ACKNOWLEDGMENT

The authors wish to thank the reviewers for their helpful suggestions.

REFERENCES

[1] J. Proakis, *Digital Communications*. New York: McGraw-Hill, 2001.
[2] S. A. Al-Semari and T. E. Fuja, "I-Q TCM: Reliable communication over the Rayleigh fading channel close to the cutoff rate," *IEEE Trans. Inf. Theory*, vol. 43, pp. 250–262, Jan. 1997.
[3] X. Giraud, "Algebraic tools to build modulation schemes for fading channels," *IEEE Trans. Inf. Theory*, vol. 43, pp. 938–952, May 1997.
[4] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo, "New algebraic constructions of rotated z^n -lattice constellations for the Rayleigh fading channel," *IEEE Trans. Inf. Theory*, vol. 50, pp. 702–714, Apr. 2004.
[5] D. Rainish, "Diversity transform for fading channels," *IEEE Trans. Commun.*, vol. 44, pp. 1653–1661, Dec. 1996.
[6] J. Boutros, E. Viterbo, C. Rastello, and J. C. Belfiore, "Good lattice constellations for both Rayleight fading and Gaussian channels," *IEEE Trans. Inf. Theory*, pp. 502–518, Mar. 1996.
[7] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*. New York: McGraw-Hill, 1991.
[8] C. Schlegel and J. D. J. Costello, "Bandwidth efficient coding for fading channels: Code construction and performance analysis," *IEEE J. Sel. Areas Commun.*, vol. 7, pp. 1356–1368, Dec. 1989.
[9] G. Caire and S. Shamai, "On the capacity of some channels with channel state information," *IEEE Trans. Inf. Theory*, vol. 45, pp. 2007–2019, Sep. 1999.
[10] G. Caire, G. Taricco, and E. Biglieri, "Bit-interleaved coded modulation," *IEEE Trans. Inf. Theory*, pp. 927–946, May 1998.
[11] A. Vardy and Y. Be'ery, "More efficient soft-decision decoding of the Golay codes," *IEEE Trans. Inf. Theory*, vol. 37, pp. 667–672, May 1991.

A Sharpened Dynamic Range of a Generalized Chinese Remainder Theorem for Multiple Integers

Huiyong Liao and Xiang-Gen Xia, *Senior Member, IEEE*

***Abstract*—A generalized Chinese remainder theorem (CRT) for multiple integers from residue sets has been studied recently, where the remainders in a residue set are not ordered. In this correspondence, we first propose a majority method and then based on the proposed majority method we present a sharpened dynamic range of multiple integers that can be uniquely determined from their residue sets.**

***Index Terms*—Chinese remainder theorem (CRT), frequency determination from multiple undersampled waveforms, phase unwrapping, residue sets, sensor networks.**

I. INTRODUCTION

Chinese remainder theorem (CRT) has applications in many areas, such as computing, coding and cryptography, such as RSA-CRT and secret sharing, [8] and digital signal processing [7]. CRT gives a reconstruction of an integer from its remainders modulo several smaller integers. The uniqueness of the reconstruction is possible if and only if the integer is smaller than the least common multiple (lcm) of the moduli that is the product of the moduli when all the moduli are co-prime. There are several generalizations of CRT, see for example [8]. Recently, a different generalization of CRT has been presented in [1]–[3]. In this generalized CRT, multiple integers are determined from their residue sets modulo several smaller integers, where the remainders in a residue set are known as the remainders of the multiple integers modulo a smaller integer but the correspondence of the remainders and the multiple integers is not known, i.e., the correct order of the remainders in a residue set is not known. As an example, consider two integers 60 and 64 and four moduli $5, 7, 11, 13$. In this case, there are four residue sets from the two integers and the four moduli and they are $\{0, 4\}, \{1, 4\}, \{5, 9\}, \{8, 12\}$ corresponding to the four moduli $5, 7, 11, 13$, respectively. The problem is to uniquely determine the two integers from these four residue sets and four moduli, where the correspondence between the two integers and their remainders in a residue set is not specified, for example, in the second residue set $\{1, 4\}$, it is not known whether 1 is the remainder of the first unknown integer or the second unknown integer modulo 7. Clearly, if the two integers are too large, the solution may not be unique similar to the conventional CRT. The problem we are interested in is how large the two integers can be so that they can be uniquely determined from their four residue sets (nonordered), which is called *dynamic range* in this correspondence. In the conventional CRT for a single integer, it is the product of the four prime moduli, i.e., $5 \cdot 7 \cdot 11 \cdot 13 = 5005$.

Based on the table look-up method, a dynamic range for the unique determination of the multiple integers has been presented in [1], where *dynamic range* means a range of integers within which multiple integers can be uniquely determined from the residue sets and the moduli. The dynamic range presented in [1] is sharpened and maximized in [2] when an additional condition on the multiple integers is imposed. More detailed descriptions of the problem and these results are stated in Section II. The motivation of the study of the above problem, i.e., the generalized CRT in [1]–[3] is the determination of multiple frequencies from multiple undersampled waveforms that may occur in, for example, phase unwrapping in synthetic aperture radar (SAR) imaging of moving targets [4], polynomial phase signal detection [5], and sensor networks where sensors have low power and low functionality [6].

In this correspondence, we propose a majority method for multiple integer determination from their residue sets. We present a sharpened dynamic range over the one presented in [1] of the unique determination of multiple integers from their residue sets when no additional condition on these integers is required. We also show an example that the sharpened dynamic range is not the maximal one, which means that further improvement is still possible.

This correspondence is organized as follows. In Section II, we describe the mathematical problem and some necessary notations. In Section III, we present a majority method for the determination and a sharpened dynamic range for multiple integers. In Section IV, we conclude this correspondence.

II. MATHEMATICAL PROBLEM DESCRIPTION

Suppose we have a set of distinct positive integers $S = \{N_1, N_2, \ldots, N_\rho\}$ and a set of positive integers, $P = \{p_1, p_2, \ldots, p_\gamma\}$, which, without loss of generality, are assumed relative co-prime, i.e., any two of $p_r, 1 \leq r \leq \gamma$, are co-prime, and $0 < p_1 < p_2 < \cdots < p_\gamma$. The remainder (or residue) of N_l modulo p_r is

$$t_{l,r} \equiv N_l \bmod p_r \quad \text{for } 1 \leq l \leq \rho, \quad 1 \leq r \leq \gamma. \tag{1}$$

Manuscript received April 5, 2005; revised June 23, 2006. This work was supported in part by the Air Force Office of Scientific Research (AFOSR) under Grants F49620-02-1-0157 and FA9550-05-1-0161, and the National Science Foundation under Grants CCR-0097240 and CCR-0325180.

The authors are with the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716 USA (e-mail: liao@ee.udel.edu; xxia@ee.udel.edu).

Communicated by V. A. Vaishampayan, Associate Editor At Large.
Digital Object Identifier 10.1109/TIT.2006.887088

For $1 \le r \le \gamma$, define the residue set of S modulo p_r

$$S_r(N_1, N_2, \ldots, N_\rho) \triangleq \bigcup_{l=1}^{\rho} \{t_{l,r}\}. \tag{2}$$

Thus, we have γ residue sets $S_r(N_1, N_2, \ldots, N_\rho), 1 \le r \le \gamma$. For each residue set $S_r(N_1, N_2, \ldots, N_\rho), 1 \le r \le \gamma$, there may be multiple integers in S which share same residue, i.e., for each r, residues $t_{l,r}, l = 1, 2, \ldots, \rho$, may not be necessarily distinct. While all the distinct residues in each residue set $S_r(N_1, N_2, \ldots, N_\rho)$ are known, the number of repeatings of any residue $t_{l,r}$ is not known. For each $r, 1 \le r \le \gamma$, we arrange the distinct elements in $S_r(N_1, N_2, \ldots, N_\rho)$ in the following increasing order:

$$S_r(N_1, N_2, \ldots, N_\rho) = \{k_{l,r} : l = 1, 2, \ldots, \mu_r\} \tag{3}$$

where $k_{l,r} < k_{m,r}$ for $1 \le l < m \le \mu_r$ and μ_r is the number of distinct elements of $S_r(N_1, N_2, \ldots, N_\rho)$. We define an onto mapping τ_r from the index set $I = \{1, 2, \ldots, \rho\}$ of S to the index set $J_r = \{1, 2, \ldots, \mu_r\}$ of $S_r(N_1, N_2, \ldots, N_\rho)$ such that

$$t_{l,r} = k_{\tau_r(l),r} \quad \text{for } l = 1, 2, \ldots, \rho. \tag{4}$$

The mapping τ_r specifies the correspondence between integers in S and residues in $S_r(N_1, N_2, \ldots, N_\rho)$ for each r. Suppose the correspondence between residue set $S_r(N_1, N_2, \ldots, N_\rho)$ and $p_r \in P$ for $1 \le r \le \gamma$ is specified, but the correspondence between N_l and its remainder $k_{l,r}$ (or equivalently, the mapping τ_r) is not known, i.e., the correct order of the remainders in a residue set is not known. Although τ_r is not known but exists.

The *problem* is to determine set S of multiple integers $N_1, N_2, \ldots, N_\rho$ from the γ residue sets $S_r(N_1, N_2, \ldots, N_\rho)$ and their corresponding moduli p_r, where the correct order of the remainders in each residue set $S_r(N_1, N_2, \ldots, N_\rho)$ is not known, $1 \le r \le \gamma$.

It is clear that, when $\rho = 1$, the above problem is back to the conventional CRT and CRT provides a complete answer to the problem. As pointed out in [1], the difficulty of the above problem when $\rho > 1$ comes from the fact that the correspondence between integers N_l and their residues $k_{\tau_r(l),r}$ is not known, i.e., for any fixed r, it is not known with which integer N_i a remainder $k_{l,r}$ satisfies $k_{l,r} = N_i \bmod p_r$, while we only know the residue set $S_r(N_1, N_2, \ldots, N_\rho)$ that comes from a set of integers modulo $p_r, 1 \le r \le \gamma$.

The above problem has been studied in [1]–[3] motivated from multiple frequency determination using multiple undersampled waveforms as mentioned in Introduction. It can be briefly described as follows.

Consider γ sensors with sampling rates p_r Hz, $1 \le r \le \gamma$. Consider ρ multiple frequencies $f_1 = N_1$ Hz, $\ldots, f_\rho = N_\rho$ Hz in a superpositioned waveform and these frequencies may include information interested and need to be accurately determined. At the rth sensor, the received analog signal is of the following form:

$$x_r(t) = \sum_{l=1}^{\rho} A_{l,r} e^{2\pi j f_l t} + w_r(t) \tag{5}$$

where $A_{l,r}, 1 \le l \le \rho$, are nonzero complex coefficients and $w_r(t)$ is the additive white noise. The sampled signal at the rth sensor with sampling rate p_r Hertz is

$$x_r[n] = x_r\left(\frac{n}{p_r}\right) = \sum_{l=1}^{\rho} A_{l,r} e^{2\pi j f_l n/p_r} + w_r\left(\frac{n}{p_r}\right). \tag{6}$$

The problem is to determine the multiple frequencies $f_l = N_l, 1 \le l \le \rho$, from the above sampled data $x_r[n], 1 \le r \le \gamma$, where the sampling rates p_r may be much lower than the signal frequencies N_l. Based on the sampled data $x_r[n]$ at the rth sensor, we take p_r-point DFT and obtain

$$\begin{aligned} X_r[k] &= \mathrm{DFT}_{p_r}(x_r[n]) \\ &= \sum_{l=1}^{\rho} \sqrt{p_r} A_{l,r} \delta(k - t_{l,r}) + W_r[k] \end{aligned} \tag{7}$$

for $0 \le k \le p_r - 1$, where $t_{l,r}$ is the remainder of N_l modulo p_r and can be detected without the order information in terms of the index l. Thus, at the rth sensor, what can be detected from the sampled waveform with sampling rate p_r Hertz is the residue set $S_r(N_1, N_2, \ldots, N_\rho)$ defined above and the frequency determination problem of $f_l, 1 \le l \le \rho$, precisely becomes the problem we described above. The case when there are errors in the detected residues $t_{l,r}$ has been considered in [6] with a lower dynamic range and this correspondence only considers the residue error free case.

Regarding the above problem, there are two questions. 1) When can the multiple integers in S be uniquely determined from the residue sets $S_r(N_1, N_2, \ldots, N_\rho)$ and p_r for $1 \le r \le \gamma$? 2) If the uniqueness is satisfied in 1), how can these multiple integers be determined? In [1], a dynamic range for the uniqueness of the determination of the multiple integers is given: If

$$\max\{N_1, N_2, \ldots, N_\rho\} < \max\{p, p_1, p_2, \ldots, p_\gamma\} \tag{8}$$

where

$$\begin{aligned} p &= \min_{1 \le r_1 < r_2 < \cdots < r_\eta \le \gamma} \mathrm{lcm}\{p_{r_1}, p_{r_2}, \ldots, p_{r_\eta}\} \\ &= p_1 p_2 \cdots p_\eta \end{aligned} \tag{9}$$

where

$$\eta = \left\lfloor \frac{\gamma}{\rho} \right\rfloor \quad \text{or} \quad \gamma = \eta\rho + \theta \tag{10}$$

for some $0 \le \theta < \rho$. In [1], the determination method is basically look-up table method. In [3], an efficient (but may be still complicated) determination algorithm is proposed, which can be thought of as a generalization of CRT. As a special case, when $\max\{p, p_1, p_2, \ldots, p_\gamma\} = p_\gamma$ in (8), all integers $N_1, N_2, \ldots, N_\rho$ can be uniquely determined directly from the residue set $S_\gamma(N_1, N_2, \ldots, N_\rho)$ alone because in this case, all the integers $N_1, N_2, \ldots, N_\rho$ are the same as the remainders $k_{1,\gamma}, k_{2,\gamma}, \ldots, k_{\rho,\gamma}$ themselves, i.e., $S = S_\gamma(N_1, N_2, \ldots, N_\rho)$.

The dynamic range in (8) is maximized in [2] with an efficient determination algorithm when an additional condition on the multiple integers is satisfied: if

$$\max_{1 \le l_1 < l_2 \le \rho} |N_{l_1} - N_{l_2}| < \frac{1}{2} \min\{p_1, p_2, \ldots, p_\gamma\} \tag{11}$$

and

$$\begin{aligned} &\max\{N_1, N_2, \ldots, N_\rho\} < lcm\{p_1, p_2, \ldots, p_\gamma\} \\ &= p_1 p_2 \cdots p_\gamma \end{aligned} \tag{12}$$

then $N_1, N_2, \ldots, N_\rho$ can be uniquely determined. Clearly, the dynamic range in (12) is already the maximal possible one since it is even the maximal possible one for the conventional CRT, i.e., when $\rho = 1$. However, the right hand side of (12) is not the dynamic range in general. One example is: $N_1 = 5, N_2 = 4$ and $p_1 = 2, p_2 = 3$. In this case, the right hand side of (12) is $p_1 p_2 = 6$ and the two integers N_1 and N_2 are within the range in (12). The two residue sets are $\{0, 1\}$ and $\{1, 2\}$, respectively. It is not hard to see there is another solution for these two sets of residues: $\hat{N}_1 = 1, \hat{N}_2 = 2$. Another example is $N_1 = 208, N_2 = 209$ and $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$. In this case, $\rho = 2, \gamma = 4$, and the right hand side of (12) is $p_1 p_2 p_3 p_4 = 210$, and the two integers N_1 and N_2 are also within the range in (12). The four residue sets are $\{0,1\},\{1,2\},\{3,4\}$, and $\{5,6\}$, respectively. One can see that $\hat{N}_1 = 13$ and $\hat{N}_2 = 194$ form another solution for the two integers N_1 and N_2, i.e., they share the same residue sets as N_1 and N_2 do.

The problems of interest of this correspondence are whether we can improve the dynamic range (8) for general multiple integers without any additional condition and how we can determine these multiple integers.

III. Majority Method and an Improved Dynamic Range

To introduce a majority method, we first introduce some notations. An m-partition π of $P = \{p_1, p_2, \ldots, p_\gamma\}$ is defined as a decomposition of P into a union of its m disjoint subsets $\{P_1^\pi, P_2^\pi, \ldots, P_m^\pi\}$ where a subset P_i^π of P can be empty, i.e.,

$$\pi : P \rightarrow \{P_1^\pi, P_2^\pi, \ldots, P_m^\pi\}$$

where $P = P_1^\pi \cup P_2^\pi \cup \cdots \cup P_m^\pi$ and $P_i^\pi \cap P_j^\pi = \emptyset$ for $1 \le i \ne j \le m$, and P_i^π can be the empty set. For $1 \le i \le m$, we define b_i^π as the product of integers $p_r \in P_i^\pi$ if P_i^π is not empty and 1 if $P_i^\pi = \emptyset$, i.e.,

$$b_i^\pi \triangleq \begin{cases} \prod_{p_r \in P_i^\pi} p_r, & \text{if } P_i^\pi \ne \emptyset \\ 1, & \text{if } P_i^\pi = \emptyset. \end{cases} \tag{13}$$

We define b^π as the minimum of b_i^π for $1 \le i \le m$ and c^π as the maximum of b_i^π for $1 \le i \le m$, i.e.,

$$b^\pi \triangleq \min_{1 \le i \le m} b_i^\pi \quad \text{and} \quad c^\pi \triangleq \max_{1 \le i \le m} b_i^\pi. \tag{14}$$

Clearly, $c^\pi \ge b^\pi$ for any m-partition π. Let $b(m)$ be the maximal b^π and $c(m)$ be the minimum c^π among all the m-partitions π of P, i.e.,

$$b(m) \triangleq \max_{m-\text{partition } \pi \text{ of } P} b^\pi$$

and

$$c(m) \triangleq \min_{m-\text{partition } \pi \text{ of } P} c^\pi \tag{15}$$

which can be calculated as long as a modulus set P is given while it may be complicated to do when the size of P is large. Let π_1 and π_2 be the two m-partitions of P with which the maximum and the minimum in (15) are reached, respectively. Then

$$\begin{aligned}(b(m))^m = (b^{\pi_1})^m \le \prod_{i=1}^m b_i^{\pi_1} = \prod_{i=1}^\gamma p_i = \prod_{i=1}^m b_i^{\pi_2} \\ \le (c^{\pi_2})^m = (c(m))^m.\end{aligned} \tag{16}$$

Thus

$$b(m) \le c(m). \tag{17}$$

We now introduce a majority method. Let π be the m-partition with that the maximal $b(m)$ in (15) is reached. Assume all the integers N_l in S satisfy

$$\max\{N_1, N_2, \ldots, N_\rho\} < \min\{c(\rho), b(m)\}. \tag{18}$$

For each $r, 1 \le r \le \gamma$, let σ_r be an arbitrarily chosen onto-mapping from the index set $I = \{1, \ldots, \rho\}$ to the index set J_r of the elements in $S_r(N_1, N_2, \ldots, N_\rho)$

$$S_r(N_1, N_2, \ldots, N_\rho) = \bigcup_{j=1}^{\rho} \{k_{\sigma_r(j),r}\}.$$

TABLE I
Remainder Table

integer	mod p_1	mod p_2	$\cdots$	mod p_γ
$\hat{N}_1$	$k_{\sigma_1(1),1}$	$k_{\sigma_2(1),2}$	$\cdots$	$k_{\sigma_\gamma(1),\gamma}$
$\hat{N}_2$	$k_{\sigma_1(2),1}$	$k_{\sigma_2(2),2}$	$\cdots$	$k_{\sigma_\gamma(2),\gamma}$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$\hat{N}_\rho$	$k_{\sigma_1(\rho),1}$	$k_{\sigma_2(\rho),2}$	$\cdots$	$k_{\sigma_\gamma(\rho),\gamma}$

For each subset $P_i^\pi, 1 \le i \le m$, we calculate the positive integers N_j^i with

$$0 \le N_j^i < \min\{c(\rho), b(m)\} \le b(m) \le b_i^\pi \tag{19}$$

for $1 \le j \le \rho$ by using the conventional CRT such that

$$N_j^i \equiv k_{\sigma_r(j),r} \bmod p_r, \quad \forall p_r \in P_i^\pi \tag{20}$$

where $k_{\sigma_r(j),r} \in S_r(N_1, N_2, \ldots, N_\rho)$ as we see from the above definitions. Note that, for an arbitrary mapping σ_r above, the integers N_j^i in (19) may not exist. However, if the mapping σ_r is the correct mapping (or the correspondence between the integers N_j and their remainders $k_{\tau_r(j),r}$), i.e., $\sigma_r = \tau_r$, although it may not have to be, integers N_j^i in (19) do exist because the remainders are the true remainders from the set of integers $\{N_1, N_2, \ldots, N_\rho\}$ modulo $\{p_1, p_2, \ldots, p_\gamma\}$, and the assumption (18) for integers N_j that are within the dynamic ranges of the conventional CRT for single integers. If an integer N_j^i in (19) does not exist, we know that the mapping σ_r is not a correct mapping, i.e., $\sigma_r \ne \tau_r$, and we then arbitrarily choose another onto-mapping from the index set $I = \{1, \ldots, \rho\}$ to the index set J_r of the elements in $S_r(N_1, N_2, \ldots, N_\rho)$ until integers N_j^i in (19) do exist. Also note that although the searching process of the above mappings σ_r so that the integers N_j^i in (19) can be found may have a high complexity, we are interested more in the uniqueness of the determination than in the complexity of the determination in this correspondence. Therefore, as long as there exist mappings σ_r such that (19) and (20) hold, it is sufficient for the results obtained later in this correspondence to hold.

Due to (19), for each valid mapping σ_r described above, a reconstruction of integer N_j^i in (20) is unique. Thus, we obtain an integer set $\hat{S}_i = \{N_1^i, N_2^i, \ldots, N_\rho^i\}$ for each subset $P_i^\pi, 1 \le i \le m$, and for each valid mapping σ_r. We then compare these m integer sets $\hat{S}_i, 1 \le i \le m$. Clearly, these integer sets depend on the choice of the arbitrarily chosen onto-mappings σ_r from I to J_r for $1 \le r \le \gamma$. We are interested in the case when all these integer sets are the same and have ρ distinct elements, i.e., $\hat{S}_1 = \cdots = \hat{S}_m = \hat{S} = \{\hat{N}_1, \ldots, \hat{N}_\rho\}$ with $\hat{N}_i \ne \hat{N}_j$ for $i \ne j$. Let

$$\begin{aligned}\Omega \triangleq \{(\sigma_1, \ldots, \sigma_\gamma) : \hat{S}_1 = \cdots \\ = \hat{S}_m \text{ contains } \rho \text{ distinct elements}\}.\end{aligned} \tag{21}$$

It is not hard to see that the set $\Omega \ne \emptyset$ since $(\tau_1, \ldots, \tau_\gamma) \in \Omega$, where τ_r is the mapping from I to J_r defined before, due to the facts (14) and (18)–(20).

Suppose we have already found γ onto-mappings $\sigma_1, \ldots, \sigma_\gamma$ for all the residue sets such that $\hat{S}_1 = \hat{S}_2 = \cdots = \hat{S}_m = \{\hat{N}_1, \ldots, \hat{N}_\rho\}$ with $\hat{N}_i \ne \hat{N}_j$ for $i \ne j$. Let us look at Table I. Note that the existence of such maps σ_r is ensured by the fact that the set Ω is not empty.

For $1 \le s \le \rho$ and $1 \le l \le \rho$, we define set

$$\hat{Q}_s^l \triangleq \{p_r : \sigma_r(l) = \tau_r(s), 1 \le r \le \gamma\}. \tag{22}$$

Then, for each $l, 1 \leq l \leq \rho, P = \bigcup_{s=1}^{\rho} \hat{Q}_s^l$. In order to form a ρ-partition of P, we define

$$Q_s^l \triangleq \left(\bigcup_{t=1}^{s} \hat{Q}_t^l \right) - \left(\bigcup_{t=1}^{s-1} \hat{Q}_t^l \right) \tag{23}$$

for $s = 1, \ldots, \rho$, such that $Q_i^l \bigcap Q_j^l = \emptyset$ for $1 \leq i \neq j \leq \rho$ and $\bigcup_{t=1}^{\rho} Q_t^l = P$. We denote the corresponding ρ-partition as μ^l for simplicity. For each fixed $s, 1 \leq s \leq \rho$, each fixed $l, 1 \leq l \leq \rho$, and any $p_r \in Q_s^l$, we have

$$p_r \mid (\hat{N}_l - N_s)$$

which is because when $p_r \in Q_s^l$, we have $\sigma_r(l) = \tau_r(s)$ and $k_{\sigma_r(l),r} = k_{\tau_r(s),r} = t_{s,r}$ and then it follows from (1) by replacing l with s in (1) and (20) by replacing j with l in (20). Thus, we have $\prod_{p_r \in Q_s^l} p_r \mid (\hat{N}_l - N_s)$, i.e., $b_s^{\mu^l} \mid (\hat{N}_l - N_s)$, and if $0 \leq \hat{N}_l, N_s < b_s^{\mu^l}$ then $\hat{N}_l = N_s$. Therefore, we have the following system of equations:

$$\begin{aligned} \hat{N}_1 &= N_1 - a_{11} b_1^{\mu^1} = \cdots = N_\rho - a_{1\rho} b_\rho^{\mu^1} \\ \hat{N}_2 &= N_1 - a_{21} b_1^{\mu^2} = \cdots = N_\rho - a_{2\rho} b_\rho^{\mu^2} \\ &\vdots \\ \hat{N}_\rho &= N_1 - a_{\rho 1} b_1^{\mu^\rho} = \cdots = N_\rho - a_{\rho\rho} b_\rho^{\mu^\rho} \end{aligned} \tag{24}$$

where the coefficient $a_{ij} \in \mathbb{Z}, 1 \leq i, j \leq \rho$, and $b_i^{\mu^l}$ is similarly defined as in (13) for an m-partition π of P when $m = \rho$.

We next find a dynamic range (a sufficient upper bound) for integers in S such that once $\hat{S}_1 = \hat{S}_2 = \cdots = \hat{S}_m$ containing ρ distinct elements occurs, or the above system of equations occur, we have $\hat{S} = S$.

Theorem 1: An integer set S above can be uniquely determined from its γ residue sets $S_r(N_1, N_2, \ldots, N_\rho)$ and moduli $p_r, 1 \leq r \leq \gamma$, by the above majority method if

$$\max\{N_1, N_2, \ldots, N_\rho\} < \min\{c, b\} = \begin{cases} \min\{c, b\}, & \text{when } \rho > 2 \\ b, & \text{when } \rho = 2 \end{cases} \tag{25}$$

where c and b are defined similar to before:

$$c \triangleq \min_{\rho-\text{partition } \pi \text{ of } P} c^\pi \quad \text{and} \quad b \triangleq \max_{2-\text{partition } \pi \text{ of } P} b^\pi, \tag{26}$$

where c^π and b^π are defined in (14) for a ρ-partition π and a 2-partition π of $P = \{p_1, p_2, \ldots, p_\gamma\}$, respectively.

Proof: Let the 2-partition of P achieving $b = \max_{2-\text{partition } \pi \text{ of } P} b^\pi$ in (25) be π_0, i.e., $P = P_1^{\pi_0} \cup P_2^{\pi_0}, P_1^{\pi_0} \cap P_2^{\pi_0} = \emptyset$, and $b^{\pi_0} = b = \max_{2-\text{partition} \pi \text{of} P} b^\pi$. Using the majority method described above with $m = 2$, we arrive at $\hat{S}_1 = \hat{S}_2 = \hat{S} = \{\hat{N}_1, \ldots, \hat{N}_\rho\}$ with $0 \leq \hat{N}_i \neq \hat{N}_j < \min\{c, b\}$ for $i \neq j$ which can be seen from (19) with $c = c(\rho)$ and $b = b(2)$. We next want to show $\hat{S} = S$.

For $1 \leq l \leq \rho$, we define set $\hat{Q}_s^l$ and Q_s^l like (22) and (23), respectively, for $1 \leq s \leq \rho$. For each $l, 1 \leq l \leq \rho$, sets $Q_s^l \subset P, s = 1, \ldots, \rho$, also form a ρ-partition of P and we denote it as μ^l. We define $c^{\mu^l} = \max\{b_1^{\mu^l}, b_2^{\mu^l}, \ldots, b_\rho^{\mu^l}\}$. Clearly

$$c^{\mu^l} \geq \min_{\rho-\text{partition } \pi \text{ of } P} c^\pi = c.$$

Therefore, $c^{\mu^l} \geq \min\{c, b\}$. Without loss of generality, we assume $c^{\mu^l} = b_{i_l}^{\mu^l}$. Thus, $b_{i_l}^{\mu^l} \geq \min\{c, b\}$. From (24), we obtain $b_{i_l}^{\mu^l} \mid (\hat{N}_l - N_{i_l})$. Combining this property with $0 \leq \hat{N}_l, N_{i_l} < \min\{c, b\} \leq b_{i_l}^{\mu^l}$, we know $\hat{N}_l = N_{i_l} \in S$. This proves $\hat{S} \subset S$. Since both $\hat{S}$ and S have ρ elements, we conclude $\hat{S} = S$. The last equality in (25) is because $c = c(2) \geq b(2) = b$ from (17) when $\rho = 2$. □

It is not hard to see that the sequence $b(m)$ defined in (15) decreases in terms of m. Thus, $b = b(2) > b(m)$ for $m > 2$. Therefore, although in the proof of Theorem 1, 2-partitions of P are used in the majority method proposed above, the majority method for m-partitions also works, i.e., when $\hat{S}_1 = \hat{S}_2 = \cdots = \hat{S}_m = \hat{S} = \{\hat{N}_1, \hat{N}_2, \ldots, \hat{N}_\rho\}$ with $\hat{N}_i \neq \hat{N}_j$ for $i \neq j$, we then have $\hat{S} = S$. In other words, the following corollary holds.

Corollary 1: The above majority method using m-partitions with $m \geq 2$ provides a solution of S, i.e., $\hat{S} = S$.

In the following, we use the pigeon hole principle and 2-partitions of P to obtain another dynamic range.

Theorem 2: When $\rho > 2$, an integer set S above can be uniquely determined from its γ residue sets $S_r(N_1, N_2, \ldots, N_\rho)$ and moduli $p_r, 1 \leq r \leq \gamma$, by the above majority method if

$$\max\{N_1, N_2, \ldots, N_\rho\} < \prod_{i=1}^{\lceil \frac{\gamma}{\rho} \rceil} p_i.$$

Proof: Similar to the proof of Theorem 1, we now use a 2-partition of $P: P = P_1 \bigcup P_2$, where $P_1 = \{p_1, p_2, \ldots, p_{\lceil \frac{\gamma}{\rho} \rceil}\}$ and $P_2 = \{p_{\lceil \frac{\gamma}{\rho} \rceil + 1}, \ldots, p_\gamma\}$. When $\rho > 2$ and $\gamma \geq 2$, we have $\gamma - \lceil \frac{\gamma}{\rho} \rceil \geq \lceil \frac{\gamma}{\rho} \rceil$. Thus

$$\prod_{i=1}^{\lceil \frac{\gamma}{\rho} \rceil} p_i < \prod_{i=\lceil \frac{\gamma}{\rho} \rceil + 1}^{\gamma} p_i$$

due to the earlier assumption $p_1 < p_2 < \cdots < p_\gamma$. Following the steps of the proof of Theorem 1 until we obtain the partition sets $Q_s^l, s = 1, \ldots, \rho$, for $l = 1, \ldots, \rho$. For each $1 \leq l \leq \rho$, all of the γ integers in P are put into ρ subsets $Q_s^l, s = 1, \ldots, \rho$. The pigeon hole principle states that there is one subset has at least $\lceil \frac{\gamma}{\rho} \rceil$ integers $p_i \in P$. Thus, for the ρ-partition, $Q_s^l, 1 \leq s \leq \rho$, of P, we have

$$c^{\mu^l} = \max\left\{b_1^{\mu^l}, b_2^{\mu^l}, \ldots, b_\rho^{\mu^l}\right\} \geq \prod_{i=1}^{\lceil \frac{\gamma}{\rho} \rceil} p_i,$$

for $l = 1, \ldots, \rho$. Without loss of generality, we assume $c^{\mu^l} = b_{i_l}^{\mu^l}$. Thus, $b_{i_l}^{\mu^l} \geq \prod_{i=1}^{\lceil \frac{\gamma}{\rho} \rceil} p_i$. From (24), we have

$$\hat{N}_l = N_{i_l} - a_{l i_l} b_{i_l}^{\mu^l}.$$

Since the condition $0 \leq \hat{N}_l, N_{i_l} < \prod_{i=1}^{\lceil \frac{\gamma}{\rho} \rceil} p_i$, we know that the above equality holds if and only if $a_{l i_l} = 0$, equivalently, $\hat{N}_l = N_{i_l} \in S$. This proves $\hat{S} \subset S$. Since both $\hat{S}$ and S have ρ elements, we conclude $\hat{S} = S$. □

Combining the above two results, we obtain the following improved dynamic range of the generalized CRT.

Corollary 2: Let b and c be defined in (26) in Theorem 1. An integer set S of ρ distinct integers can be uniquely determined from its γ residue sets $S_r(N_1, N_2, \ldots, N_\rho)$ and moduli $p_r, 1 \leq r \leq \gamma$, by the above majority method if

$$\max\{N_1, N_2, \ldots, N_\rho\} < \max\left\{\min\{c, b\}, \prod_{i=1}^{\lceil \frac{\gamma}{\rho} \rceil} p_i, \ p_\gamma\right\}$$

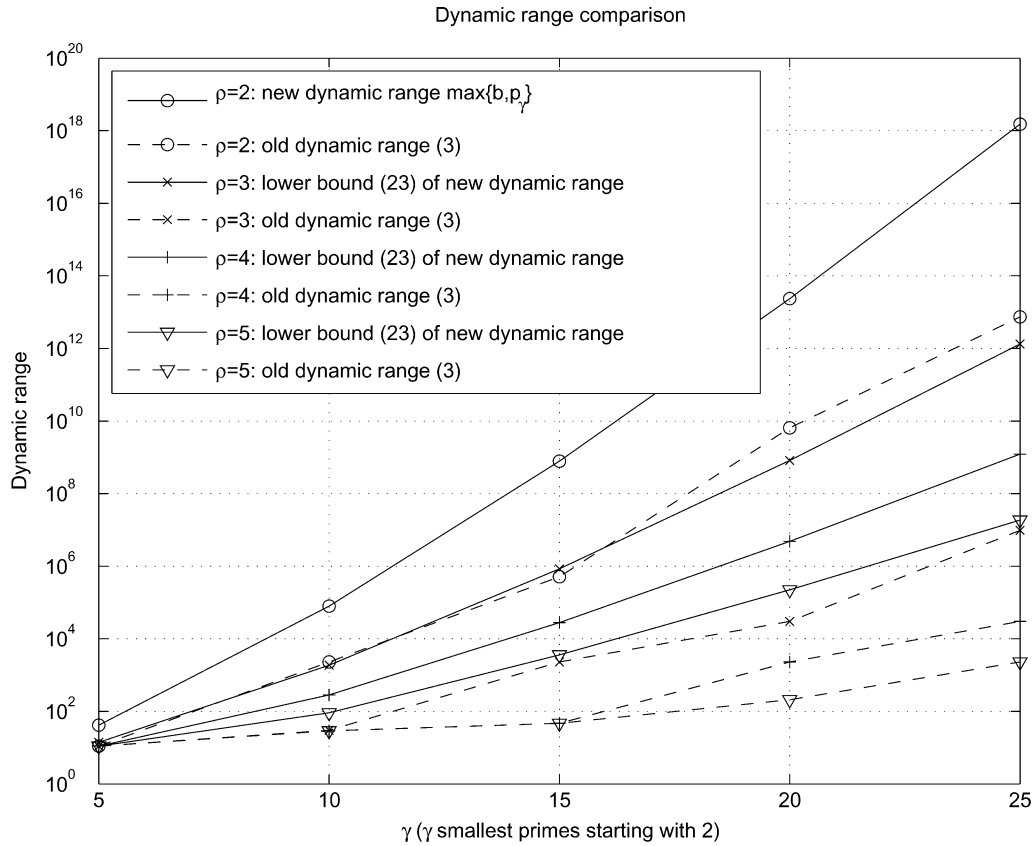

Fig. 1. Dynamic range comparison.

when $\rho > 2$, and

$$\max\{N_1, N_2, \ldots, N_\rho\} < \max\{b, p_\gamma\}$$

when $\rho = 2$.

Proof: If $\max\{N_1, N_2, \ldots, N_\rho\} < p_\gamma$, then $S_\gamma(N_1, N_2, \ldots, N_\rho) = S = \{N_1, N_2, \ldots, N_\rho\}$ as mentioned in Section II. The rest follows from Theorems 1 and 2 directly. ■

It is not hard to see that the new dynamic range presented in Corollary 2 is greater than the one (8) in [1] when there are more than two moduli, i.e., $\gamma > 2$:

$$\min\{c, b\} > p_1 p_2 \cdots p_\eta \tag{27}$$

which is because of the following argument. By the definition of c in (26), (14), and (15) where $c = c(\rho)$, we immediately have $c > p_1 p_2 \cdots p_\eta$. When $\gamma > 2$, we specify a 2-partition π of P such that $P = \{p_1, p_3, \ldots, p_{2\lceil\gamma/2\rceil-1}\} \cup \{p_2, p_4, \ldots, p_{2\lfloor\gamma/2\rfloor}\}$. Thus, from (26), (14), and (15), we know $b = b(2) \geq b^\pi > p_1 p_2 \cdots p_{\lfloor\gamma/2\rfloor} \geq p_1 p_2 \cdots p_\eta$ since $\lfloor\gamma/2\rfloor \geq \eta = \lfloor\gamma/\rho\rfloor$ when $\rho \geq 2$. When $\gamma = 2$, both dynamic ranges in Corollary 2 and (8) in [1] become trivial, i.e., p_1. When $\rho = 1$, it reduces to the conventional CRT.

As example, let us consider the case of $p_1 = 5, p_2 = 7, p_3 = 11, p_4 = 13$, and $\rho = 2$. We want to determine two integers N_1, N_2 from their residue sets. From Corollary 2, we conclude that they can be uniquely determined if $\max\{N_1, N_2\} < 65$. Comparing with the one in (8) in [1], $\max\{N_1, N_2\} < 35$, one can see that the new dynamic range, 65, obtained in this correspondence almost doubles 35 previously obtained in [1]. The improvement becomes more significant when the size of the modulus set P becomes larger, which can be seen from Fig. 1. Regarding to the application of multiple frequency determination proposed in [1], the maximal frequency in this example is 65 Hz in a superposition of two harmonic signals so that these two frequencies can be uniquely determined from four sensors with sampling rates 5, 7, 11, and 13 Hz, respectively, based on the proposed majority method above, while the maximal frequency is 35 Hz based on the method proposed in [1]. Note that, the above dynamic range 65 is a sufficient range of two integers for their unique determination and it does not mean that two integers above 65 can not be uniquely determined, i.e., the above dynamic range may not be necessary as we shall see later in another example.

For a general ρ, the calculation of c in (26) in the dynamic range in Corollary 2 may not be easy. Due to (16), it can be easily lower bounded by

$$c \geq \left\lceil \left(\prod_{i=1}^{\gamma} p_i\right)^{\frac{1}{\rho}} \right\rceil. \tag{28}$$

Clearly, the lower bound of c in (28) is greater than the dynamic range (8) obtained in [1]:

$$\left\lceil \left(\prod_{i=1}^{\gamma} p_i\right)^{\frac{1}{\rho}} \right\rceil > p_1 p_2 \cdots p_\eta \tag{29}$$

where η is defined in (10).

The lower bound of c in (28) provides the following lower bound for the new dynamic range in Corollary 2.

Corollary 3: The dynamic range in Corollary 2 is lower bounded by

$$\max\left\{\min\left\{\left\lceil \left(\prod_{i=1}^{\gamma} p_i\right)^{\frac{1}{\rho}} \right\rceil, b\right\}, \prod_{i=1}^{\lceil\frac{\gamma}{\rho}\rceil} p_i, p_\gamma\right\} \tag{30}$$

when $\rho > 2$, and $\max\{b, p_\gamma\}$ when $\rho = 2$.

In Fig. 1, we compare the existing dynamic range (8) in [1] with the new dynamic range $\max\{b, p_\gamma\}$ when $\rho = 2$ and the lower bound (30) of the new dynamic range in Corollary 2 when $\rho > 2$. In Fig. 1, the moduli $p_1 = 2, p_2, \ldots, p_\gamma$ are the γ smallest primes, and $\rho = 2, 3, 4, 5$ and $\gamma = 5, 10, 15, 20, 25$ are considered. The existing dynamic ranges are plotted with dashed lines and the new dynamic ranges or their lower bounds are plotted with solid lines. One can see that the improvement of the newly obtained dynamic ranges are significantly better than the existing ones.

On the other hand, the new dynamic range presented in Corollary 2 is still not necessary. As a counter example, let us consider the case of $p_1 = 5, p_2 = 7, p_3 = 11, p_4 = 13$, and $\rho = 3$. In this case, the new dynamic range from Corollary 2 is 35, i.e., if $\max\{N_1, N_2, N_3\} < 35$, then these three nonnegative integers can be uniquely determined. This is not necessary. In fact, it is not hard to check that if $\max\{N_1, N_2, N_3\} < 65$, we can uniquely reconstruct N_1, N_2, N_3 from their four residue sets as follows. Arrange p_1, p_4 as a group and p_2, p_3 as another group. Then, these three integers can be determined by using the majority method described before. We omit its details here.

IV. Conclusion

In this correspondence, we further studied a generalized CRT for multiple integer determination from their residue sets and moduli. We first presented a majority method for the determination and then obtained an improved dynamic range over the existing one for the unique determination of multiple integers based on the proposed majority method. Besides the mentioned application in multiple frequency determination from multiple undersampled waveforms, such as, from low functionality sensors, the above generalized CRT can be applied to cryptography, for example, for secret sharing similar to the conventional CRT [8]. As a remark, the majority method for the multiple integer determination has a high complexity. Any simplified determination algorithm for the generalized CRT with the newly proposed dynamic range would be interesting.

Acknowledgment

The authors would like to thank the associate editor and the anonymous reviewers for their detailed and constructive comments that have helped the presentation of this correspondence.

References

[1] X.-G. Xia, "Estimation of multiple frequencies in undersampled complex valued waveforms," *IEEE Trans. Signal Processing*, vol. 47, pp. 3417–3419, Dec. 1999.

[2] G. C. Zhou and X.-G. Xia, "Multiple frequency detection in undersampled complex-valued waveforms with close multiple frequencies," *Electron. Lett.*, vol. 33, pp. 1294–1295, Jul. 1997.

[3] X.-G. Xia, "An efficient frequency determination algorithm from multiple undersampled waveforms," *IEEE Signal Processing Lett.*, vol. 7, pp. 34–37, Feb. 2000.

[4] G. Wang, X.-G. Xia, V. C. Chen, and R. L. Fiedler, "Detection, location, and imaging of fast moving targets using multifrequency antenna array SAR," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 40, pp. 345–355, Jan. 2004.

[5] X.-G. Xia, "Dynamic range of the detectable parameters for polynomial phase signals using multiple-lag diversities in high-order ambiguity functions," *IEEE Trans. Inf. Theory*, vol. 47, pp. 1378–1384, May 2001.

[6] X.-G. Xia and K. J. 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 Processing Lett.*, vol. 12, pp. 768–771, Nov. 2005.

[7] J. H. McClellan and C. M. Rader, *Number Theory in Digital Signal Processing*. Englewood Cliffs, N. J.: Prentice-Hall, 1979.

[8] C. Ding, D. Pei, and A. Salomaa, *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*. Singapore: World Scientific, 1999.

A Note on the Optimal Quadriphase Sequences Families

Xiaohu H. Tang, *Member, IEEE*, and
Parampalli Udaya, *Member, IEEE*

***Abstract*—In this note, by using a modification of the families $\mathcal{B}$ and $\mathcal{C}$, we obtain a larger family of optimal quadriphase sequences, $\mathcal{D}$ over $\mathbf{Z}_4$. In contrast to the families $\mathcal{B}$ and $\mathcal{C}$, the family $\mathcal{D}$ has the same length and the same maximal nontrival correlation value, but with double the size.**

***Index Terms*—Galois ring, optimal sequences, quadriphase sequences.**

I. Introduction

In code-division multiple-access (CDMA) communication systems, nonbinary signature sequences are preferred over binary sequences as they offer 3-dB improvement in signal to interference ratio [2]. This is because the lower bound on smallest possible nontrivial correlation parameter C_{max} for non binary sequences is $\sqrt{2}$ times better than that for binary sequences [5]. Among the non binary alphabets, quadriphase sequences are preferred for signature sequences because of easy implementation of modulators and availability of optimal sequences.

In the early 1990s, the theory of $\mathbf{Z}_4$ maximal length sequences was established, leading to the discovery of optimal quadriphase sequences meeting the Welch and Sidelnikov bounds [2], [6], [7]. Unlike in field case, the possible periods for sequences over $\mathbf{Z}_4$ are $2^n - 1$ and $2(2^n - 1)$, where n is a positive integer. There are three optimal families derived as a sequences satisfying a linear recursion over $\mathbf{Z}_4$. The first basic optimal family is known as family $\mathcal{A}$ which comprises of $2^n + 1$ $\mathbf{Z}_4$ maximal length sequences [2]. The second optimal family known as family $\mathcal{B}$ [2] which can be seen as interleaved version of sequences in family $\mathcal{A}$. This family consists of 2^{n-1} sequences of period $2(2^n - 1)$. A third optimal family not discussed in [2] exists with the same parameters as family $\mathcal{B}$ with n odd integer [7]. We refer to this family as family $\mathcal{C}$. A complete treatment of all such families of trace sequences over $\mathbf{Z}_4$ is given in [7] which includes three more suboptimal families.

Quadriphase sequences based on a generalization of the above $\mathbf{Z}_4$ families have been adopted as spectrum spreading sequences in 3G wideband CDMA standards [4]. It is expected that fourth generation CDMA systems need to handle higher data rates of up to 1 Gbytes/s.

Manuscript received March 26, 2006; revised September 29, 2006. This work of X. H. Tang was supported by the Program for New Century Excellent Talents in University (NCET) under Grants 04-0888, the National Science Foundation of China (NSFC) under Grants 60302015, and the Key (Key grant) Project of Chinese Ministry of Education under Grants 105147. The work of P. Udaya was supported by Australian Research Council(ARC) and Melbourne Research Grant Scheme (MRGS) of the University of Melbourne.

X. H. Tang is with the Institute of Mobile Communications, Southwest Jiaotong University, Chengdu, China (e-mail: xhutang@ieee.org).

P. Udaya is with the Department of Computer Science and Software Engineering, University of Melbourne, VIC 3010, Australia (e-mail: udaya@cs.mu.oz.au).

Communicated by G. Gong, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2006.887502