国 防 科 技 大 学 学 报
JOURNAL OF NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY
一九八七年第一期　总第五十七期　No. 1 1987 Sum. 57

一维变换与二维变换的等价以及二维DFT的向量算法

蒋 增 荣

提　要　本文证明了当且仅当 $[R]=[P]^T\otimes[Q]$ 时，一维变换 $Y=[R]X$ 与二维变换 $[Y]=[Q][X][P]$ 相互等价。此外，讨论了Hadamard 变换以及具有循环卷积特性的一维变换与二维变换的等价问题。最后，利用上述等价定理，导出了二维DFT的一种比行列算法更为有效的快速算法——向量算法。

B. Arazi 在[1]中讨论了当 $[P]$ 是对称矩阵的情况下，二维变换 $[Y]=[P][X][P]$ 与一维变换 $Y=X[R]$ 的等价问题。在本文中，我们讨论了一般 $N\times M$ 二维变换 $[Y]=[Q][X][P]$ 与一般一维变换 $Y=[R]X$ 之间的等价问题，得到的结果是，当且仅当 $[R]=[P]^T\otimes[Q]$ 时，它们等价，这里 $[P]^T$ 是 $[P]$ 的转置矩阵，$\otimes$ 表示矩阵的Kronecker乘积。这样就为一维变换的二维处理或二维变换的一维处理创造了条件。然后讨论了具有CCP 的一维变换（如DFT，NTT，PT）与二维变换的等价问题，还证明了 2^k 阶一维Hadamard 变换可与二维 Hadamard 变换等价。最后，利用上述等价定理，导出了二维DFT的一种比行列算法更为有效的快速算法——向量算法。

定义 1　设 X 是 NM 向量

$$X=(x_0, x_1, \cdots, x_{NM-1})^T$$

$[X]$ 是 $N\times M$ 矩阵

$$[X]=(x_{ij})_{N\times M}$$

当且仅当

$$x_{ij}=x_{i+jN} \qquad (i=0,1,\cdots,N-1;\ j=0,1,\cdots,M-1) \tag{1}$$

时，称 $[X]$ 是 X 的矩阵表示，X 是 $[X]$ 的向量表示。

定义 2　设 $N\times M$ 矩阵 $[X]$ 是 NM 向量 X 的矩阵表示，$[R]$，$[Q]$，$[P]$ 分别是 NM

本文1985年2月18日收到

$\times NM$，$N\times N$，$M\times M$方阵，作变换

$$Y=[R]X \tag{2}$$

$$[Y]=[Q][X][P] \tag{3}$$

如果$[Y]$是Y的矩阵表示（或Y是$[Y]$的向量表示），则称一维变换(2)与二维变换(3)等价。

定理 设$[X]$，$[Y]$，X，Y，$[R]$，$[Q]$，$[P]$如定义2所示，则

(1) 对于任意向量X，$Y=[R]X$与$[Y]=[Q][X][P]$等价的充要条件是

$$[R]=[P]^T\otimes[Q] \tag{4}$$

这里$[P]^T$是$[P]$的转置矩阵，$\otimes$是矩阵的Kronecker 乘积；

(2) 如果对于向量X，$Y=[R]X$和$[Y]=[Q][X][P]$等价，则$[R]$是对称矩阵的充要条件是$[Q]$和$[P]$同时是对称矩阵或同时是反对称矩阵，且有

$$\begin{aligned}&R_{i+jN,\,k+lN}=\pm R_{i+lN,\,k+jN}\\&R_{i+jN,\,k+lN}=\pm R_{k+jN,\,i+lN}\\&\qquad(i,k=0,1,\cdots,N-1;\ j,l=0,1,\cdots,M-1)\end{aligned} \tag{5}$$

证明 设

$$X=(x_j)_{NM\times1}，\ Y=(y_j)_{NM\times1}$$

$$[X]=(x_{ij})_{N\times M}，\ [Y]=(y_{ij})_{N\times M}$$

$$[R]=(R_{ij})_{NM\times NM}，\ [Q]=[Q_{ij}]_{N\times N}，\ [P]=(P_{ij})_{M\times M}$$

(1) 首先证明必要性。由于

$$y_p=\sum_{q=0}^{NM-1}R_{pq}x_q \qquad (p=0,1,\cdots,NM-1) \tag{6}$$

$$y_{ij}=\sum_{k=0}^{N-1}\sum_{l=0}^{M-1}Q_{ik}x_{kl}P_{lj} \qquad (i=0,1,\cdots N-1;\ j=0,1,\cdots,M-1) \tag{7}$$

在(6)式中，作下标变换

$$p=i+jN \qquad (i=0,1,\cdots,N-1;\ j=0,1,\cdots,M-1)$$

$$q=k+lN \qquad (k=0,1,\cdots,N-1;\ l=0,1,\cdots,M-1)$$

于是(6)式就成为

$$y_{i+jN}=\sum_{k=0}^{N-1}\sum_{l=0}^{M-1}R_{i+jN,\,k+lN}x_{k+lN} \tag{8}$$

由假设，$[X]$，$]Y]$分别是向量X，Y的矩阵表示，于是有

$$y_{ij}=\sum_{k=0}^{N-1}\sum_{l=0}^{M-1}R_{i+jN,\,k+lN}x_{kl} \tag{9}$$

由于(6)与(7)式互相等价，故有

$$\sum_{k=0}^{N-1}\sum_{l=0}^{M-1}(R_{i+jN,\,k+lN}-Q_{ik}P_{lj})x_{kl}=0$$

由向量的任意性，有

$$R_{i+jN,k+lN}=Q_{ik}P_{lj} \quad (i,k=0,1,\cdots,N-1;\ j,l=0,1,\cdots,M-1) \tag{10}$$

记$P'_{jl}=P_{lj}$，就有

$$R_{i+jN,k+lN}=P'_{jl}\cdot Q_{ik}$$

于是，由矩阵的Kronecker乘积的定义，有

$$[R]=[P]^T\otimes[Q]$$

再证明充分性。设$[R]=[P]^T\otimes[Q]$，于是

$$R_{i+jN,\ k+lN}=P'_{jl}\cdot Q_{ik}=P_{lj}\cdot Q_{ik}$$

$$(i,k=0,1,\cdots,N-1;\ \ j,l=0,1,\cdots,M-1)$$

由上述下标变换，一维变换$Y=[R]X$成为

$$y_{i+jN}=\sum_{k=0}^{N-1}\sum_{l=0}^{M-1}R_{i+jN,\ k+lN}x_{kl}$$

从而

$$y_{i+jN}=\sum_{k=0}^{N-1}\sum_{l=0}^{M-1}P_{lj}Q_{ik}x_{kl}\qquad(i=0,1,\cdots,N-1;\ \ j=0,1,\cdots,M-1)$$

与(7)式比较，知有

$$y_{i+jN}=y_{ij}\qquad(i=0,1,\cdots,N-1;\ \ j=0,1,\cdots,M-1)$$

这表示$[Y]$是Y的矩阵表示，充分性证完。

(2) 若$Y=[R]X$与$[Y]=[Q][X][P]$等价，则由(10)式有

$$R_{i+jN,\ k+lN}=P_{lj}\cdot Q_{ik}\quad(i,k=0,1,\cdots,N-1;\ \ j,l=0,1,\cdots,M-1)$$

当$[Q]$和$[P]$同时是对称矩阵或同时是反对称矩阵时，有

$$R_{i+jN,\ k+lN}=P_{lj}\cdot Q_{ik}=P_{jl}\cdot Q_{ki}=R_{k+lN,\ i+jN}$$

这表示$[R]$是对称的，且有

$$R_{i+jN,\ k+lN}=P_{lj}\cdot Q_{ik}=\pm P_{jl}\cdot Q_{ik}=\pm R_{i+lN,\ k+jN}$$

$$R_{i+jN,\ k+lN}=P_{lj}\cdot Q_{ik}=P_{lj}\cdot\pm Q_{ki}=\pm R_{k+jN,\ i+lN}$$

反之，当$[R]$是对称矩阵时，$R_{i+jN,\ k+lN}=R_{k+lN,\ i+jN}$，于是有

$$P_{lj}\cdot Q_{ik}=P_{jl}\cdot Q_{ki}\quad(i,k=0,1,\cdots,N-1;\ \ j,l=0,1,\cdots,M-1)$$

如果$[P]$或$[Q]$的主对角线上的某个元素不等于零，比如$Q_{00}\neq0$（或$P_{00}\neq0$），则令$i=k=0$，就有

$$P_{lj}=P_{jl}\qquad(j,l=0,1,\cdots,M-1)$$

这表示$[P]$是对称的，从而$[Q]$也是对称的。

当$[P]$和$[Q]$的主对角线上的所有元素均为零，这时有

$$P_{lj}=\pm P_{jl}\qquad(j,l=0,1,\cdots,M-1)$$

$$Q_{ik}=\pm Q_{ki}\qquad(i,k=0,1,\cdots,N-1)$$

这表示$[P]$和$[Q]$同时是对称矩阵或反对称矩阵。(5)式的关系这时显然成立。 证毕

推论 1 一维Hadamard 变换

$$Y=[H_{NM}]X\tag{11}$$

与二维Hadamard 变换

$$[Y]=[H_N][X][H_M]\tag{12}$$

互相等价，其中N，M均为2的幂。

2^k 阶Hadamard矩阵是

$$[H_{2^k}]=(H_{ij})_{2^k\times 2^k}$$

$$H_{ij}=(-1)^{\sum\limits_{l=0}^{k-1} i_l j_l} \qquad (i,j=0,1,\cdots,2^k-1)$$

$$i=\sum_{l=0}^{k-1} i_l\cdot 2^l \qquad i_l\in(0,1)$$

$$j=\sum_{l=0}^{k-1} j_l\cdot 2^l \qquad j_l\in(0,1)$$

由此知$[H_{2^k}]$是对称矩阵，且

$$[H_{2^k}]=[H_2]\otimes[H_2]\otimes\cdots\otimes[H_2] \quad (k\text{个相乘})$$

$$[H_2]=\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

因此，当$n+m=k$时，有

$$[H_{2^k}]=[H_{2^m}]\otimes[H_{2^n}]$$

由定理知，(11)式和(12)式互相等价。

由于长为$N=2^k$的一维Hadamard 变换有快速算法，所需加法次数为

$$A_d=N\log_2 N$$

从而计算$N\times M$二维 Hadamard 变换，只需

$$A_d=NM\log_2 NM$$

次加法。

推论 2 一维DFT不能与任何二维变换等价。

事实上，N点Fourier矩阵是

$$[R]=[W]=(W^{ij})_{N\times M}=\begin{bmatrix}1 & 1 & \cdots 1\\ 1 & W & \cdots W^{N-1}\\ \vdots & & \\ 1 & W^{N-1} & \cdots W^{(N-1)^2}\end{bmatrix} \tag{13}$$

其中 $W=e^{-i2\pi/N}$. $[R]$ 是对称矩阵。$R_{ij}=W^{ij}$不满足 (5) 式表示的关系。例如，当$[R]$是 6×6 对称矩阵时，按(5)式，应有 $R_{03}=R_{12}$, $R_{05}=R_{14}$, $R_{25}=R_{34}$ 等关系，但6×6 Fourier矩阵不满足这些关系。

同样，一维数论变换(NTT)与一维多项式变换(PT) 均不能与任何二维变换等价，因为这些变换均具有CCP，变换矩阵均具有(13)这种形式[2]。

推论 3 二维DFT可与一维变换等价，但这一维变换不具有CCP.

二维DFT定义作

$$[Y]=[W_N][X][W_M] \tag{14}$$

其中$[W_N]$与$[W_M]$都具有(13)式表示的形式，但以$W_N=e^{i\text{-}2\pi/N}$，$W_M=e^{i\text{-}2\pi/M}$代换其中的W. 由定理知，只需取

$$[R]=[W_M]\otimes[W_N]$$

则二维DFT(14)与一维变换

$$Y=[R]X \tag{15}$$

等价，其中$[R]$的元素R_{ij}还具有(5)式表示之关系。又如果一维变换(15)具有 CCP，则$[R]$必具有形式：

$$R_{ij}=a^{ij}$$

其中 $a^{NM}=1$ [2]，但这是不可能的。

由推论 3 知，二维 DFT$[Y]=[W_N][X][W_M]$ 可用一维变换 $Y=[R]X$ 来计算，其中

$$[R]=[W_M]\otimes[W_N] \tag{16}$$

下面我们寻求(15)式的快速算法，从而得到(14)式的快速算法。将(15)式写作

$$Y=[R]X=[W_M]\otimes[W_N]X=[W_M]\begin{bmatrix}[W_N]X_0\\ [W_N]X_1\\ \vdots \quad \vdots\\ [W_N]X_{M-1}\end{bmatrix} \tag{17}$$

也就是

$$Y_k=\sum_{m=0}^{M-1}W_M^{mk}[W_N]X_m \qquad (k=0,1,\cdots,M-1) \tag{18}$$

其中X_m和Y_k分别是输入与输出二维数组$[X]$和$[Y]$的M个列向量。

(18)式有很丰富的含义，首先它是一个向量等式，如果将它写作

$$Y_k=\sum_{m=0}^{M-1}W_M^{mk}([W_N]X_m) \qquad (k=0,1,\cdots,M-1) \tag{19}$$

那么它就是以N维向量$[W_N]X_m$为元素的M点一维DFT，先计算

$$X'_m=[W_N]X_m \qquad (m=0,1,\cdots,M-1) \tag{20}$$

这是一个N点一维DFT，共M个，再计算

$$Y_k=\sum_{m=0}^{M-1}W_M^{mk}X'_m \qquad (k=0,1,\cdots,M-1) \tag{21}$$

这是一个M点一维DFT，输入、输出向量是N维的，所以相当于N个一维DFT．这样计算，就是通常二维DFT的行列算法，所需运算量（复乘与复加）是：

$$\begin{cases}M_u=MM_u(N)+NM_u(M)\\ A_d=MA_d(N)+NA_d(M)\end{cases} \tag{22}$$

其中$M_u(k)$和$A_d(k)$表示 k 点一维DFT所需的复乘与复加数。

但是，如果将(18)式写作

$$Y_k=\sum_{m=0}^{M-1}(W_M^{mk}[W_N])X_m \qquad (k=0,1,\cdots,M-1) \tag{23}$$

就得到二维DFT的一种异于行列算法的另一种算法——向量算法，这种向量算法与一维DFT的Winograd 算法很相似，也可称作二维DFT的Winograd 算法。它是在通常的M点一维DFT(标量式)中，用向量X_m和Y_k 来代替标量，用与 $W_M^{mk}[W_N]$的乘法代替与W_M^{mk}的乘法，每一个与$W_M^{mk}[W_N]$的乘法是一个N点一维DFT，不过是用与$W_M^{mk}W_N^{ij}$的乘法代替与W_N^{ij}的乘法。因此，如果导出了N点及M点一维DFT的快速算法，那个就可按(23)式来计算$N\times M$二维DFT．当$N=2,3,4,5,7,8,9,16$ 时，可用 [3]、[5]附录中小NDFT算

法，当$N=p, p^a$(p是素数)时，可用Rader 算法[4]，当$N=2^t$时，可用基-2的各种快速算法[5]。具体算法流程见例 1．

也可以把(14)式等价为

$$Y_k=\sum_{n=0}^{N-1} X_n(W_N^{nk}[W_M]) \qquad (k=0,1,\cdots,N-1) \tag{24}$$

其中X_n和Y_k分别是$[X]$和$[Y]$的N个行向量。计算方法同(23)式。

下面来导出向量算法所需的运算量。设M点及N点一维 DFT 的 某 个快速算法需要$M_u(M)$，$M_u(N)$次复乘和$A_d(M)$，$A_d(N)$次复加，由(23)式知，需 计算 $M_u(M)$个N点一维DFT，这需要运算量是

$$M_u=M_u(M)\cdot M_u(N)$$

$$A_1=M_u(M)\cdot A_d(N)$$

此外，还需要$A_d(M)$对N维向量的加法，所需复加数是

$$A_2=A_d(M)\cdot N$$

因此，总运算量是

$$\begin{cases} M_u=M_u(M)\cdot M_u(N) \\ A_d=A_1+A_2=A_d(M)\cdot N+M_u(M)\cdot A_d(N) \end{cases} \tag{25}$$

如果按(24)式计算，总运算量是

$$\begin{cases} M_u'=M_u(N)\cdot M_u(M) \\ A_d'=A_d(N)\cdot M+M_u(N)A_d(M) \end{cases} \tag{26}$$

因此，按行向量计算与按列向量计算，两者乘法量相同，但加法量不同。如果

$$\frac{M_u(M)-M}{A_d(M)}<\frac{M_u(N)-N}{A_d(N)} \tag{27}$$

按列向量计算，加法量少些，反之按行向量计算，加法量少些。因此，可按

$$T(k)=\frac{M_u(k)-k}{A_d(k)} \tag{28}$$

之值作为标志，若$T(M)<T(N)$，则按列向量计算，反之，则按行向量计算。

例 1 试画出4×3二维DFT向量算法流程图。

$$[Y]=[W_4][X][W_3]$$

其中$W_4=-i$，$W_3=e^{-i2\pi/3}=-\dfrac{1+i\sqrt{3}}{2}$．由(23)式有

$$Y_k=\sum_{m=0}^{2}(W_3^{mk}[W_4])X_m \qquad (k=0,1,2)$$

其中

$$X_m=\begin{bmatrix} x_{0m} \\ x_{1m} \\ x_{2m} \\ x_{3m} \end{bmatrix} \quad (m=0,1,2), \qquad Y_k=\begin{bmatrix} y_{0k} \\ y_{1k} \\ y_{2k} \\ y_{3k} \end{bmatrix} \quad (k=0,1,2)$$

利用三点DFT的Rader算法[3][5]，有

$$\begin{cases} t_1 = X_1 + X_2 \\ t_2 = X_0 + t_1 \\ t_3 = X_2 - X_1 \end{cases} \qquad \begin{aligned} m_0 &= [W_4]t_2 \\ m_1 &= -\frac{3}{2}[W_4]t_1 \\ m_2 &= i\frac{3}{2}[W_4]t_3 \end{aligned}$$

$$\begin{cases} Z = m_0 + m_1 \\ Y_0 = m_0 \\ Y_1 = Z + m_2 \\ Y_2 = Z - m_2 \end{cases} \tag{I}$$

其中每一个等式都是向量式，每一个乘法 m_i 都是一个四点 DFT，每一个四点DFT均可如下计算：设

$$X = [W_4]x$$

利用四点DFT的Rader算法[3][5]，有

$$\begin{cases} s_1 = x_0 + x_2, & s_2 = x_3 + x_1 \\ s_3 = x_0 - x_2, & s_4 = x_3 - x_1 \\ s_5 = s_1 + s_2, & s_6 = s_1 - s_2 \end{cases} \qquad \begin{cases} n_0 = 1\cdot s_5, & n_1 = 1\cdot s_6 \\ n_2 = 1\cdot s_3, & n_3 = i\cdot s_4 \end{cases}$$

$$\begin{cases} X_0 = n_0 & X_1 = n_2 + n_3 \\ X_2 = n_1 & X_3 = n_2 - n_3 \end{cases} \tag{II}$$

这里每个式子都是标量式，$X = (x_0, x_1, x_2, x_3)^T$，$Y = (y_0, y_1, y_2, y_3)^T$。

将(I)和(II)结合起来，就得到1×3二维DFT向量算法的流程图，如图1所示。

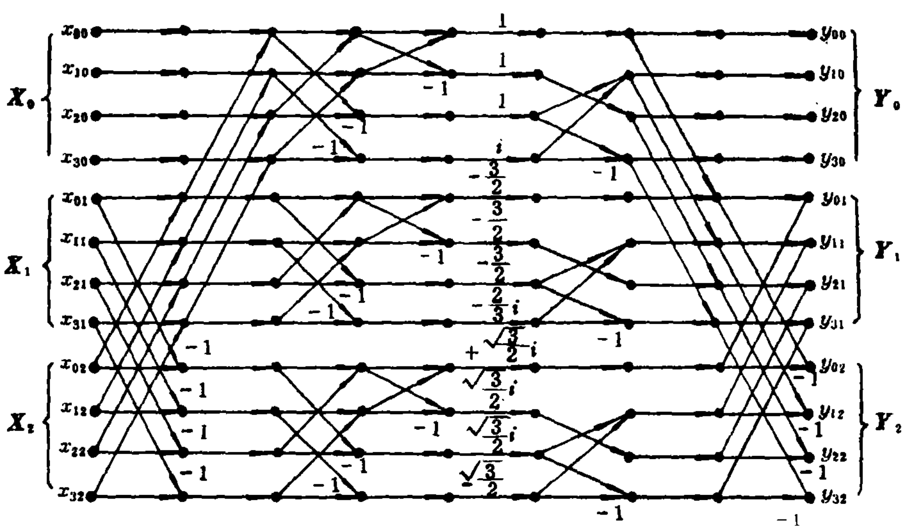

图 1　4×3二维DFT向量算法流程图

参 考 文 献

[1] B.Arazi, Two-Dimensional Digital Procesing of One-Dimensional Signal, IEEE Trans. ASSP-22, No.2, April 1974,

[2] 蒋增荣，数论变换，上海科技出版社，1980.
[3] S.Winograd, On Computing the Descrete Fourier Transform, Math. Comput. 32, 175—199(1978).
[4] C.M.Rader, Discrete Fourier Transforms When the Number of Data Samples is Prime, Proc. IEEE 56, 1107—1108(1968).
[5] H.J.Nussbaumer, Fast Fourier Transforms and Convolution Algorithms, Springer-Verlag Berlin Heidelberg New York 1981.
[6] C.M.Rader, N.M.Brenner, A New Principle for Fast Fourier Transformation, IEEE Trans. ASSP-24, 246—256(1969).

Equivalence of One-Dimensional General Transforms and Two-Dimensional General Transforms and the Vector Algorithm of Two-Dimensional DFTs

Jiang Zengrong

Abstract

In this paper, we discuss necessary and sufficient condition under which the one-dimensional general transforms equivalent to two-dimensional general transforms.

Theorem: Let $[X],[Y]$ be the matrix representations of vectors X, Y respectively, and let $[R],[Q],[P]$ be three matrices of order $NM\times NM$, $N\times N$, $M\times M$ respectively, $[X],[Y]$ are of order $N\times M$, X, Y are dimension NM.

(1) If and only if $[R]=[P]^T\otimes[Q]$, $Y=[R]X$ and $[Y]=[Q][X][Q]$ for any vector X, where $\otimes$ denotes Kronecker Product of matrices;

(2) If $Y=[R]X$ and $[Y]=[Q][X][P]$ for any vector X, then $[R]$ is symmetric, if and only if $[Q]$, $[P]$ are symmetric or anti-symmetric matrices, simultaneously, and

$$R_{i+jN,\,k+lN}=\pm R_{i+lN,\,k+jN}$$
$$R_{i+jN,\,k+lN}=\pm R_{k+jN,\,i+lN}$$
$$(i,k=0,1,\cdots,N-1;\ j,l=0,1,\cdots,M-1)$$

Nextly, we have discussed the equivalence of Walsh-Hadamard transforms and that of any general transforms having the cyclic convolution property (CCP) (DFT, NTT, PT). Lastly, we have introduced a fast algorithm of 2D-DFT—Vector Algorithm by using above equivalence theorem, which is more efficient than the row-column method of 2D-DFTs.