbf{p}$ of (52) into

$$\mathbf{p}' = \begin{bmatrix} 3 & 223.5 & 223.75 & 224 & 1719 & 1719.25 & 1719.5 & 1940 \end{bmatrix}. \tag{53}$$

We choose $s_i = 0.02$, thus avoiding that any final estimated $\hat{N}$ lie further than 0.01 from the optimal point. The determination of the optimized value of s_i is beyond the scope of this paper, but it suffices to note that infinite other values of s_i are possible. Clearly, the smaller the s_i, the higher the accuracy, but also the computational cost, since smaller s_i entails more values to test in each selected slot. On the other hand, shortening the interval 1/4 yields more resultant cells of test, yet of smaller length. All in all, we have in the choice of the length (in our case, 1/4) and incremental step s_i two tuning parameters that aid us to control the complexity of our system. We then set the matrix $\mathbf{Q} \in \mathbb{R}^{13\times 8}$, whose values are shown in (54). The first row of $\mathbf{Q}$ is $\mathbf{p}'$ in (53).

$$\mathbf{Q} = \begin{bmatrix} 3.00 & 223.50 & 223.75 & 224.00 & 1719.00 & 1719.25 & 1719.50 & 1940.00 \\ 3.02 & 223.52 & 223.77 & 224.02 & 1719.02 & 1719.27 & 1719.52 & 1940.02 \\ 3.04 & 223.54 & 223.79 & 224.04 & 1719.04 & 1719.29 & 1719.54 & 1940.04 \\ 3.06 & 223.56 & 223.81 & 224.06 & 1719.06 & 1719.31 & 1719.56 & 1940.06 \\ 3.08 & 223.58 & 223.83 & 224.08 & 1719.08 & 1719.33 & 1719.58 & 1940.08 \\ 3.10 & 223.60 & 223.85 & 224.10 & 1719.10 & 1719.35 & 1719.60 & 1940.10 \\ 3.12 & 223.62 & 223.87 & 224.12 & 1719.12 & 1719.37 & 1719.62 & 1940.12 \\ 3.14 & 223.64 & 223.89 & 224.14 & 1719.14 & 1719.39 & 1719.64 & 1940.14 \\ 3.16 & 223.66 & 223.91 & 224.16 & 1719.16 & 1719.41 & 1719.66 & 1940.16 \\ 3.18 & 223.68 & 223.93 & 224.18 & 1719.18 & 1719.43 & 1719.68 & 1940.18 \\ 3.20 & 223.70 & 223.95 & 224.20 & 1719.20 & 1719.45 & 1719.70 & 1940.20 \\ 3.22 & 223.72 & 223.97 & 224.22 & 1719.22 & 1719.47 & 1719.72 & 1940.22 \\ 3.24 & 223.74 & 223.99 & 224.24 & 1719.24 & 1719.49 & 1719.74 & 1940.24 \end{bmatrix} \tag{54}$$

We then calculate $\mathbf{W}$ according to the lines 29–40 of the Algorithm 3, entrywise in terms of $\mathbf{Q}$. Hence, given every entry $\mathbf{Q}(i, j)$, the entry $\mathbf{W}(i, j)$ informs the respective error, either according to (23) or (24).

As a last step, search the minimum absolute value in $\mathbf{W}$. Since this is $\mathbf{W}(2, 3) = 0.1605$ and $M = 5$, $\hat{N} = 5\mathbf{Q}(2, 3) = 5 \times 223.77 = 1118.85$, i.e., the estimated frequency value is $\hat{N} = 1118.85$ kHz. This value lies in the tolerance interval around the true value $N = 1120$ kHz, as $|N - \hat{N}| < M/2$. It is worth it to remark that the result of the same system given by CFR-CRT is $\hat{N} = 8597.2$ kHz and by MLE-CRT is $\hat{N} = 8597.1$ kHz, values significantly distant from the true N.

4.2. Results of experiments in terms of errors variance

Next, we compare the results of the proposed KME-CRT with the state-of-the-art CFR-CRT and MLE-CRT for the case of same and different variances of errors. This comparison is based on the fact that CFR-CRT is the state-of-the-art method for constant variances of the errors Δ_i, whereas MLE-CRT is suitable for different variances of Δ_i, $i \in \{1, 2, \ldots, L\}$.

In both scenarios, we also compare the proposed KME-CRT with the complete ME, which is the application of the ME routine over the entire dynamic range D without the help of the Kroenecker mapping vector. Hence, with the complete ME, the total number of iterations is D/s_i. This comparison is performed in order to make clear how effective is the proposed KME-CRT due to the Kroenecker product of the specified vectors.

The evaluation of the computational time required to perform the proposed KME-CRT, the CFR-CRT and the MLE-CRT is carried out in MATLAB by means of commands tic and toc, which are used to measure the time the computer takes to perform a sequence of commands. The processor used to undertake the measurements is a dual core i7-5500U at 2.4 GHz, with double precision in MATLAB settings. We do not employ parallel structures as the goal is to illustrate the total required computational effort. Nevertheless, we highlight that CFR-CRT and MLE-CRT can be deployed in parallel

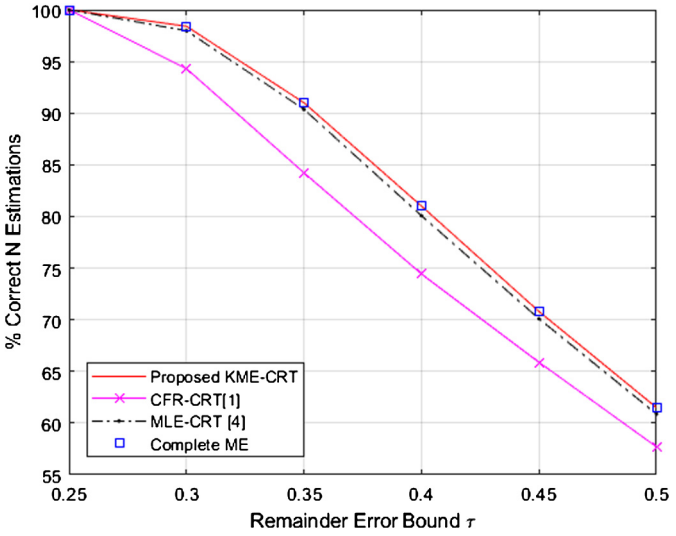

Fig. 11. Percentages of successful estimations of N with the proposed KME-CRT, the CFR-CRT [1], MLE-CRT [4] and complete ME for constant variances in the errors.

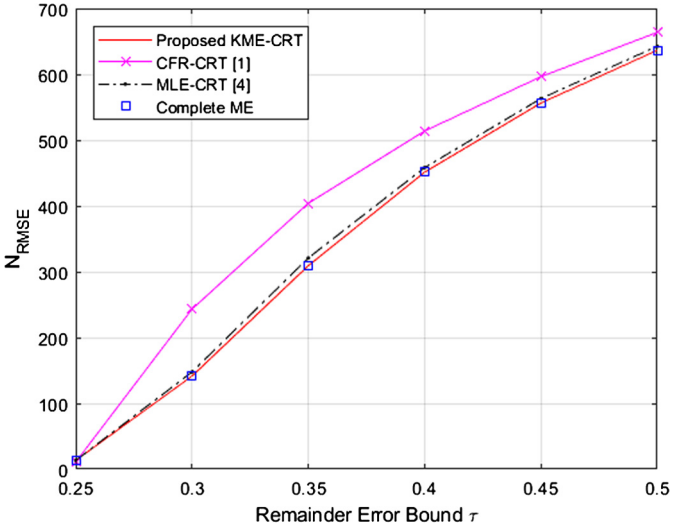

Fig. 12. N_{RMSE} values with the proposed KME-CRT, the CFR-CRT [1], MLE-CRT [4] and complete ME for constant variances in the errors.

Table 1
% of Correct $\hat{N}$ Estimation with 2 or 3 Remainders with Errors $M/4 \leq |\Delta_i| < M/2$ over 10^5 Realizations.

CRT method	2 remainders	3 remainders
Proposed KME-CRT	63.49%	8.01%
CFR-CRT	60.58%	7.41%
MLE-CRT	61.81%	7.41%

Table 2
Sets of moduli for the results shown in Fig. 15 for $\tau = 0.45$.

Set of moduli	Moduli of the CRT system
1	$M_i \in \{8, 11\}$
2	$M_i \in \{8, 11, 13\}$
3	$M_i \in \{8, 11, 13, 15\}$
4	$M_i \in \{8, 11, 13, 15, 17\}$

structures. The proposed KME-CRT can be executed in a parallel fashion with regards to the vectors assemblage of (49)–(51) and in testing each value of matrix **Q**. However, since several possible arrangements are possible which depend on the number of processors available, for the sake of simplicity we execute all routines sequentially.

In our simulations, the moduli are $\Gamma_i \in \{11, 13, 17\}$. Recall that, if $M \neq 1$, the previous normalization with regards to M is assumed. Errors Δ_i are generated under the Gaussian distribution in the range $[N - \tau, N + \tau]$ for each value of τ. At each iteration, a real valued N with two decimals is randomly chosen from 0 up to $D = 2431$ over 10^5 iterations. The estimation is accepted as correct when $N - M/2 \leq \hat{N} \leq N + M/2$.

In Fig. 11, the percentages of correct estimation of N are shown for constant variances for the proposed KME-CRT, CFR-CRT [1], MLE-CRT [4] and the complete ME. Throughout the values of τ, the percentages of correct calculations of N are higher with the proposed KME-CRT than with CFR-CRT or MLE-CRT. The results are shown for $\tau \in \{0.25, 0.30, 0.35, 0.40, 0.45, 0.50\}$ since for $\tau \in \{0.05, 0.10, 0.15, 0.20\}$ the correct estimation is 100% for all the three compared methods.

Defining the root mean squared error of N as

$$N_{\text{RMSE}} = \sqrt{\text{E}\{|\hat{N} - N|^2\}}, \tag{55}$$

Fig. 12 shows the results of N_{RMSE} for the proposed KME-CRT, CFR-CRT, MLE-CRT and the complete ME. The smallest values of N_{RMSE} are in the proposed KME-CRT and complete ME results, even considering the interval where the limit $\tau < M/4$ is observed, i.e., $\tau \in \{0.05, 0.10, 0.15, 0.20, 0.25\}$.

When all variances are presumably equal, Table 1 informs the percentage of correct estimation of N in the case of two or three moduli with error Δ_i that are in the range $M/4 \leq |\Delta_i| < M/2$. The results are derived from 10^5 realizations.

The same analysis is repeated, now focusing on the case of $\sigma_i \neq \sigma_j$, for $i, j \in \{1, 2, \ldots, L\}, i \neq j$, and establishing $\sigma_i = \tau M_i$. In Fig. 13(a), percentages of successful estimations of N with the proposed KME-CRT, the CFR-CRT [1], MLE-CRT [4] and complete ME for different σ_i^2, with $i \in \{1, 2, \ldots, L\}$. In 13(b), the values around $\tau = 0.3$ in different scale. Throughout the values of τ, the percentages of correct calculations of N are higher with the proposed KME-CRT than with CFR-CRT or MLE-CRT. However, the results of the proposed KME-CRT and the MLE-CRT present significant proximity.

Fig. 14 shows the evolution of N_{RMSE} values obtained via (55) for the proposed KME-CRT, CFR-CRT, MLE-CRT and the complete ME. The smallest values of N_{RMSE} are in the proposed KME-CRT and complete ME results. Note that once more the results of the proposed KME-CRT and MLE-CRT are very similar.

We have also tested the performance of the methods for different sets of moduli through 10^4 iterations with different variances in errors considering only the case $\tau = 0.45$. Table 2 shows the sets of moduli, which are analogous to sensors sampling rates if the CRT system is applied to undersampling systems.

Finally, we monitor the disparity between the performances of the proposed KME-CRT and complete ME. At each of the 10^5 realizations, we count the times in which the proposed KME-CRT returns a successful estimation but the complete ME does not, and vice versa, summing it to each entry corresponding to each value of τ. Over 10^5 realizations, and in each $\tau \in \{0.25, 0.30, 0.35, 0.40, 0.45, 0.50\}$, it is possible to conclude that the proposed KME-CRT and complete ME have the identical performance for practical applications. As a consequence, the proposed KME-CRT provides an optimized version of complete ME.

4.3. Computational cost

The comparison of computational cost of the proposed KME, the CFR-CRT and the MLE-CRT comprises the following cases: Case 1 with $M_i \in \{7, 11\}$, Case 2 with $M_i \in \{7, 11, 13\}$, Case 3 with $M_i \in \{7, 11, 13, 15\}$, Case 4 with $M_i \in \{7, 11, 13, 15, 17\}$, and Case 5

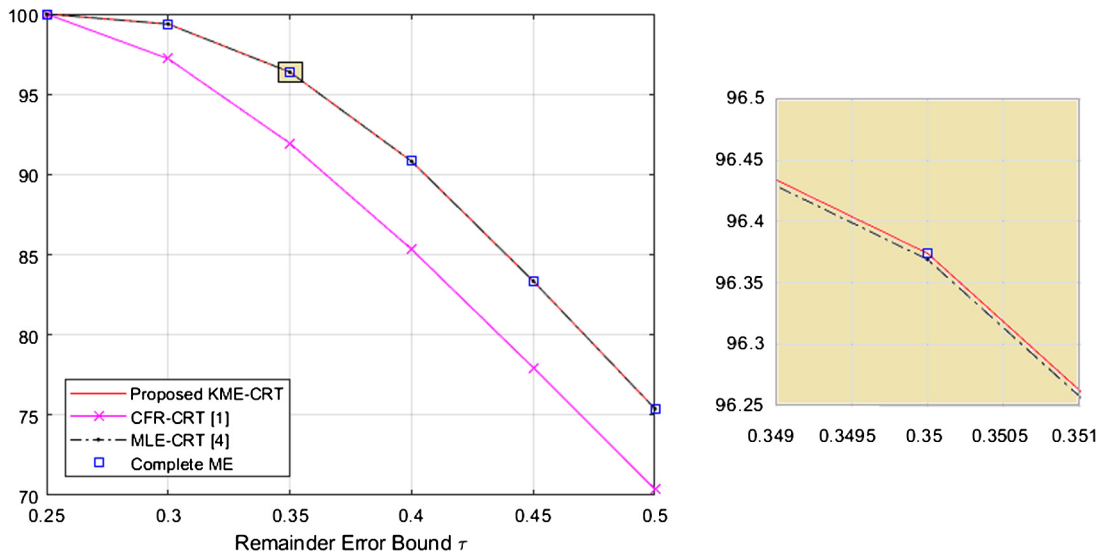

Fig. 13. In (a), percentages of successful estimations of N with the proposed KME-CRT, the CFR-CRT [1], MLE-CRT [4] and complete ME for different σ_i^2, with $i \in \{1, 2, \ldots, L\}$. In (b), the values around $\tau = 0.3$ in different scale.

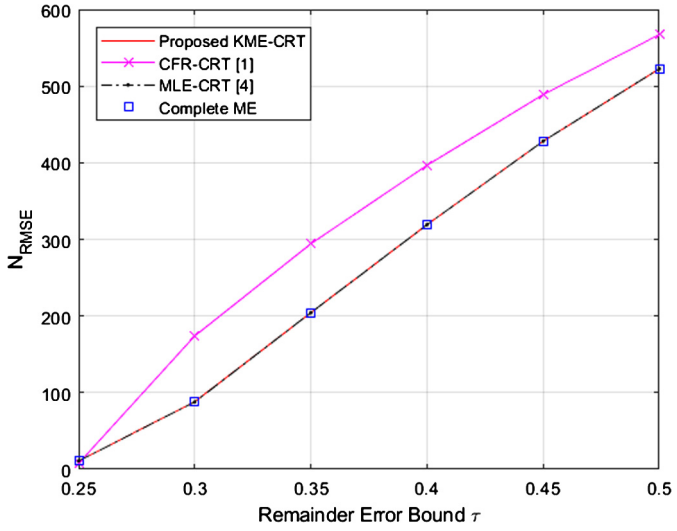

Fig. 14. N_{RMSE} values with the proposed KME-CRT, the CFR-CRT [1], MLE-CRT [4] and complete ME for different σ_i^2, with $i \in \{1, 2, \ldots, L\}$.

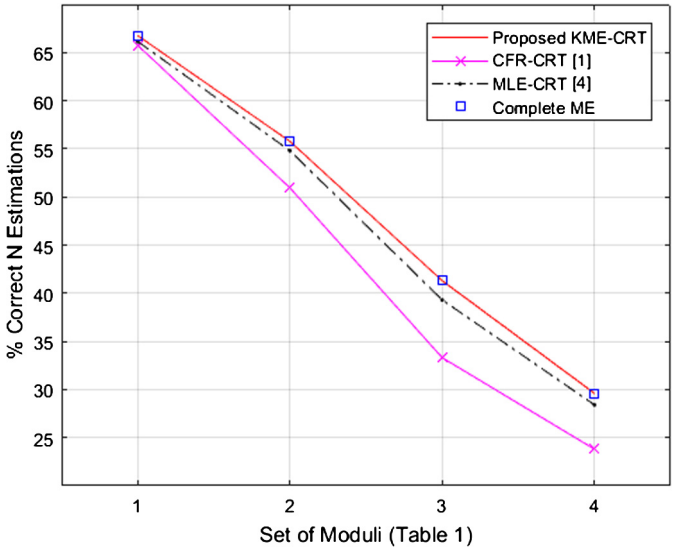

Fig. 15. % of Correct Estimations with the CFR-CRT [1], MLE-CRT [4], the proposed KME-CRT and complete ME for the sets of moduli shown in Table 2 with $\tau = 0.45$.

with $M_i \in \{7, 11, 13, 15, 17, 19\}$. In each case, the time of computational processing is taken as the mean of 10^3 realizations. In sequel, we highlight the reduction of computational effort of the proposed KME-CRT in terms of complete ME. All premises adopted in Subsection 4.2 with regards to time measurements are maintained, such as avoiding parallel settings and the MATLAB commands used.

Table 3 shows the time of computational processing in milliseconds (ms) for each case. The incremental step of the proposed KME-CRT is kept as $s_i = 0.02$. The time of processing for the proposed KME-CRT increases significantly with the addition of further values in M_i as all $\mathbf{c}_i \in \mathbb{Z}^{4D}$, i.e., vectors $\mathbf{c}_i$ have the length of the dynamic range. Due to this fact, KME-CRT is supposed to be suitable for systems with low number of sensors. Table 3 also includes the average time processing of tensorial version of the proposed KME-CRT for comparison.

Sets of few moduli are frequently encountered in the literature, as for instance in simulations where $L = 2$ as in [2,6,35,44], $L = 3$, as in [9,12,38,45,46], and $L = 4$ as in [5]. Even in [1], L assumes different values, from 3 up to 12, hence starting with low values. The case of few remainders is thus a matter of attention in the state-of-the-art, which is the most indicated case of application for the proposed KME-CRT. One can also notice that the proposed tensorial version of the KME-CRT has a lower computational time than the purely vectorial form in the cases $L = 4$ and $L = 5$, i.e., for greater values of L.

In comparison with the complete ME, however, the proposed KME-CRT shows great capability of computational economy as shown in Table 4, where the number of rows filtered by the proposed KME-CRT and the respective reduction of computational effort are shown. The economy in comparison with complete ME is based on the fraction of the filtered rows in relation to the complete number of rows $4D$ in $\mathbf{v}$.

For instance, in case 4, $\mathbf{v} \in \mathbb{Z}^{1021020}$, but at maximum 35 rows of $\mathbf{v}$ can have 1 as value. This filtering reduces the computational effort to $35/1021020 = 0.00343\%$ of the undertaken by complete ME. Nevertheless, the result that the proposed KME-CRT delivers is the same of the complete ME, as shown in subsection 4.2.

5. Conclusion

In this paper a novel method for estimating a real number using the CRT was presented. The method is based on an ME scheme

Table 3
Time of computational processing in milliseconds (ms) averaged over 1000 realizations.

Moduli set	Proposed KME	Proposed tensor-KME	CFR	MLE	ME
1: {7, 11}	0.124	65.2	0.128	0.0787	0.496
2: {7, 11, 13}	1.3	69.3	0.152	0.0868	8.7
3: {7, 11, 13, 15}	21.2	65.5	0.167	0.0898	179.4
4: {7, 11, 13, 15, 17}	430.2	159.7	0.291	0.157	4259.1
5: {7, 11, 13, 15, 17, 19}	9966.6	2515.9	4.2	0.615	109508.4

Table 4
Reduction of computational effort in terms of rows – Proposed KME-CRT and complete ME.

Case	Proposed KME-CRT – rows of test	Economy – complete ME
1: $M_i \in \{7, 11\}$	7	97.7272%
2: $M_i \in \{7, 11, 13\}$	11	99.7352%
3: $M_i \in \{7, 11, 13, 15\}$	19	99.9684%
4: $M_i \in \{7, 11, 13, 15, 17\}$	35	99.9965%
5: $M_i \in \{7, 11, 13, 15, 17, 19\}$	67	99.9996%

that is optimized by means of a mapping vector that indicates in which parts of the dynamic range the search for the real number should occur. This mapping vector is assembled via tensorial operations, i.e., Kroenecker product of previously defined vectors. We also provide a version of the mapping vectors based on tensorial n-mode products, delivering in the end the same information of the original method. For its characteristics, it is suitable overall for CRT systems with few moduli, which in the case of sensors networks corresponds to low quantity of sensors.

In our proposal, the errors in the remainders of CRT system may have the same or different variances, allowing our work to be compared with state-of-the-art methods CFR-CRT [1] and MLE-CRT [4]. According to results tested over 10^5 iterations, in the case of equal variances, the proposed KME-CRT is consistently superior to the state-of-the-art methods in terms of percentage of correct estimations. On the other hand, with regards to the case of different variances, the superiority of our proposal is comparatively small, not outperforming the state-of-the-art MLE-CRT significantly. Hence, in this particular, both methods can be considered as of equivalent performances. However, for all that was shown, our proposed technique enhances the probability of estimating an unknown number accurately even when the errors in the remainders surpass 1/4 of the greatest common divisor of all moduli. A drawback is that, as shown in Table 3, the computational cost of the proposed KME-CRT increases more than linearly and surpasses the costs of CFR-CRT and MLE-CRT in certain scenarios.

The proposed KME-CRT was also compared with the complete ME, which by definition cannot be outperformed. KME-CRT has the same results of complete ME, while reduces their necessary computational effort in at least 97%, thus offering a decisive advantage in terms of computational effort.

For future works, we envisage the need for optimization of the mapping vector as a searching method. Furthermore, errors with distributions different from the Gaussian one should be investigated. Tensor based mapping vector routines of Algorithms 3 and 5 are still under development and are also a matter of concern for future studies. In terms of CRT techniques, the possibility of applying the mapping vector to the Multi-Stage Robust CRT and studies involving CRT in a probabilistic way, as in the case of unrestricted errors of [32], are also supposed to have a good applicability towards the technique proposed here.

Conflict of interest statement

The Authors declare no conflict of interest of any type or nature.

Acknowledgments

The Authors acknowledge the Brazilian Electricity Regulatory Agency (A-gência Nacional de Energia Elétrica – ANEEL), whose support enabled the completion of this work, and the Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) for the scholarship under the process n. 290145/2015-5.

References

[1] W. Wang, X.-G. Xia, A closed-form robust Chinese Remainder Theorem and its performance analysis, IEEE Trans. Signal Process. 58 (11) (2010) 5655–5666.
[2] X. Li, H. Liang, X.-G. Xia, A robust Chinese Remainder Theorem with its applications in frequency estimation from undersampled waveforms, IEEE Trans. Signal Process. 57 (11) (2009) 4314–4322.
[3] W. Wang, X. Li, X.-G. Xia, An ML estimation based robust Chinese Remainder Theorem for reals, in: 2015 IEEE China Summit and International Conference on Signal and Information Processing, ChinaSIP, 2015, pp. 363–367.
[4] W. Wang, X. Li, Wei Wang, X.-G. Xia, Maximum likelihood estimation based robust Chinese Remainder Theorem for real numbers and its fast algorithm, IEEE Trans. Signal Process. 63 (13) (2015) 3317–3331.
[5] L. Xiao, X.-G. Xia, A new robust Chinese Remainder Theorem with improved performance in frequency estimation from undersampled waveforms, Signal Process. 117 (2015) 242–246.
[6] H. Liang, H. Zhang, N. Jia, A generalized robust Chinese Remainder Theorem for multiple numbers and its application in multiple frequency estimation with low sampling rates, in: IEEE International Conference on Signal Processing, Communications and Computing, ICSPCC, 2011, pp. 1–4.
[7] Z. Jiang, J. Wang, Q. Song, Z. Zhou, A closed-form robust Chinese Remainder Theorem based multibaseline phase unwrapping, in: International Conference on Circuits, Devices and Systems, ICCDS, 2017, pp. 115–119.
[8] L. Xiao, X.-G. Xia, W. Wang, Multi-stage robust Chinese Remainder Theorem, IEEE Trans. Signal Process. 62 (18) (2014) 4772–4785.
[9] X. Li, X.-G. Xia, W. Wang, Wei Wang, A robust generalized Chinese Remainder Theorem for two integers, IEEE Trans. Inf. Theory 62 (12) (December 2016) 7491–7504.
[10] X.-G. Xia, On estimation of multiple frequencies in undersampled complex valued waveforms, IEEE Trans. Signal Process. 47 (12) (December 1999).
[11] G. Hill, The benefits of undersampling, Electron. Des. (1994) 69–79.
[12] H. Xiao, G. Xiao, Notes on CRT-based robust frequency estimation, Signal Process. 133 (2017) 13–17.
[13] L. Xiao, X.-G. Xia, Frequency determination from truly sub-Nyquist samplers based on robust Chinese Remainder Theorem, Signal Process. 150 (2018) 248–258.
[14] A. Koochakzadeh, P. Pal, On the robustness of co-prime sampling, in: 23rd European Signal Processing Conference, EUSIPCO, 2015, pp. 2825–2829.
[15] P.P. Vaidyanathan, P. Pal, Sparse sensing with co-prime samplers and arrays, IEEE Trans. Signal Process. 59 (2) (2011).
[16] X.-G. Xia, K. Liu, A generalized Chinese Remainder Theorem for residue sets with errors and its application in frequency determination from multiple sensors with low sampling rates, IEEE Signal Process. Lett. 12 (11) (November 2005) 768–771.
[17] Piya Pal, P.P. Vaidyanathan, Coprime sampling and the music algorithm, in: IEEE Digital Signal Processing and Signal Processing Education Meeting, DSP/SPE, 2011, pp. 289–294.

[18] X. Huang, Y. Han, Z. Yan, H. Xian, W. Lu, Resolution doubled co-prime spectral analyzers for removing spurious peaks, IEEE Trans. Signal Process. 64 (10) (2016) 2489–2498.
[19] T. Moon, H.W. Choi, N. Tzou, A. Chatterjee, Wideband sparse signal acquisition with dual-rate time-interleaved undersampling hardware and multicoset signal reconstruction algorithms, IEEE Trans. Signal Process. 63 (24) (2015) 6486–6497.
[20] L. Ding, Y. Ye, G. Ye, X. Wang, Y. Zhu, Bistatic synthetic aperture radar with undersampling for terahertz 2-D near-field imaging, IEEE Trans. Terahertz Sci. Technol. 8 (2) (2018) 174–182.
[21] Z.Y. Peng, L. Xia, W. Qiang, Asymmetric cryptography algorithm with Chinese Remainder Theorem, in: 2011 IEEE 3rd International Conference on Communication Software and Networks, 2011, pp. 450–454.
[22] X. Shen, Y. Jia, J. Wang, L. Zhang, New families of balanced quaternary sequences of even period with three-level optimal autocorrelation, IEEE Commun. Lett. 21 (10) (2017) 2146–2149.
[23] K. Kaya, A.A. Selçuk, Sharing DSS by the Chinese Remainder Theorem, J. Comput. Appl. Math. 259 (2014) 495–502.
[24] P.W. Adi, Y.P. Astuti, E.R. Subhiyakto, Imperceptible image watermarking based on Chinese Remainder Theorem over the edges, in: IEEE 4th International Conference on Electrical Engineering, Computer Science and Informatics, EECSI, September 2017, pp. 1–5.
[25] S.K. Singh, V.P. Gopi, P. Palanisamy, Image security using DES and RNS with reversible watermarking, in: 2014 International Conference on Electronics and Communication Systems, ICECS, 2014, pp. 1–5.
[26] N. Singh, A.N. Tentu, A. Basit, V.Ch. Venkaiah, Sequential secret sharing scheme based on Chinese Remainder Theorem, in: 2016 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC, 2016, pp. 1–6.
[27] L. Harn, M. Fuyou, Multilevel threshold secret sharing based on the Chinese Remainder Theorem, Inf. Process. Lett. 114 (2014) 504–509.
[28] S. Iftene, General secret sharing based on the Chinese Remainder Theorem with applications in E-voting, Electron. Notes Theor. Comput. Sci. 186 (2007) 67–84.
[29] J.-P. Sheu, J.-J. Lin, A multi-radio rendezvous algorithm based on Chinese Remainder Theorem in heterogeneous cognitive radio networks, IEEE Trans. Mob. Comput. 99 (2018) 1, https://doi.org/10.1109/TMC.2018.2790408.
[30] L. Xiao, X.-G. Xia, Robust polynomial reconstruction via Chinese Remainder Theorem in the presence of small degree residue errors, IEEE Trans. Circuits Syst. II, Express Briefs 99 (2017) 1, https://doi.org/10.1109/TCSII.2017.2756343.
[31] L. Xiao, X.-G. Xia, Minimum degree-weighted distance decoding for polynomial residue codes with non-coprime moduli, IEEE Wirel. Commun. Lett. 6 (4) (2017) 558–561.
[32] L. Xiao, X.-G. Xia, Error correction in polynomial remainder codes with non-pairwise coprime moduli and robust Chinese Remainder Theorem for polynomials, IEEE Trans. Commun. 63 (3) (2015) 605–616.
[33] G.C. Cardarilli, L. Di Nunzio, R. Fazzolari, L. Gerardi, M. Re, G. Campolo, D. Cascone, A new electric encoder position estimator based on the Chinese Remainder Theorem for the CMG performance improvements, in: 2017 IEEE International Symposium on Circuits and Systems, ISCAS, 2017, pp. 1–4.
[34] X. Li, W. Wang, W. Zhang, Y. Cao, Phase-detection-based range estimation with robust Chinese Remainder Theorem, IEEE Trans. Veh. Technol. 65 (12) (2016) 10132–10137.
[35] H. Liang, X. Li, X.-G. Xia, Adaptive frequency estimation with low sampling rates based on robust Chinese Remainder Theorem and IIR notch filter, in: 4th IEEE Conference on Industrial Electronics and Applications, 2009, pp. 2999–3004.
[36] K. Schaecke, On the Kroenecker product, CiteSeer, August 2004.
[37] G. Xu, On solving a generalized Chinese Remainder Theorem in the presence of remainder errors, https://arxiv.org/abs/1409.0121, 2014.
[38] Wei Wang, X. Li, X.-G. Xia, W. Wang, The largest dynamic range of a generalized Chinese Remainder Theorem for two integers, IEEE Signal Process. Lett. 22 (2) (February 2015) 254–258.
[39] H. Liao, X.-G. Xia, A sharpened dynamic range of a generalized Chinese Remainder Theorem for multiple integers, IEEE Trans. Inf. Theory 53 (1) (January 2007) 428–433.
[40] G. Davida, B. Litow, G. Xu, Fast arithmetics using Chinese remaindering, Inf. Process. Lett. 109 (2009) 660–662.
[41] J. Grossschadl, The Chinese Remainder Theorem and its application in a high-speed RSA crypto chip, in: Proceedings 16th Annual Computer Security Applications Conference, ACSAC'00, August 2002.
[42] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
[43] T.G. Kolda, B.W. Bader, Tensor Decompositions and Applications, Sandia National Laboratories, SAND2007-6702, 2007.
[44] L. Xiao, X.-G. Xia, H. Huo, Towards robustness in residue number systems, IEEE Trans. Signal Process. 65 (6) (2016) 1497–1510.
[45] E. Lin, L. Monte, Joint frequency and angle of arrival estimation using the Chinese Remainder Theorem, in: IEEE Radar Conference, RadarConf, 2017, pp. 1547–1551.
[46] G. Zhou, X.-G. Xia, Multiple frequency detection in undersampled complex-valued waveforms with close multiple frequencies, Electron. Lett. 33 (15) (1997) 1294–1295.

Jayme Milanezi Junior received the Diploma degree in electrical engineering in 2004 from the Military Institute of Engineering (IME) in Rio de Janeiro, Brazil. He received his Master of Science degree in electrical engineering in 2013 from the University of Brasilia (UnB). In 2014, he joined the Doctoral Program of UnB in "Co-tutelle de thèse" with the Ilmenau University of Technology (TU Ilmenau) in Germany. Currently he is also one of the Regulatory Specialists who work in the Brazilian Electricity Regulatory Agency (ANEEL). Among his duties there is the technical evaluation of R&D projects that are submitted by Brazilian companies of the electrical sector. In parallel, he is also author of three patent pending applications in the Brazilian Patent Office (INPI). His current research interests include energy harvesting sources, Smart Grid privacy protection systems and signal processing tools, specially including the Chinese Remainder Theorem and multidimensional applications.

João Paulo Carvalho Lustosa da Costa received the Diploma degree in electronic engineering in 2003 from the Military Institute of Engineering (IME) in Rio de Janeiro, Brazil, his M.Sc. degree in telecommunications in 2006 from University of Brasília (UnB) in Brazil, and his Doktor-Ingenieur (Ph.D.) degree in electrical and information engineering in 2010 at Ilmenau University of Technology (TU Ilmenau) in Germany. Since 2010, he coordinates the Laboratory of Array Signal Processing (LASP) and, from 2012 to 2014, he worked as a senior researcher at the Ministry of Planning in projects related to Business Intelligence. He was a visiting scholar at University Erlangen-Nuremberg (FAU), at Munich Technical University (TUM), at Seville University (US), at Harvard University, at TU Ilmenau and at Fraunhofer Institute for Integrated Circuits IIS. From 2014 to 2017, he coordinated a special visiting researcher (PVE) project related to satellite communication and navigation together with the German Aerospace Center (DLR) supported by the Brazilian government and he served as senior researcher of a distance learning (DL) project in cooperation with the National School of Public Administration (Enap). He has been named an IEEE Senior Member in 2015. He obtained five best paper awards on the following conferences: 19th International Conference on OFDM and Frequency (ICOF), IV IEEE International Conference on Ultra Modern Telecommunications and Control Systems (ICUMT'12), ICoFCS'12, ICoFCS'13 and ICoFCS'15. Currently he is an associate professor at UnB and an associate researcher at TU Ilmenau, since 2014, he has been twice awarded as a productivity researcher level 2 by the Brazilian National Council for Scientific and Technological Development (CNPq) [303343/2017-6], and since 2018 he coordinates a governmental data analysis project in cooperation with Enap.

Florian Römer (S'04-M'13-SM'16) studied computer engineering at the Ilmenau University of Technology, Germany, and McMaster University, Hamilton, ON, Canada. He received the Diplom-Ingenieur degree in communications engineering and the doctoral (Dr.-Ing.) degree in electrical engineering from the Ilmenau University of Technology in October 2006 and October 2012, respectively. From December 2006 until September 2012, he has been a Research Assistant in the Communications Research Laboratory at Ilmenau University of Technology. In October 2012 he has joined the Digital Broadcasting Research Group, a joint research activity between the Fraunhofer Institute for Integrated Circuits IIS and Ilmenau University of Technology, as a postdoctoral research fellow. In January 2018 he joined the Fraunhofer Institute for Nondestructive Testing IZFP where he is leading the SigMaSense group with a research focus on innovative sensing and signal processing for material diagnostics and nondestructive testing. Mr. Römer received the Siemens Communications Academic Award for his diploma thesis in 2006 and the EURASIP best dissertation award in 2016 for his dissertation. He has also served as a member of the organizing committee of the 19-th International Workshop on Smart Antennas (WSA) 2015 in Ilmenau, Germany, as well as the IEEE Statistical Signal Processing Workshop (SSP) 2018 in Freiburg, Germany. Since 2018, he is a member of the Special Area Team (SAT) "Signal Processing for Multisensor Systems" of the Euopean Association for Signal Processing EURASIP.

Ricardo Kehrle Miranda received the Diploma degree in telecommunications engineering in 2010 and the M.Sc. degree in electronic and automation systems in 2013 both from the University of Brasília (UnB), Brazil. He holds a double Ph.D. degree at both the UnB and TU Ilmenau

in March 2017. During his Ph.D. he was a visiting student at the German Aerospace Center (DLR) and an intern in the microsatellite industry. Currently, he is a Postdoctoral researcher at the University of Brasília. His research focuses on array signal processing and tensor-based techniques.

Marco Antonio Marques Marinho received the B.Eng. degree in Network Engineering in 2012 from the University of Brasília (UnB). He received his M.Sc. degree in Electrical Engineering from the University of Brasília in cooperation with the Institute of Communications and Navigation of the German Aerospace Center in 2013, where he was a research fellow from 2014 to 2016. In 2018 he received his joint Ph.D. from the University of Brasília and Halmstad University. His research interests are in the field of array signal processing.

Giovanni Del Galdo studied telecommunications engineering at Politecnico di Milano. In 2007 he received his doctoral degree from Technische Universität Ilmenau on the topic of MIMO channel modeling for mobile communications. He then joined Fraunhofer Institute for Integrated Circuits IIS working on audio watermarking and parametric representations of spatial sound. Since 2012 he leads a joint research group composed of a department at Fraunhofer IIS and, as a full professor, a chair at TU Ilmenau on the research area of electronic measurements and signal processing. His current research interests include the analysis, modeling, and manipulation of multi-dimensional signals, over-the-air testing for terrestrial and satellite communication systems, and sparsity promoting reconstruction methods.