SIMPLIFICATION ON DYNAMIC RANGE OF A GENERALIZED CHINESE REMAINDER THEOREM FOR MULTIPLE INTEGERS

Wei Wang
School of Mathematical Sciences, Xiamen University, Xiamen, China
and
College of Information Engineering, Tarim University, Alar, China
wangwei.math@gmail.com

Xiaoping Li
School of Mathematical Sciences, University of Electronic Science and Technology of China, Chengdu, China
lixiaoping.math@uestc.edu.cn

Xiang-Gen Xia
Department of Electrical and Computer Engineering, University of Delaware, Newark, Delaware
xxia@ee.udel.edu

Wenjie Wang
MOE Key Lab for Intelligent Networks and Network Security, Xi'an Jiaotong University, Xi'an, China
wjwang@xjtu.edu.cn

Jianguo Qian
School of Mathematical Sciences, Xiamen University, Xiamen, China
jgqian@xmu.edu.cn

Received: 3/25/16, Revised:12/4/16, Accepted: 6/29/17, Published: 7/17/17

Abstract

Motivated by multiple frequency determination in multiple undersampled waveforms, a generalization of the Chinese remainder theorem for multiple integers has been of recent interest. Liao and Xia (2007) obtained a lower bound on the dynamic range of multiple integers for their unique recovery. In this paper, we present a simplified bound with a simplified proof.

1. Introduction

The Chinese remainder theorem (CRT) tells us that a single nonnegative integer can be reconstructed from its remainders modulo several pairwise coprime moduli if and only if the integer is less than the product of all the moduli. This ability to represent a large integer as a list of small residues or remainders leads to applications in numerous areas, such as cryptography, channel coding, and digital signal processing [4, 9].

There are various generalizations of the CRT; see [1–3, 5, 6, 8, 10, 12–14, 16] for some of them. In [12], motivated by multiple frequency detection from multiple undersampled rates, Xia presented the following generalized CRT problem for multiple integers.

Let $\gamma \geq 2$ and $m_1, \ldots, m_\gamma$ be γ *pairwise coprime* integers with $1 < m_1 < \cdots < m_\gamma$ and let $\mathcal{N} = \{N_1, \ldots, N_\rho\}$ be a set of ρ different nonnegative integers. For each $r \in \{1, \ldots, \gamma\}$, define the r-th residue set of $\mathcal{N}$

$$S_r(\mathcal{N}) = \bigcup_{l=1}^{\rho} \{k_{l,r}\}, \tag{1}$$

where $k_{l,r}$ is the remainder of N_l modulo m_r.

The generalized CRT problem for multiple integers is to reconstruct the set $\mathcal{N}$ from its residue sets $S_r(\mathcal{N})$, $1 \leq r \leq \gamma$. Note that it is unknown which element in $\mathcal{N}$ produces a given element in $S_r(\mathcal{N})$ for any r. Moreover, $|S_r(\mathcal{N})|$ may be strictly less than ρ for some r, since two or more integers in $\mathcal{N}$ may produce the same residue in $S_r(\mathcal{N})$. We use $|\cdot|$ to denote the cardinality of a set.

A basic question for the generalized CRT is to determine the *dynamic range* for the unique recovery. In what follows, we use $\mathcal{M}$ and $S(\mathcal{N})$ to denote the sets $\{m_1, \ldots, m_\gamma\}$ and $S_1(\mathcal{N}) \times \cdots \times S_\gamma(\mathcal{N})$, respectively.

Definition 1. The dynamic range of $\mathcal{M}$, denoted $D_\rho(\mathcal{M})$, is the minimal positive integer D such that there exist two different ρ-subsets $\mathcal{N}, \mathcal{N}'$ of $\{0, \ldots, D\}$ satisfying $S(\mathcal{N}) = S(\mathcal{N}')$.

Equivalently, the dynamic range $D_\rho(\mathcal{M})$ is the largest positive integer D such that the mapping

$$y = S(\mathcal{N}), \mathcal{N} \subseteq \{0, 1, \ldots, D-1\} \text{ and } |\mathcal{N}| = \rho$$

is invertible. For example, $D_1(\mathcal{M}) = \prod_{r=1}^{\gamma} m_r$ by the conventional Chinese remainder theorem. However, due to the unknown correspondence between $\mathcal{N}$ and $S_r(\mathcal{N})$ for any $r \in \{1, \ldots, \gamma\}$, the dynamic range for $\rho > 1$ seems extremely difficult.

Example 1. Let $\gamma = 4$, $\mathcal{M} = \{5, 7, 11, 13\}$, $\rho = 3$, $\mathcal{N} = \{13, 22, 35\}$ and $\mathcal{N}' = \{0, 13, 22\}$. One can check that $S(\mathcal{N}) = S(\mathcal{N}') = \{0, 2, 3\} \times \{0, 1, 6\} \times \{0, 2\} \times \{0, 9\}$. As $\mathcal{N}$ and $\mathcal{N}'$ are two different 3-subsets of $\{0, 1, \ldots, 35\}$, the minimality of $D_3(\mathcal{M})$ implies $D_3(\mathcal{M}) \leq 35$.

The following basic lower bound on $D_\rho(\mathcal{M})$ was obtained by Xia [12]. For a set $\mathcal{S}$, we use $\max \mathcal{S}$ (resp. $\min \mathcal{S}$) to denote the maximum (resp. minimum) value of $\mathcal{S}$.

Proposition 1. *[12] We have*

$$D_\rho(\mathcal{M}) \geq \max\left\{ \prod_{r=1}^{\lfloor \frac{\gamma}{\rho} \rfloor} m_r, m_\gamma \right\}. \tag{2}$$

The lower bound was improved further in [7]. To state their result, we need some notation.

Definition 2. An (ordered) *ρ-partition* of $\mathcal{M}$ is a sequence of (possibly empty) subsets, $\mathcal{M}_1, \ldots, \mathcal{M}_\rho$ of $\mathcal{M}$, denoted $(\mathcal{M}_1, \ldots, \mathcal{M}_\rho)$, such that each m_r belongs to one and only one of these subsets.

Following [7], we define

$$b(\rho) = \max_{(\mathcal{M}_1,\ldots,\mathcal{M}_\rho)} \min_{1\leq l\leq\rho} \prod_{m_r\in\mathcal{M}_l} m_r \tag{3}$$

and

$$c(\rho) = \min_{(\mathcal{M}_1,\ldots,\mathcal{M}_\rho)} \max_{1\leq l\leq\rho} \prod_{m_r\in\mathcal{M}_l} m_r, \tag{4}$$

where the outermost maximum of (3) and the minimum of (4) are taken over all ρ-partitions $(\mathcal{M}_1, \ldots, \mathcal{M}_\rho)$ of $\mathcal{M}$, and $\prod_{m_r\in\mathcal{M}_l} m_r = 1$ if $\mathcal{M}_l = \emptyset$.

The main result of Liao and Xia [7] can now be stated as follows:

Proposition 2. *[7] We have*

$$D_2(\mathcal{M}) \geq \max\left\{b(2), m_\gamma\right\} \tag{5}$$

and for $\rho \geq 3$,

$$D_\rho(\mathcal{M}) \geq \max\left\{ \min\left\{c(\rho), b(2)\right\}, \prod_{r=1}^{\lceil \frac{\gamma}{\rho} \rceil} m_r, m_\gamma \right\}. \tag{6}$$

The goal of this paper is to show that the right-hand side of (6) is simply $c(\rho)$. Moreover, this leads to a simpler proof of (6). We remark that the exact dynamic range for two integers ($\rho = 2$) was obtained recently in [11], by extending a key idea in [15].

2. Simplification of (6)

We begin with bounds on $b(\rho)$ and $c(\rho)$ obtained in [7].

Lemma 1. *[7] Let $\rho \geq 2$. We have*
(i) $b(\rho) \leq \left(\prod_{r=1}^{\gamma} m_r\right)^{\frac{1}{\rho}}$ *and*
(ii) $c(\rho) \geq \max\left\{\prod_{r=1}^{\lceil \frac{\gamma}{\rho} \rceil} m_r, m_\gamma\right\}$.

Lemma 2. *Let $\rho \geq 3$. If*

$$\prod_{r=1}^{\gamma-1} m_r < m_\gamma \tag{7}$$

then $b(2) < c(\rho) = m_\gamma$; otherwise, $c(\rho) \leq b(2)$.

Proof. Assume (7) holds. Let

$$(\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_\rho) = (\{m_1, \ldots, m_{\gamma-1}\}, \{m_\gamma\}, \emptyset, \ldots, \emptyset). \tag{8}$$

Then, by (7), we have

$$\max_{1 \leq l \leq \rho} \prod_{m_r \in \mathcal{M}_l} m_r = \max\left\{\prod_{r=1}^{\gamma-1} m_r, m_\gamma, 1, \ldots, 1\right\} = m_\gamma, \tag{9}$$

which implies $c(\rho) \leq m_\gamma$ by the minimality of $c(\rho)$. On the other hand, by Lemma 1 (ii), $c(\rho) \geq m_\gamma$. This proves $c(\rho) = m_\gamma$.

Now by Lemma 1 (i) and (7),

$$b(2) \leq \left(\prod_{r=1}^{\gamma} m_r\right)^{\frac{1}{2}} < m_\gamma. \tag{10}$$

This completes the proof of the first half.

Next, we assume

$$\prod_{r=1}^{\gamma-1} m_r \geq m_\gamma. \tag{11}$$

Let $(\mathcal{M}_1, \mathcal{M}_2) = (\{m_1, \ldots, m_{\gamma-1}\}, \{m_\gamma\})$. Then, by (11),

$$\min_{1 \leq l \leq 2} \prod_{m_r \in \mathcal{M}_l} m_r = \min\left\{\prod_{r=1}^{\gamma-1} m_r, m_\gamma\right\} = m_\gamma. \tag{12}$$

This, by the maximality of $b(2)$, implies

$$b(2) \geq m_\gamma. \tag{13}$$

Let $(\mathcal{M}_1', \mathcal{M}_2')$ be a bipartition of $\mathcal{M}$ such that

$$b(2) = \min\left\{\prod_{m_r \in \mathcal{M}_1'} m_r, \prod_{m_r \in \mathcal{M}_2'} m_r\right\}. \tag{14}$$

Without loss of generality, we may assume

$$b(2) = \prod_{m_r \in \mathcal{M}_1'} m_r, \tag{15}$$

i.e., $\prod_{m_r \in \mathcal{M}_1'} m_r \le \prod_{m_r \in \mathcal{M}_2'} m_r$. Note that the inequality is necessarily strict since $m_1, \ldots, m_\gamma$ are pairwise coprime. Thus,

$$\prod_{m_r \in \mathcal{M}_1'} m_r < \prod_{m_r \in \mathcal{M}_2'} m_r. \tag{16}$$

From (13), (15) and (16), we have

$$\prod_{m_r \in \mathcal{M}_2'} m_r > m_\gamma \tag{17}$$

and hence $|\mathcal{M}_2'| \ge 2$ since m_γ is the largest modulus in $\mathcal{M}$.

Now let $(\mathcal{M}_{2,1}', \mathcal{M}_{2,1}')$ be any bipartition of $\mathcal{M}_2'$ with $\mathcal{M}_{2,i}' \neq \emptyset$ for $i = 1, 2$. We claim

$$\prod_{m_r \in \mathcal{M}_{2,i}'} m_r \le \prod_{m_r \in \mathcal{M}_1'} m_r \text{ for } i = 1, 2. \tag{18}$$

Suppose to the contrary that (18) does not hold, say,

$$\prod_{m_r \in \mathcal{M}_{2,1}'} m_r > \prod_{m_r \in \mathcal{M}_1'} m_r. \tag{19}$$

Then we consider a new bipartition of $\mathcal{M}$:

$$(\mathcal{M}_1'', \mathcal{M}_2'') = (\mathcal{M}_1' \cup \mathcal{M}_{2,2}', \mathcal{M}_{2,1}'). \tag{20}$$

As $\mathcal{M}_{2,2}' \neq \emptyset$, we have

$$\prod_{m_r \in \mathcal{M}_1''} m_r > \prod_{m_r \in \mathcal{M}_1'} m_r. \tag{21}$$

Combining (19) with (21) leads to

$$\min\left\{\prod_{m_r \in \mathcal{M}_1''} m_r, \prod_{m_r \in \mathcal{M}_2''} m_r\right\} > \prod_{m_r \in \mathcal{M}_1'} m_r \tag{22}$$

and hence $b(2) > \prod_{m_r \in \mathcal{M}'_1} m_r$ by the maximality of $b(2)$. This is a contradiction to (15) and hence (18) is proved.

Now, as $\rho \geq 3$, we can define

$$(\mathcal{M}^*_1, \mathcal{M}^*_2, \ldots, \mathcal{M}^*_\rho) = (\mathcal{M}'_1, \mathcal{M}'_{2,1}, \mathcal{M}'_{2,2}, \emptyset, \ldots, \emptyset), \tag{23}$$

where the last $\rho - 3$ (possibly zero) parts are all empty sets. By (18), we have

$$\max_{1 \leq l \leq \rho} \prod_{m_r \in \mathcal{M}^*_l} m_r = \prod_{m_r \in \mathcal{M}'_1} m_r \tag{24}$$

and hence $c(\rho) \leq \prod_{m_r \in \mathcal{M}'_1} m_r$ by the minimality of $c(\rho)$. This implies $c(\rho) \leq b(2)$ by (15) and hence finishes the proof of this lemma. □

Now, we can give a simplification for the right-hand side of (6).

Theorem 1. *For $\rho \geq 3$, we have*

$$\max\left\{ \min\left\{c(\rho), b(2)\right\}, \prod_{r=1}^{\lceil \frac{\gamma}{\rho} \rceil} m_r, m_\gamma \right\} = c(\rho). \tag{25}$$

Proof. We consider two cases according to Lemma 2 as follows.

If (7) holds, then $b(2) < m_\gamma$. Clearly, $\lceil \frac{\gamma}{\rho} \rceil \leq \gamma - 1$ and hence by (7),

$$\prod_{r=1}^{\lceil \frac{\gamma}{\rho} \rceil} m_r \leq \prod_{r=1}^{\gamma-1} m_r < m_\gamma. \tag{26}$$

Thus, the left-hand side of (25) is equal to m_γ. Note in this case, $m_\gamma = c(\rho)$ by Lemma 2. Thus, (25) holds.

If (7) does not hold, then $c(\rho) \leq b(2)$. Now, (25) clearly follows by Lemma 1 (ii). □

3. A Simple Proof of (6)

We begin with a simple but crucial lemma, whose proof can be regarded as a refinement of that used in [12].

Lemma 3. *Let $N \in \{0, \ldots, c(\rho) - 1\}$ and $\mathcal{N} = \{N_1, \ldots, N_\rho\} \subseteq \{0, \ldots, c(\rho) - 1\}$. If $N \bmod m_r \in S_r(\mathcal{N})$ for each $r \in \{1, \ldots, \gamma\}$, then $N \in \mathcal{N}$.*

Proof. For each $l \in \{1, \ldots, \rho\}$, we define the set

$$\mathcal{A}_l = \{m_r \colon\ N \equiv N_l \bmod m_r\}. \tag{27}$$

For each m_r, since $N \bmod m_r \in S_r(\mathcal{N})$, there exists at least one $l \in \{1, \ldots, \rho\}$ such that $N \equiv N_l \mod m_r$, i.e., $m_r \in \mathcal{A}_l$. Therefore, $\bigcup_{l=1}^{\rho} \mathcal{A}_l = \mathcal{M}$. In order to form a ρ-partition of $\mathcal{M}$, we define

$$\mathcal{M}_l = \left(\bigcup_{i=1}^{l} \mathcal{A}_i\right) - \left(\bigcup_{i=1}^{l-1} \mathcal{A}_i\right) \tag{28}$$

for $l = 1, \ldots, \rho$, where the empty union $\bigcup_{i=1}^{0} \mathcal{A}_i$ is defined as the empty set. Clearly, $(\mathcal{M}_1, \ldots, \mathcal{M}_\rho)$ is a ρ-partition of $\mathcal{M}$ and $\mathcal{M}_l \subseteq \mathcal{A}_l$. Let $\mathcal{M}_{l^*}$ be the one in $\mathcal{M}_1, \ldots, \mathcal{M}_\rho$ such that the product of all $m_r \in \mathcal{M}_{l^*}$ is the maximum, i.e.,

$$\prod_{m_r \in \mathcal{M}_{l^*}} m_r = \max_{1 \le l \le \rho} \prod_{m_r \in \mathcal{M}_l} m_r. \tag{29}$$

Hence, by the minimality of $c(\rho)$,

$$c(\rho) \le \prod_{m_r \in \mathcal{M}_{l^*}} m_r. \tag{30}$$

It suffices to show $N = N_{l^*}$. As $\mathcal{M}_{l^*} \subseteq \mathcal{A}_{l^*}$, the definition of $\mathcal{A}_{l^*}$ implies

$$N \equiv N_{l^*} \bmod m_r \ \text{ for } m_r \in \mathcal{M}_{l^*}. \tag{31}$$

By (30) and the assumption of this lemma, we see that both N and N_{l^*} are less than $\prod_{m_r \in \mathcal{M}_{l^*}} m_r$. Therefore, the conventional CRT implies $N = N_{l^*}$ from (31). □

Now, we can give a proof of (6). We rewrite (6) as follows by Theorem 1.

Theorem 2. *For $\rho \ge 3$, we have*

$$D_\rho(\mathcal{M}) \ge c(\rho). \tag{32}$$

Proof. It follows from Definition 1 that $D_\rho(\mathcal{M}) \ge \rho$. Thus, if $c(\rho) \le \rho$ then (32) holds. Therefore, we may assume $c(\rho) > \rho$. Let $\mathcal{N}$ and $\mathcal{N}'$ be any two ρ-subsets of $\{0, 1, \ldots, c(\rho) - 1\}$ satisfying $S_r(\mathcal{N}') = S_r(\mathcal{N})$ for each $r \in \{1, \ldots, \gamma\}$. It suffices to show $\mathcal{N}' = \mathcal{N}$.

Let $N' \in \mathcal{N}'$. Then $0 \le N' < c(\rho)$ and $N' \bmod m_r \in S_r(\mathcal{N}') = S_r(\mathcal{N})$. By Lemma 3, we obtain that $N' \in \mathcal{N}$ and hence $\mathcal{N}' \subseteq \mathcal{N}$. Similarly, $\mathcal{N} \subseteq \mathcal{N}'$ and hence $\mathcal{N}' = \mathcal{N}$, as desired. □

We remark that the equality in (32) may hold for some special cases. Consider Example 1. Clearly, $c(3) = 5 \times 7 = 35$ and hence $D_3(\mathcal{M}) \ge 35$. Recalling $D_3(\mathcal{M}) \le 35$ in Example 1, we have $D_3(\mathcal{M}) = 35$.

Acknowledgements. This work was partially supported by the 973 Program under Grant 2013CB329404, the NSFC (Nos.61370147, 11471273, 11561058, 61563046, and 61462074), and the Fundamental Research Funds for the Central Universities (No. ZYGX2013Z005). We are also grateful to the anonymous referee for his/her helpful suggestions.

References

[1] B. Arazi, A generalization of the Chinese remainder theorem, *Pac. J. Math.* **70** (1977), 289-296.

[2] C. C. Chang and Y. P. Lai, A fast modular square computing method based on the generalized chinese remainder theorem for prime moduli, *Appl. Math. Comput.* **161** (2005), 181-194.

[3] I. M. Davydova and E. Y. Fedoseeva, Generalization of the Chinese remainder theorem, *Vestnik St Petersburg University Mathematics* **40** (2007), 209-217.

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

[5] M. A. Fiol, Congruences in Z^n, finite Abelian groups and the Chinese remainder theorem, *Discrete Math.* **67** (1987), 101-105.

[6] O. Goldreich, D. Ron and M. Sudan, Chinese remaindering with errors, *IEEE Trans. Inf. Theory* **46** (2000), 1330-1338.

[7] H. Liao and X.-G. Xia, A sharpened dynamic range of a generalized Chinese remainder theorem for multiple integers, *IEEE Trans. Inf. Theory* **53** (2007), 428-433.

[8] X. P. Li, X.-G Xia, W. J. Wang and W. Wang, A robust generalized Chinese remainder theorem for two integers, *IEEE Trans. Inf. Theory* **62** (2016), 7491 - 7504.

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

[10] O. Ore, The general Chinese remainder theorem, *Amer. Math. Monthly* **59** (1952), 165-370.

[11] W. Wang, X. P. Li, X.-G. Xia and W. J. Wang, The largest dynamic range of a generalized Chinese remainder theorem for two integers, *IEEE Signal Process. Lett.* **22** (2015), 254-258.

[12] X.-G. Xia, On estimation of multiple frequencies in undersampled complex valued waveforms, *IEEE Trans. Signal Process.* **47** (1999), 3417-3419.

[13] X.-G. Xia and 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** (2005), 768-771.

[14] X. -G. Xia and G. Wang, Phase unwrapping and a robust Chinese remainder theorem, *IEEE Signal Process. Lett.* **14** (2007), 247-250.

[15] L. Xiao and X.-G. Xia, A generalized Chinese remainder theorem for two integers, *IEEE Signal Process. Lett.* **21** (2014), 55-59.

[16] L. Yu and L. Luo, The generalization of the Chinese remainder theorem, *Acta Math. Sin. (Engl. Ser.)* **18** (2002), 531-538.