Journal of Mathematical Research & Exposition
Vol.23, No.1, 21–27, February, 2003

Matrix Decomposition and Calculation of Chrestenson Spectra *

HU Lei

(State Key Laboratory of Information Security, Graduate School, Academic Sinica, Beijing 100039, China)

Abstract: Calculation of a variation of discrete Fourier transform, Chrestenson spectra of functions of n indeterminates over integer modulo m (composite integer), is considered. Based on sparse matrix decomposition, two fast algorithms with complexity $O(m^n n \sum_{i=1}^{r} p_i)$ are given to calculate the Chrestenson spectra, where $p_1 p_2 \cdots p_r$ is the prime factor decomposition of m.

Key words: discrete Fourier transform; Chrestenson spectra; sparse matrix; fast algorithm.

Classification: AMS(2000) 15A33,94A60/CLC number: O151, TP309

Document code: A **Article ID**: 1000-341X(2003)01-0021-07

1. Introduction

Discrete Fourier transform (DFT) is applied in many fields such as communication, geophysical signal processing and computer tomography[1]. The fast Fourier transform (FFT), fast algorithms on DFT, is widely researched[2,3]. In cryptology, a variation of DFT, Walsh transform, is an important tool to study properties of cryptological functions over the binary field[4]. Recently, functions over $Z/(m)$, the integer modulo m (composite integer) residue class ring, are applied to the fields of cryptology, designs of circuits and digital communication[5]. The corresponding tool for functions over $Z/(m)$ is Chrestenson spectrum, a concept which can be traced back to [6], but fast computation for it has not been well developed. Based on sparse matrix decomposition, a fast algorithm with complexity $O(m^n nm)$ is given in [5] to calculate Chrestenson spectra of functions over $Z/(m)$ of n indeterminates. In this paper, we further develop the idea of [5], and by more sparse matrix decomposition, a faster algorithm with complexity $O(m^n n \sum_{i=1}^{r} p_i)$ is

*Received date: 2000-08-03
Foundation item: Supported by the National Natural Science Foundation of China (90104034), the 863 Program (2002AA141020) and the Guangdong Provincial Natural Science Foundation (990336)
Biography: HU Lei (1967-), male, Ph.D., Professor.

deduced, where $p_1p_2\cdots p_r$ is the prime factor decomposition of m. This algorithm is a generalization of that in [2] for the case of $n = 1$. When m is a power of prime, we develop another sparse matrix decomposition with simple and direct form, which induces another fast algorithm.

2. Chrestenson spectra

Let $R = Z/(m)$ be the integer module m residue class ring, all elements of R are naturally regarded as integers in $[0, m-1]$. Let $f(x_1, \cdots, x_n)$ be a function over R of n indeterminates, the Chrestenson spectrum at $w = (w_1, \cdots, w_n) \in R^n$ of f is defined as

$$S_{(f)}(w) = \sum_{x \in R^n} \xi_m^{f(x) - w \cdot x}, \tag{1}$$

where $\xi_m = \exp(\frac{2\pi\sqrt{-1}}{m})$ and $w \cdot x = w_1x_1 + \cdots + w_nx_n$. The set $S = \{S_{(f)}(w) \mid w \in R^n\}$ is called the Chrestenson spectra of f.

Obviously, the complexity to calculate directly S according to (1) is $O(m^{2n})$. To accelerate the calculation of S, we define the Chrestenson transform matrix M_n for functions of n indeterminates as the matrix of order m^n

$$M_n = (\xi_m^{-A \cdot B})_{A,B \in R^n}, \tag{2}$$

where the row label A and the column label B are arranged in the ascending order of the m-adic integers corresponding to A and B, here an n-tuple $A = (a_{n-1}, \cdots, a_1, a_0) \in R^n$ is naturally corresponding to the m-adic integer $\sum_{i=0}^{n-1} a_i m^i$. Write S and the value set of f as column vectors $S = (S_{(f)}(w))_{w \in R^n}$ and $F = (\xi_m^{f(x)})_{x \in R^n}$, where the column labels of S and F are arranged in the same order as above A. Then

$$S = M_n \cdot F. \tag{3}$$

Let $G = (g_{ij})$ and H be respectively $u \times v$ and $u' \times v'$ matrices, the tensor product $G \otimes H$ of G and H is the $uu' \times vv'$ matrix[3]

$$\begin{pmatrix} g_{11}H & \cdots & g_{1v}H \\ & \cdots & \\ g_{u1}H & \cdots & g_{uv}H \end{pmatrix}.$$

For each $i = 1, \cdots, n$, put

$$D_i = I^{(m)} \otimes \cdots \otimes I^{(m)} \otimes M_1 \otimes I^{(m)} \otimes \cdots \otimes I^{(m)},$$

where M_1 is in the i-th position of the tensor product and $I^{(m)}$ denotes the identity matrix of order m. Then[5]

$$M_n = M_1 \otimes M_1 \otimes \cdots \otimes M_1 = D_nD_{n-1}\cdots D_1, \tag{4}$$

and

$$S = D_n(D_{n-1}(\cdots(D_2(D_1F))\cdots)). \tag{5}$$

Note that any nonzero entries of D_i is of form ξ_m^e, and since that $\xi_m^m = 1$, the matrix multiplication in (5) only involves additions of polynomials of ξ_m of degree at most $m-1$. (Multiplying a polynomial of ξ_m by a monomial of ξ_m is only a cyclic shift of m-tuple when polynomials of ξ_m of degree at most $m-1$ are represented as m-tuples.) So, the complexity of the calculation of S can be measured by the total number of the nonzero entries in the D_i's. Since D_i is a sparse matrix with m nonzero entries in each row, it is easy to see that the calculation complexity according to (5) is $O(m^{n+1}n)$.

Remark 1 The calculation of DFT of general complex functions usually involves error of some extent (so-called computational noise) since inaccurate real approximation to complex values and limited computation precision[1]. This phenomenon does not exist in the calculation of Chrestenson spectra since only operations of algebraic integers are required.

3. Sparse matrix decomposition and improved fast algorithm

We further accelerate the calculation of S by decomposing M_1 into a product of sparse matrices.

Let $m = p_1 p_2 \cdots p_r$ be the prime factor decomposition of m, where $r > 1$ and some pairs of the p_i's may be the same. We introduce two mixed-adic representation of integers in $[0, m-1]$, each of which represents each integer i in $[0, m-1]$ as a unique r-tuple $(i_{r-1}, \cdots, i_1, i_0)$ satisfying

$$0 \le i_{r-1} < p_r, \cdots, 0 \le i_1 < p_2, 0 \le i_0 < p_1. \tag{6}$$

Representation 1 Dividing i and the remainder in the preceding division step in turn by $p_1 p_2 \cdots p_{r-1}$, $p_1 p_2 \cdots p_{r-2}$, $\cdots$, $p_1 p_2$, p_1, we have

$$i = p_1 p_2 \cdots p_{r-1} i_{r-1} + p_1 p_2 \cdots p_{r-2} i_{r-2} + \cdots + p_1 p_2 i_2 + p_1 i_1 + i_0.$$

The resulting r-tuple $(i_{r-1}, \cdots, i_1, i_0)$ is denoted by $\mathrm{rep}_1(i) = (i_{r-1}, \cdots, i_1, i_0)$.

Representation 2 Dividing i and the quotient in the preceding division step in turn by p_r, p_{r-1}, $\cdots$, p_2, we have

$$i = i_{r-1} + p_r(i_{r-2} + p_{r-1}(i_{r-3} + p_{r-2}(\cdots + p_3(i_1 + p_2 i_0)\cdots))).$$

This r-tuple $(i_{r-1}, \cdots, i_1, i_0)$ is denoted by $\mathrm{rep}_2(i) = (i_{r-1}, \cdots, i_1, i_0)$.

Clearly, if $p_1 = p_2 = \cdots = p_r = p$ and $m = p^r$, then $\mathrm{rep}_1(i) = (j_{r-1}, \cdots, j_1, j_0)$ is the usual p-adic representation of i while $\mathrm{rep}_2(i)$ is the inverse code of this p-adic representation, i.e., $\mathrm{rep}_2(i) = (j_0, j_1, \cdots, j_{r-1})$. Set

$$\Gamma_i = \{0, 1, \cdots, p_i - 1\}, \quad i = 1, 2, \cdots, r,$$

$$\Gamma = \Gamma_r \times \cdots \times \Gamma_2 \times \Gamma_1,$$

define σ be the lexicographical order over Γ with prior of more right components, i.e., the lexicographical order satisfying

$$(1, 0, \cdots, 0) <_\sigma (0, 1, 0, \cdots, 0) <_\sigma \cdots <_\sigma (0, \cdots, 0, 1).$$

It is easy to see that the integer domain $[0, m-1]$ is one-to-one corresponding to Γ under each of the above two representations, and under Representation 2 the usual ascending order over $[0, m-1]$ is corresponding to the ascending order over Γ under σ.

Now we redefine the Chrestenson transform matrices and the spectra as

$$M_1 = (\varsigma_m^{ij})_{0\le i,j<m},\ M_n = (\varsigma_m^{A\cdot B})_{A,B\in R^n},\ S = (S_{(f)}(i))_{i\in R^n}, \tag{7}$$

where $\varsigma_m = \xi_m^{-1} = \exp(\frac{-2\pi\sqrt{-1}}{m})$, the column labels j and B are respectively arranged in the usual ascending order of integers and corresponding m-adic integers, the row label i is arranged such that $\mathrm{rep}_1(i)$ is ascending under σ, and the row label A is arranged in the following ascending order: let $A = (a_{n-1}, \cdots, a_1, a_0) \in R^n$, $A' = (a'_{n-1}, \cdots, a'_1, a'_0) \in R^n$, $A \neq A'$, A is called smaller than A' if

$$a_1 = a'_1, a_2 = a'_2, \cdots, a_s = a'_s, \mathrm{rep}_1(a_{s+1}) <_\sigma \mathrm{rep}_1(a'_{s+1})$$

for some integer s in $[0, n-1]$. The M_1 and M_n in (7) are respectively images of the original M_1 and M_n in (2) under some matrix row permutations. Formula (3) and the formula $M_n = M_1 \otimes \cdots \otimes M_1$ also hold for the new M_1 and M_n.

Let $\mathrm{rep}_1(i) = (i_{r-1}, \cdots, i_1, i_0)$, $\mathrm{rep}_2(j) = (j_{r-1}, \cdots, j_1, j_0)$. Set $q = p_1 p_2 \cdots p_{r-1}$, $p = p_r$, $m = pq$, and write

$$i = i_{r-1}q + i', j = j_{r-1} + j'p, \tag{8}$$

where $0 \le i', j' < q, 0 \le i_{r-1}, j_{r-1} < p$, and $\mathrm{rep}_1(i') = (0, i_{r-2}, \cdots, i_1, i_0)$. Then

$$\varsigma_m^{ij} = \varsigma_m^{i_{r-1}j_{r-1}q + i'j_{r-1}} \varsigma_q^{i'j'}.$$

Divide evenly M_1 into q^2 submatrices of order p, for each submatrix all of its entries ς_m^{ij} correspond to the same i' and the same j' according to (8) while i_{r-1} and j_{r-1} vary in $[0, p-1]$ in the ascending order. For each $i' \in [0, q-1]$, define a matrix of order p

$$T_r(i') = (\varsigma_m^{qkl+i'l})_{0\le k,l<p}. \tag{9}$$

Then the block form of M_1 is $(\varsigma_q^{i'j'} T_r(i'))_{0\le i',j'<q}$. Define a diagonal block matrix Q_r and a matrix M' of order q as

$$Q_r = \mathrm{diag}(T_r(i'))_{0\le i'<q},\ M' = (\varsigma_q^{i'j'})_{0\le i',j'<q}, \tag{10}$$

where i' and j' are arranged in similar order as i and j in (7). Since

$$\varsigma_q^{i'j'} T_r(i') = T_r(i') \cdot (\varsigma_q^{i'j'} I^{(p)}),$$

one has

$$M_1 = Q_r \cdot (M' \otimes I^{(p)}). \tag{11}$$

It is clear that M' is a matrix of order q and with similar structure as M_1, and therefore we can further decompose M' into a form similar as the right side of (11) provided $r-1 > 1$. Rewrite (7),(9),(10) for $s = 2, 3, \cdots, r$ as

$$\begin{gathered} M(p_1 p_2 \cdots p_s) = (\varsigma_{p_1 p_2 \cdots p_s}^{ij})_{0\le i,j<p_1 p_2 \cdots p_s}, \\ T_s(i') = (\varsigma_{p_1 p_2 \cdots p_s}^{p_1 p_2 \cdots p_{s-1} kl + i'l})_{0\le k,l<p_s},\ \text{for } 0 \le i' < p_1 p_2 \cdots p_{s-1}, \\ Q_s = \mathrm{diag}(T_s(i'))_{0\le i'<p_1 p_2 \cdots p_{s-1}}. \end{gathered} \tag{12}$$

Similarly as in (11) one deduces that

$$\begin{aligned} M(p_1p_2\cdots p_s) =& Q_s\cdot(M(p_1p_2\cdots p_{s-1})\otimes I^{(p_s)}) \\ =& Q_s(Q_{s-1}\otimes I^{(p_s)})(Q_{s-2}\otimes I^{(p_{s-1}p_s)})\cdots(Q_1\otimes I^{(p_2p_3\cdots p_s)}). \end{aligned} \tag{13}$$

Put

$$H_r = Q_r, H_s = Q_s\otimes I^{(p_{s+1}p_{s+2}\cdots p_r)},\ s=1,2,\cdots,r-1,$$

$$D_{ts} = I^{(m)}\otimes\cdots\otimes I^{(m)}\otimes H_s\otimes I^{(m)}\otimes\cdots\otimes I^{(m)},\ 1\le t\le n, 1\le s\le r, \tag{14}$$

where H_s is in the t-th position of the tensor product of the n matrices. Then H_s and D_{ts} are sparse matrices with p_s nonzero entries in each row, and there exist totally $m^n n\sum_{s=1}^r p_s$ nonzero entries in D_{ts} $(1\le t\le n, 1\le s\le r)$. From (13),(14),(4) and (3), one deduces

$$M_1 = M(p_1p_2\cdots p_r) = H_rH_{r-1}\cdots H_1,$$

$$\begin{aligned} M_n &= D_{nr}D_{n,r-1}\cdots D_{n1}D_{n-1,r}\cdots D_{n-1,1}\cdots D_{1r}D_{1,r-1}\cdots D_{11}, \\ S &= D_{nr}(D_{n,r-1}(\cdots(D_{n1}(\cdots(D_{12}(D_{11}T))\cdots))\cdots)). \end{aligned} \tag{15}$$

We summarize the above as

Theorem 1 *Let $m = p_1p_2\cdots p_r$ be the prime factor decomposition of m. Then*

(i) The Chrestenson transform matrix for functions over $Z/(m)$ of n indeterminates is a product of nr sparse matrices;

(ii) The complexity to compute the Chrestenson spectra according to (15) is $O(m^n n\sum_{i=1}^{r} p_i)$

Remark 2 A fast algorithm of complexity $O(m\sum_{i=1}^r p_i)$ is given in [2] to calculate $\{\sum_{j=0}^{m-1} v_j\xi_m^{wj} \mid 0\le w\le m-1\}$, the DFT of complex vector $v=(v_0,\cdots,v_{m-1})$ of length m. This is an analogy of Chrestenson spectra of functions of one indeterminate. Our algorithm can be regarded as a generalization of this algorithm.

In some applications, for example in cryptology[4], functions over $Z/(p^r)$, especially over $Z/(2^r)$, play an important role. For this kind of rings, below we show that M_1 and M_n can be decomposed into products of sparse matrices in a simple and direct way, such that all the sparse matrices of M_1 have nonzero entries in the same positions.

Let $m=p^r$, $r>1$, $\Gamma=\{0,1,\cdots,p^r-1\}$. For $s=1,2,\cdots,r$, define maps $\phi_s:\Gamma\times\Gamma\to Z$ and $\delta:\Gamma\times\Gamma\to\{0,1\}$ as

$$\phi_s(i,j) = j_{r-1}(i_0p^{r-1}+i_1p^{r-2}+\cdots+i_{s-1}p^{r-s}),$$

$$\delta(i,j)=1 \quad \text{if } (j_0,j_1,j_2,\cdots,j_{r-2})=(i_1,i_2,i_3,\cdots,i_{r-1}),\quad \text{and 0 otherwise,}$$

where $i,j\in\Gamma$, $\mathrm{rep}_1(i)=(i_{r-1},\cdots,i_1,i_0)$, and $\mathrm{rep}_1(j)=(j_{r-1},\cdots,j_1,j_0)$. Define the matrix

$$H'_s = (\delta(i,j)\varsigma_m^{\phi_s(i,j)})_{0\le i,j<m} \quad \text{for } s=1,2,\cdots,r, \tag{16}$$

where the row label i and the column label j are arranged in the usual ascending order of integers. Similarly as in (14) we define

$$D'_{ts} = I^{(m)}\otimes\cdots\otimes I^{(m)}\otimes H'_s\otimes I^{(m)}\otimes\cdots\otimes I^{(m)}, 1\le t\le n, 1\le s\le r. \tag{17}$$

Theorem 2 *Let $m = p^r, r > 1$, and M_n be as in (7). Then*

$$M_1 = H'_r H'_{r-1} \cdots H'_1, \tag{18}$$

and the complexity to compute the Chrestenson spectra according to

$$S = D'_{nr}(D'_{n,r-1}(\cdots(D'_{n1}(\cdots(D'_{12}(D'_{11}T))\cdots))\cdots)) \tag{19}$$

is $O(m^n nrp)$.

Proof Suppose $i, j \in \Gamma$, $\mathrm{rep}_1(i) = (i_{r-1}, \cdots, i_1, i_0)$, $\mathrm{rep}_1(j) = (j_{r-1}, \cdots, j_1, j_0)$, and suppose $a_r, a_{r-1}, \cdots, a_2 \in \Gamma$, $a_{r+1} = i$, $a_1 = j$. If

$$\delta(a_{r+1}, a_r) = \delta(a_r, a_{r-1}) = \cdots = \delta(a_2, a_1) = 1,$$

then for $s = 2, 3, \cdots, r$, the first component of $\mathrm{rep}_1(a_s)$ is equal to the second component of $\mathrm{rep}_1(a_{s-1})$ and is equal to the third component of $\mathrm{rep}_1(a_{s-2})$, and so on. So, it is equal to the s-th component j_{r-s} of $\mathrm{rep}_1(a_1)$ =$\mathrm{rep}_1(j)$, and hence,

$$\begin{aligned}
\mathrm{rep}_1(a_r) &= (j_0, i_{r-1}, \cdots, i_2, i_1), \\
\mathrm{rep}_1(a_{r-1}) &= (j_1, j_0, i_{r-1}, \cdots, i_3, i_2), \\
&\cdots \\
\mathrm{rep}_1(a_2) &= (j_{r-2}, j_{r-3}, \cdots, j_0, i_{r-1}),
\end{aligned}$$

therefore, $a_r, a_{r-1}, \cdots, a_2$ are uniquely determined by i and j. From the definitions of H'_s, the (i,j)-entry of $H'_r H'_{r-1} \cdots H'_1$ is $\varsigma_m^{\varepsilon}$, where $\varepsilon = \sum_{s=1}^{r} \phi_s(a_{s+1}, a_s)$. Since

$$\begin{aligned}
\mathrm{rep}_1(a_{s+1}) &= (j_{r-s-1}, \cdots, j_1, j_0, i_{r-1}, i_{r-2}, \cdots, i_{r-s}), \\
\mathrm{rep}_1(a_s) &= (j_{r-s}, \cdots, j_1, j_0, i_{r-1}, i_{r-2}, \cdots, i_{r-s+1}), \\
\phi_s(a_{s+1}, a_s) &= j_{r-s}(i_{r-s}p^{r-1} + \cdots + i_{r-2}p^{r-s+1} + i_{r-1}p^{r-s}) \\
&\equiv j_{r-s}p^{r-s}(i_0 p^{r-1} + \cdots + i_{r-s-1}p^s + i_{r-s}p^{s-1} + \cdots + i_{r-2}p + i_{r-1}) (\bmod\ p^r),
\end{aligned}$$

set

$$\bar{i} = i_0 p^{r-1} + \cdots + i_{r-s-1}p^s + i_{r-s}p^{s-1} + \cdots + i_{r-2}p + i_{r-1},$$

i.e., $\bar{i}$=$\mathrm{rep}_1^{-1}(\mathrm{rep}_2(i))$, then

$$\varepsilon = \bar{i} \cdot \sum_{s=1}^{r} j_{r-s}p^{r-s} = \bar{i} \cdot j, \ \varsigma_m^{\varepsilon} = \varsigma_m^{\bar{i} \cdot j}.$$

But $\varsigma_m^{\bar{i} \cdot j}$ is the entry of M_1 with row label $\bar{i}$ and column label j, so this entry is exact the (i,j)-entry of M_1 in the ordinary row and column labels, and Formula (18) is proved. The last statement of the theorem is clear as in Theorem 1.

References:

[1] BUHLER J, SHOKROLLAHI M A, STEMANN V. *Fast and precise Fourier transforms* [J]. IEEE Trans. on Information Theory, 2000, **46**(1): 213–228.
[2] COOLEY J W, TUKEY J W. *An algorithm for the machine calculation of complex Fourier series* [J]. Mathematics of Computation, 1965, **19**(2): 297–301.
[3] GUAN Zhao-zhi, CHEN Wen-de. *Walsh functions and Walsh transforms* [M]. Beijing: National Defence Industry Press, 1984. (in Chinese)
[4] DING Cun-sheng, XIAO Guo-zhen. *Stream Cipher and Its Applications* [M]. Beijing: National Defence Industry Press, 1994. (in Chinese)
[5] ZHOU Jin-jun, GAO Feng-xiu. *A fast algorithm for computing Chrestenson spectra and the best linear approximation of functions over ring $Z/(m)$* [C]. Proceedings of Advance in Cryptology–CHINACRYPT'96, Beijing: Science Press, 1996, 185–201.
[6] CHRESTENSON H. *A class of generalized Walsh functions* [J]. Pacific J. Math., 1955, **5**(5): 17–23.

矩阵分解与 Chrestenson 谱的计算

胡 磊

(中国科学院研究生院信息安全国家重点实验室，北京 100039)

摘 要: 本文研究离散 Fourier 变换的一类变型 – 整数模合数 m 剩余类环上 n 元函数的 Chrestenson 谱的快速计算. 基于稀疏矩阵分解，给出了两种复杂度为 $O(m^n n \sum_{i=1}^{r} p_i)$ 的计算 Chrestenson 谱的快速算法，其中 $p_1 p_2 \cdots p_r$ 是 m 的素因子分解.