New Results on Multidimensional Chinese Remainder Theorem

Yuan-Pei Lin, See-May Phoong, and P. P. Vaidyanathan

Abstract— **The Chinese remainder theorem (CRT) [1] has been well known for applications in fast DFT computations and computer arithmetic. In [2], Guessoum and Mersereau first made headway in extending the CRT to multidimensional (MD) nonseparable systems and showing its usefulness. This letter will generalize the result and present a more general form. This more general MDCRT is an exact counterpart of 1DCRT.**

I. Introduction

THE Chinese remainder theorem (CRT) has been well known in the signal processing community in the context of fast DFT computations. It also finds applications in computer arithmetic using modular techniques, e.g., multiplication of very large integers [3]. The problem of efficient computation for an M-point DFT was studied extensively in the past. When M is a composite number, Cooley and Tukey suggested using index maps to achieve fast computation [4]. However, in their approach, there are some twiddle factors involved. To eliminate the twiddle factors, the CRT is used [5].

A natural question is how to extend the CRT to the MD case so that it can be used in the computation of multidimensional DFT's (MDFT's) or other applications in MD systems. The first extension of the CRT to the nonseparable MD case was advanced by Guessoum and Mersereau [2]. Even though this result applies only to a restricted class, the authors have already shown its usefulness in the computation of nonseparable DFT's. In this letter, we will generalize this result to a broader class of MD nonseparable systems. This will allow computation of a broader class of MDFT. The aim of this letter is to state and prove the generalized form of the MDCRT.[1] Applications will be discussed in future publications.

A. Notations

1) Boldfaced lower-case letters are used to represent vectors, and boldfaced upper-case letters are reserved for matrices. The notation $\mathbf{A}^T$ represents the transpose of $\mathbf{A}$. 2) Matrix $\mathbf{I}$ denotes an identity matrix. 3) A $D \times D$ diagonal matrix $\mathbf{\Lambda}$ with diagonal entries $\lambda_1, \lambda_2, \ldots, \lambda_D$ will be denoted by $\mathbf{\Lambda} = diag(\lambda_1, \lambda_2, \ldots, \lambda_D)$.

Manuscript received July 16, 1994; approved September 11, 1994. This work was supported by NSF grant MIP 92-15785, Tektronix, Inc., and Rockwell International. The assosciate editor coordinating the review of this letter and approving it for publication was H. J. Trussell.

The authors are with the Department of Electrical Engineering, California Institute of Technology, Pasadena, CA 91125 USA.

IEEE Log Number 9406536.

[1] Subsequent to the submission of this letter, we came across [6] and [7], which deal with a closely related topic.

B. Definitions and Fundamentals of Integer Matrices, [2] and [8]:

1) *Unimodular matrix*: An integer matrix $\mathbf{U}$ is unimodular if $|det(\mathbf{U})| = 1$.
2) *Left divisor, left common divisor*: An integer matrix $\mathbf{A}$ is a left divisor of a integer matrix $\mathbf{M}$ if $\mathbf{A}^{-1}\mathbf{M}$ is an integer matrix. If $\mathbf{M}$ and $\mathbf{L}$ have the same left divisor $\mathbf{A}$, $\mathbf{A}$ is a left common divisor of $\mathbf{M}$ and $\mathbf{L}$.
3) *Coprimeness*: Two matrices $\mathbf{M}$ and $\mathbf{L}$ are called left (right) coprime if every left (right) common divisor is unimodular. When $\mathbf{M}$ and $\mathbf{L}$ are left and right coprime, we will simply call them coprime.
4) *The $\mathcal{N}(\mathbf{M})$ notation*: Let $\mathbf{M}$ be a $D \times D$ nonsingular integer matrix. The notation $\mathcal{N}(\mathbf{M})$ is defined as $\mathcal{N}(\mathbf{M}) = \{\mathbf{n} \mid \mathbf{n} = \mathbf{M}\mathbf{x}, \mathbf{x} \in [0,1)^D, \mathbf{n} \text{ is an integer vector}\}$. The number of elements in $\mathcal{N}(\mathbf{M})$ is equal to $|det(\mathbf{M})|$. In the 1-D case, $D = 1$, and $\mathcal{N}(\mathbf{M}) = \{0, 1, 2, \ldots, \mathbf{M} - 1\}$.
5) *Smith form*: A $D \times D$ integer matrix $\mathbf{M}$ can always be factorized into a so-called Smith form $\mathbf{M} = \mathbf{U}\mathbf{\Lambda}\mathbf{V}$, where $\mathbf{U}$ and $\mathbf{V}$ are unimodular, and $\mathbf{\Lambda} = diag(\lambda_1, \lambda_2, \ldots, \lambda_D)$ is unique with λ_i dividing λ_{i+1}.
6) *Division theorem for integer vectors*: A D-dimensional integer vector $\mathbf{n}$ has a unique representation with respect to a $D \times D$ integer matrix $\mathbf{M}$, $\mathbf{n} = \mathbf{n}_0 + \mathbf{M}\mathbf{k}, \mathbf{n}_0 \in \mathcal{N}(\mathbf{M})$. This relation is denoted by $\mathbf{n} = \mathbf{n}_0 \bmod \mathbf{M}$.

II. Previous Results

A. Chinese Remainder Theorem (1-D)

Assume M is a positive composite integer, and $M = \prod_{i=1}^{\mu} M_i$, where M_i's are pairwise coprime. Let $r = n \bmod M$, and $r_i = n \bmod M_i$; then

$$r = \left(\sum_{i=1}^{\mu} a_i r_i \right) \bmod M, \quad \text{with } a_i \triangleq \left(\prod_{k=1, k \neq i}^{\mu} M_k \right)^{\phi(M_i)} \tag{2.1}$$

where $\phi(M)$ (the Euler Totient function) is the number of positive integers less than M and coprime to M.

Remarks:

1) The Euler Totient function $\phi(M)$ has the property that $L^{\phi(M)} = 1 \bmod M$, for any positive integer L that is coprime to M.
2) The quantities a_i and M_j are related by $a_i = 1 \bmod M_i$, and $a_i = 0 \bmod M_j$, $i \neq j$.

B. The Multidimensional DFT and 2-D CRT

First, we need some reviews of MDFT of MD signals.

1) Multidimensional DFT: The MDFT [9] of an MD signal $x(\mathbf{n})$ with respect to a $D \times D$ integer matrix $\mathbf{M}$ is given by $X(\mathbf{k}) = \sum_{\mathbf{n} \in \mathcal{N}(\mathbf{M})} x(\mathbf{n}) \exp[-j2\pi \mathbf{k}^T \mathbf{M}^{-1} \mathbf{n}], \mathbf{k} \in \mathcal{N}(\mathbf{M}^T)$.

Express $\mathbf{M}$ in Smith form $\mathbf{M} = \mathbf{U}\mathbf{\Lambda}\mathbf{V}$, and $\mathbf{\Lambda} = diag(\lambda_1, \lambda_2, \ldots, \lambda_D)$. The MDFT also assumes the form

$$X(\mathbf{k}) = \sum_{\mathbf{n} \in \mathcal{N}(\mathbf{M})} x(\mathbf{n}) \exp[-j2\pi (\mathbf{V}^{-T}\mathbf{k})^T \mathbf{\Lambda}^{-1} (\mathbf{U}^{-1}\mathbf{n})], \quad \mathbf{k} \in \mathcal{N}(\mathbf{M}^T). \tag{2.2}$$

The operations $\mathbf{V}^{-T}\mathbf{k}$ and $\mathbf{U}^{-1}\mathbf{n}$ are mere rearrangements, and no multiplications are needed. Therefore, direct computation of $X(\mathbf{k})$ requires DFT calculations of lengths $\lambda_1, \lambda_2, \ldots,$ and λ_D. To achieve fast computation, we would like to break each of these DFT's into smaller ones. This can be accomplished by decomposing $\mathbf{M}$ in a manner similar to what we did in 1DCRT.

2) Previously Known 2-D CRT: The problem of 2DCRT was first addressed in [2]. The results hold for 2×2 nonsingular integer matrix $\mathbf{M}$ with Smith form $\mathbf{M} = \mathbf{U}diag(1, pq)\mathbf{V}$, where p and q are prime numbers. Direct computation of MDFT with respect to $\mathbf{M}$ requires a DFT calculation of length pq. It is shown therein that this operation of the pq-point DFT can be divided into a p-point DFT and a q-point DFT. However, the result of [2] is only for a matrix $\mathbf{M}$ whose determinant is a product of two prime numbers, and we can only break a long DFT into two smaller DFT's. In the next section, we will present the more general MDCRT, which is an exact counterpart of 1DCRT. As a result, a long DFT can be divided into many smaller DFT's.

III. New Results on Multidimensional CRT

To emulate the 1-D situation, the first step is to factorize a given $D \times D$ nonsingular integer matrix $\mathbf{M}$ into several factors that are pairwise coprime in the MD sense. To do this, we start from the Smith form $\mathbf{M} = \mathbf{U}\mathbf{\Lambda}\mathbf{V}$ and factorize $\mathbf{\Lambda}$ into diagonal matrices that are pairwise coprime $\mathbf{\Lambda} = \mathbf{\Lambda}_1\mathbf{\Lambda}_2 \ldots \mathbf{\Lambda}_\mu$ with $\mathbf{\Lambda}_i = diag(\lambda_1^{(i)}, \lambda_2^{(i)}, \ldots, \lambda_D^{(i)})$. Notice that $\mathbf{\Lambda}_i$ and $\mathbf{\Lambda}_j$ are coprime if and only if $\gcd(\lambda_k^{(i)}, \lambda_k^{(j)}) = 1$, for $k = 1, 2, \ldots, D$. Therefore, the factorization can be done as in the scalar case. We can also write $\mathbf{M}$ as

$$\mathbf{M} = (\mathbf{U}\mathbf{\Lambda}_1\mathbf{U}^{-1})(\mathbf{U}\mathbf{\Lambda}_2\mathbf{U}^{-1}) \ldots (\mathbf{U}\mathbf{\Lambda}_\mu\mathbf{U}^{-1})\mathbf{U}\mathbf{V} \tag{3.1}$$

that is, $\mathbf{M} = \mathbf{M}_1\mathbf{M}_2 \ldots \mathbf{M}_\mu\mathbf{U}\mathbf{V}$, with $\mathbf{M}_i = \mathbf{U}\mathbf{\Lambda}_i\mathbf{U}^{-1}$. Since the ordering of $\mathbf{M}_i$ does not affect the product, we will use $\prod_{i=1}^{\mu} \mathbf{M}_i$ to denote $\mathbf{M}_1\mathbf{M}_2 \ldots \mathbf{M}_\mu$. Each $\mathbf{M}_i$ can be pulled to the left of the product; every $\mathbf{M}_i$ is a left divisor of $\mathbf{M}$. It can be verified that $\mathbf{M}_i = \mathbf{U}\mathbf{\Lambda}_i\mathbf{U}^{-1}$ are pairwise coprime if and only if $\mathbf{\Lambda}_i$ are pairwise coprime.

Theorem 3.1: Let $\mathbf{M}$ be a $D \times D$ nonsingular integer matrix with Smith form $\mathbf{M} = \mathbf{U}\mathbf{\Lambda}\mathbf{V}$. The matrix $\mathbf{\Lambda} = diag(\lambda_1, \lambda_2, \ldots \lambda_D)$. Factorize $\mathbf{M}$ as in (3.1), i.e., $\mathbf{M} = (\prod_{i=1}^{\mu} \mathbf{M}_i)\mathbf{U}\mathbf{V}$, where the matrices $\mathbf{M}_i$ given by $\mathbf{M}_i = \mathbf{U}\mathbf{\Lambda}_i\mathbf{U}^{-1}$ are pairwise coprime. Let $\mathbf{r} = \mathbf{n} \bmod \mathbf{M}$ and $\mathbf{r}_i = \mathbf{n} \bmod \mathbf{M}_i, i = 1, 2, \ldots, \mu$.Then

$$\mathbf{r} = \left(\sum_{i=1}^{\mu} \mathbf{A}_i \mathbf{r}_i \right) \bmod \mathbf{M}, \quad \text{with } \mathbf{A}_i \triangleq \left(\prod_{j=1, j \neq i}^{\mu} \mathbf{M}_j \right)^{\Phi(\mathbf{M}_i)} \tag{3.2}$$

where $\Phi(\mathbf{M}_i) = \mathrm{lcm}(\phi(\lambda_1^{(i)}), \phi(\lambda_2^{(i)}), \ldots, \phi(\lambda_D^{(i)}))$. ■

The role of $\mathbf{A}_i$ corresponds to that of a_i in 1DCRT. We will see that $\mathbf{A}_i$ and $\mathbf{M}_j$ are related in the same way as a_i and M_j are related in the 1-D case. The proof of the theorem will be presented after Lemma 3.1.

Lemma 3.1: The matrix $\mathbf{A}_i$ given by $\mathbf{A}_i = \left(\prod_{j=1, j \neq i}^{\mu} \mathbf{M}_j\right)^{\Phi(\mathbf{M}_i)}$ can be written as

$$\mathbf{A}_i = \mathbf{M}_i\mathbf{B}_{ii} + \mathbf{I}, \quad \text{and} \quad \mathbf{A}_i = \mathbf{M}_j\mathbf{B}_{ji}, \quad j \neq i \tag{3.3}$$

for some integer matrices $\mathbf{B}_{ji}, 1 \leq i, j, \leq \mu$. ■

Proof of Lemma 3.1: Since the $\mathbf{M}_i'$s commute, the relation $\mathbf{A}_i = \mathbf{M}_j\mathbf{B}_{ji}$ follows from the definition of $\mathbf{A}_i$. We only need to show the first relation. Using $\mathbf{M}_i = \mathbf{U}\mathbf{\Lambda}_i\mathbf{U}^{-1}$, we get $\mathbf{A}_i = \mathbf{U}\left(\prod_{j=1, j \neq i}^{\mu} \mathbf{\Lambda}_j\right)^{\Phi(\mathbf{M}_i)} \mathbf{U}^{-1}$, but the fact that $\mathbf{\Lambda}_i's$ are pairwise coprime means that the diagonal entries of $\prod_{j=1, j \neq i}^{\mu} \mathbf{\Lambda}_j$ and $\mathbf{\Lambda}_i$ are coprime. By the property of the Euler Totient function, we have

$$\left(\prod_{j=1, j \neq i}^{\mu} \mathbf{\Lambda}_j \right)^{\Phi(\mathbf{M}_i)} = \mathbf{\Lambda}_i\mathbf{D} + \mathbf{I}, \quad i = 1, 2, \ldots, \mu \tag{3.4}$$

for some diagonal integer matrix $\mathbf{D}$. Premultiplying (3.4) by $\mathbf{U}$ and postmultiplying (3.4) by $\mathbf{U}^{-1}$ will give us $\mathbf{U}\left(\prod_{j=1, j \neq i}^{\mu} \mathbf{\Lambda}_j\right)^{\Phi(\mathbf{M}_i)} \mathbf{U}^{-1} = (\mathbf{U}\mathbf{\Lambda}_i\mathbf{U}^{-1})(\mathbf{U}\mathbf{D}\mathbf{U}^{-1}) + \mathbf{I}$. Letting $\mathbf{B}_{ii} = \mathbf{U}\mathbf{D}\mathbf{U}^{-1}$, we get the desired result. △

Proof of Theorem 3.1: Let $\mathbf{r}' = (\sum_{i=1}^{\mu} \mathbf{A}_i\mathbf{r}_i) \bmod \mathbf{M}$. The proof will be done in two steps. First, we show that $\mathbf{r}' = \mathbf{r}_i \bmod \mathbf{M}_i, i = 1, 2, \ldots, \mu$. Based on this fact, it can be shown that $\mathbf{r}' = \mathbf{r}$.

Step 1: Substituting (3.3) into the definition of $\mathbf{r}'$ and rearranging, we get $\mathbf{r}' = \mathbf{r}_i + \mathbf{M}\mathbf{k} + \mathbf{M}_i \sum_{j=1}^{\mu} \mathbf{B}_{ij}\mathbf{r}_j$, for some integer vector $\mathbf{k}$. From this expression, we can observe that $\mathbf{r}' = \mathbf{r}_i \bmod \mathbf{M}_i$.

Step 2: Let $\mathbf{r}'' = \mathbf{r}' - \mathbf{r}$, and then, $\mathbf{r}'' = \mathbf{M}\mathbf{x}, \mathbf{x} \in (-1, 1)^D$. From Step 1, we know $\mathbf{r}'' = \mathbf{0} \bmod \mathbf{M}_i$; therefore, $\mathbf{r}'' = \mathbf{M}_i\mathbf{d}_i, i = 1, 2, \ldots, \mu$, for some integer vectors $\mathbf{d}_i$. Premultiplying both sides by $\mathbf{U}^{-1}$ yields $\mathbf{U}^{-1}\mathbf{r}'' = \mathbf{\Lambda}_i(\mathbf{U}^{-1}\mathbf{d}_i)$. This implies that $\lambda_k^{(i)}$ divides the kth entry of $\mathbf{U}^{-1}\mathbf{r}''$. Since $\lambda_k^{(1)}, \lambda_k^{(2)}, \ldots, \lambda_k^{(\mu)}$ are pairwise coprime, the kth entry of $\mathbf{U}^{-1}\mathbf{r}''$ is a multiple of $\lambda_k = \prod_{i=1}^{\mu} \lambda_k^{(i)}$. Therefore, we can write $\mathbf{U}^{-1}\mathbf{r}'' = \mathbf{\Lambda}\mathbf{d}$, for some integer vector $\mathbf{d}$, or $\mathbf{r}'' = (\mathbf{U}\mathbf{\Lambda}\mathbf{V})(\mathbf{V}^{-1}\mathbf{d})$. Defining $\mathbf{v} = \mathbf{V}^{-1}\mathbf{d}$, we get $\mathbf{r}'' = \mathbf{M}\mathbf{v}$, but $\mathbf{r}'' = \mathbf{M}\mathbf{x}$, and $\mathbf{x}$ is an integer vector only when $\mathbf{x} = \mathbf{0}$. This implies $\mathbf{r}'' = \mathbf{0}$, and the proof is complete. △

Remark: To achieve efficiency, we would like to break a MDFT into as many small DFT's as possible. For this reason, we would like to factorize $\mathbf{M}$ into as many pairwise coprime factors as possible. This hinges on the diagonal matrix $\mathbf{\Lambda}$. In our construction, the property of the Smith form is not used, and $\mathbf{M}$ need not be diagonalized in Smith form. For example,

we could use $\mathbf{M} = \hat{\mathbf{U}}\hat{\mathbf{\Lambda}}\hat{\mathbf{V}}$, where $\hat{\mathbf{U}}$ and $\hat{\mathbf{V}}$ are unimodular, and $\hat{\mathbf{\Lambda}}$ is diagonal. In this situation, one wonders if we can get more pairwise coprime factors out of $\mathbf{M}$ if we start the factorization from $\mathbf{M} = \hat{\mathbf{U}}\hat{\mathbf{\Lambda}}\hat{\mathbf{V}}$. However, we have found that doing this will give us just as many factors as the Smith form will.

IV. Conclusion

We have given a general form of the MDCRT, which is an exact counterpart of 1DCRT. We expect that MDCRT can be used in MD systems for many applications similar to the 1-D case. More on this subject will be studied in future publications.

References

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

[2] A. Guessoum and R. M. Mersereau, "Fast algorithms for the multidimensional discrete Fourier transform," *IEEE Trans. Acoust. Speech Signal Processing*, vol. ASSP-34, pp. 937-943, Aug. 1986.

[3] D. E. Knuth, *The Art of Computer Programming*. Reading, MA: Addison-Wesley, 1969.

[4] J. W. Cooley and J. W. Tukey, "An algorithm for the machine computation of complex Fourier series," *Math. Comput.*, vol. 19, pp. 297-301, Apr. 1965.

[5] L. H. Thomas, "Using a computer to solve problems in physics," in *Applications of Digital Computers*.Boston: Ginn, 1963.

[6] R. Bernardini, G. M. Cortelazzo, and G. A. Mian, "A general scrambling rule for multidimensional FFT algorithms," *IEEE Trans. Signal Processing*, vol. 42, pp. 1786-1794, July 1994.

[7] ——, "A new technique for twiddle-factor elimination in multidimensional FFT's," *IEEE Trans. Signal Processing*, vol. 42, pp. 2176-2178, Aug. 1994.

[8] P. P. Vaidyanathan, *Multirate Systems and Filter Banks*. Englewood Cliffs, NJ: Prentice Hall, 1993.

[9] D. E. Dudgeon and R. M. Mersereau, *Multidimensional Digital Signal Processing*. Englewood Cliffs, NJ: Prentice Hall, 1984.