二维及多维多项式变换

罗建书　戴细英

提　要　本文提出了用二维多项式变换计算数字循环卷积的方法，指出了用二维多项式变换计算三维循环卷积所需的运算量。详细地讨论了实现二维多项式变换的条件，并推广到多维的情形。

一、引　言

计算自相关函数及互相关函数，设计及实现有限脉冲响应，计算大整数及多项式乘积，解微分方程及计算功率谱等均用到数字卷积的计算。尤其是一維卷积多維处理非常有效，故很有必要研究多維卷积的有效算法。

直接计算 $q\times q\times q$ 型的三維卷积，需 q^6 个乘法及 $q^3(q^3-1)$ 个加法。虽用快速付立叶变换（FFT）或数论变换（NTT）法[1]，可使运算量大为減少。但 FFT 需预先处理三角函数，有舍入误差，且仍对应较多的乘法。NTT 本身不需乘法，也无舍入误差，但变换长度受字长 b 的限制，且模运算也影响了运算效率。

为避免上述问题，H.J.Nussbaumer 和 P.Quandalle 近来提出了数字卷积的新算法[3]。这种变换法本身不需乘法，也无需移位，只需作多项式系数间的转移，所用运算为普通运算，不受 NTT 的其它限制。

蒋增荣老师研究了“一維多项式变换及其在卷积计算中的应用”[2]，承蒙蒋老师指导，本文在 [2] 的基础上讨论了“二維及多維多项式变换”，研究了实现这种变换的条件。

二、二维多项式变换的引进

三維数阵 $h=[h_{i,j,k}]_{N_1\times N_2\times N_3}$ 和 $x=[x_{i,j,k}]_{N_1\times N_2\times N_3}$ 的循环卷积 $y=h*x$ 定义为

$$y_{l,m,n}=\sum_{i=0}^{N_1-1}\sum_{j=0}^{N_2-1}\sum_{k=0}^{N_3-1}h_{\langle l-i\rangle_{N_1},\langle m-j\rangle_{N_2},\langle n-k\rangle_{N_3}}x_{i,j,k}$$
$$(0\leqslant l\leqslant N_1-1,0\leqslant j\leqslant N_2-1,0\leqslant k\leqslant N_3-1)\qquad(1)$$

定义 1　数阵 h，x，y 的母多项式矩阵是

本文1982年7月23日收到

$$H_{j,k}(z)=\sum_{i=0}^{N_1-1} h_{i,j,k}z^i \tag{2}$$

$$X_{j,k}(z)=\sum_{i=0}^{N_1-1} x_{i,j,k}z^i \quad (0\leqslant j\leqslant N_2-1, 0\leqslant k\leqslant N_3-1) \tag{3}$$

$$Y_{j,k}(z)=\sum_{i=0}^{N_1-1} y_{i,j,k}z^i \tag{4}$$

定义 2 设多项式矩阵如 (2)～(4) 定义，则称

$$S_{s,t}(z)\equiv\sum_{m=0}^{N_2-1}\sum_{n=0}^{N_3-1} H_{<s-m>_{N_2},<t-n>_{N_3}}(z)X_{m,n}(z)\bmod(z^{N_1}-1) \tag{5}$$

为 $[H_{j,k}(z)]_{N_2\times N_3}$ 与 $[X_{j,k}(z)]_{N_2\times N_3}$ 的二維多项式循环卷积。

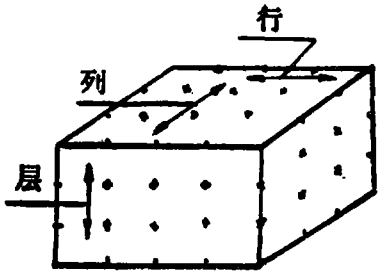
定理 1 设 $Y_{m,n}(z), H_{j,k}(z), X_{j,k}(z)$ 如 (2)～(4)，则

$$Y_{m,n}(z)\equiv\sum_{j=0}^{N_2-1}\sum_{k=0}^{N_3-1} H_{<m-j>_{N_2},<n-k>_{N_3}}(z)X_{j,k}(z)\bmod(z^{N_1}-1) \tag{6}$$

证明 $Y_{m,n}(z)=\sum_{l=0}^{N_1-1} y_{l,m,n}z^l$

$$=\sum_{k=0}^{N_3-1}\left\{\sum_{l=0}^{N_1-1}\left[\sum_{i=0}^{N_1-1}\sum_{j=0}^{N_2-1} h_{<l-i>_{N_1},<m-j>_{N_2},<n-k>_{N_3}}x_{i,j,k}\right]z^l\right\}$$

上式右端方括号内是矩阵 h 的第 $<n-k>_{N_3}$ 层与 x 的第 k 层的二維循环卷积的第 (l,m) 个元素，从而花括号内的多项式是这二維循环卷积的母多项式。由一維多项式变换理论[2]知



$$T_{m,k}(z)\equiv\sum_{j=0}^{N_2-1} H_{<m-j>_{N_2},<n-k>_{N_3}}(z)X_{j,k}(z)\bmod(z^{N_1}-1)$$

因此 $$Y_{m,n}(z)\equiv\sum_{j=0}^{N_2-1}\sum_{k=0}^{N_3-1} H_{<m-j>_{N_2},<n-k>_{N_3}}(z)X_{j,k}(z)\bmod(z^{N_1}-1)$$

$$(0\leqslant m\leqslant N_2-1, 0\leqslant n\leqslant N_3-1)$$

定理 1 证完。

由定理 1 知，可把三維循环卷积 (1) 化为母多项式矩阵的二維循环卷积的计算。

下面讨论用孙子定理计算 (6)：

设 $N_1=N_2=N_3=q$，q 为奇素数。

$$z^q-1=(z-1)(z^{q-1}+z^{q-2}+\cdots+z+1)=(z-1)M(z)$$

因 $M(z)$ 不可约，故 $(z-1, M(z))=1$. 记

$$Y_{1,m,n}(z)\equiv Y_{m,n}(z)\bmod M(z),\quad Y_{2,m,n}(z)\equiv Y_{m,n}(z)\bmod(z-1)$$

则由孙子定理有

$$Y_{m,n}(z)\equiv Y_{1,m,n}(z)S_1(z)(z-1)+Y_{2,m,n}(z)S_2(z)M(z)\bmod(z^q-1)$$

其中 $S_1(z)(z-1)\equiv 1\bmod M(z)$，$S_2(z)M(z)\equiv 1\bmod(z-1)$，可取

$$S_1(z)(z-1)=\frac{1}{q}(q-M(z)),\quad S_2(z)=\frac{1}{q}$$

于是

$$Y_{m,n}(z)\equiv\frac{1}{q}(q-M(z))Y_{1,m,n}(z)+\frac{1}{q}M(z)Y_{2,m,n}(z)\bmod(z^q-1)\qquad(7)$$

由于

$$Y_{2,m,n}(z)=\sum_{j=0}^{q-1}\sum_{k=0}^{q-1}H_{2,<m-j>q,<n-k>q}X_{2,j,k}$$

其中 $H_{2,j,k}=\sum_{i=0}^{q-1}h_{i,j,k}$，$X_{2,j,k}=\sum_{i=0}^{q-1}x_{i,j,k}(j,k=0,1,\cdots,q-1)$. 因此 $Y_{2,m,n}$ 是一个二維循环卷积，可用一維多项式变换计算[2]. 而

$$Y_{1,m,n}(z)\equiv\sum_{j=0}^{q-1}\sum_{k=0}^{q-1}H_{1,<m-j>q,<n-k>q}(z)X_{1,j,k}(z)\bmod M(z)$$

其中 $H_{1,j,k}(z)\equiv H_{j,k}(z)\bmod M(z)$，$X_{1,j,k}(z)\equiv X_{j,k}(z)\bmod M(z)$，$(j,k=0,1,\cdots,q-1)$

为计算 $Y_{1,m,n}(z)$，我们引进二維多项式变换。

定义 3 设 $M(z)=z^{q-1}+z^{q-2}+\cdots+1$，$q$ 为奇素数，$[H_{j,k}(z)]_{q\times q}$ 为一多项式矩阵，则称

$$\overline{H}_{s,t}(z)\equiv\sum_{m=0}^{q-1}\sum_{n=0}^{q-1}H_{m,n}(z)z^{ms+nt}\bmod M(z)\qquad(8)$$

为以 $M(z)$ 为模的二維多项式变换（其中 $s,t=0,1,\cdots,q-1$）. 其逆变换定义作

$$H_{m,n}(z)\equiv\frac{1}{q^2}\sum_{s=0}^{q-1}\sum_{t=0}^{q-1}\overline{H}_{s,t}(z)z^{-ms-nt}\bmod M(z)(m,n=0,1,\cdots,q-1)\qquad(9)$$

因 $z^q\equiv 1\bmod M(z)$，故计算 (8)、(9) 不需乘法。在第三节中，我们将证明 (8) 和 (9) 为一对互逆变换且具有 CCP. 二維多项式变换具有 CCP 是指：

定义 4 设 $[H_{j,k}(z)]_{q\times q}$ 和 $[X_{j,k}(z)]_{q\times q}$ 为次数不超过 q 的 q 阶多项式矩阵，$M(z)=(z^q-1)/(z-1)$

$$Y_{m,n}(z)\equiv\sum_{j=0}^{q-1}\sum_{k=0}^{q-1}H_{<m-j>q,<n-k>q}(z)X_{j,k}(z)\bmod M(z)\quad(m,n=0,1,\cdots,q-1)$$

$\overline{H}_{s,t}(z)$，$\overline{X}_{s,t}(z)$ 和 $\overline{Y}_{s,t}(z)$ 如 (8)所定义，若有

$$\overline{Y}_{s,t}(z)\equiv\overline{H}_{s,t}(z)\overline{X}_{s,t}(z)\bmod M(z)\quad(s,t=0,1,\cdots,q-1)$$

则称二維多项式变换 (8) 和 (9) 具有 CCP.

利用 (8)、(9) 及其 CCP 可计算 $Y_{1,m,n}(z)$. 步骤是：

1. 计算 $H_{1,j,k}(z)$ 和 $X_{1,j,k}(z)$ 的多项式变换 $\overline{H}_{1,s,t}(z)$ 和 $\overline{X}_{1,s,t}(z)$，

$$\bar{H}_{1,s,t}(z)\equiv\sum_{j=0}^{q-1}\sum_{k=0}^{q-1}H_{1,j,k}(z)z^{sj+tk}\bmod M(z)$$

$$\bar{X}_{1,s,t}(z)\equiv\sum_{j=0}^{q-1}\sum_{k=0}^{q-1}X_{1,j,k}(z)z^{sj+tk}\bmod M(z)\quad(s,t=0,1,\cdots,q-1)$$

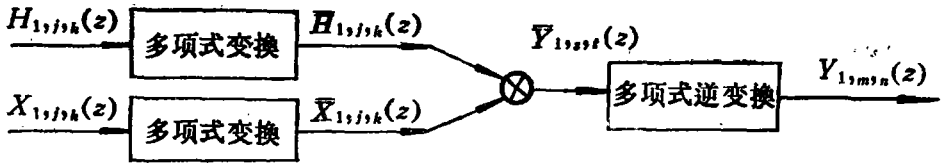
2. 作 $\bar{H}_{1,s,t}(z)$ 与 $\bar{X}_{1,s,t}(z)$ 的乘积（模 $M(z)$），

$$\bar{Y}_{1,s,t}(z)\equiv\bar{H}_{1,s,t}(z)\bar{X}_{1,s,t}(z)\bmod M(z)\quad(s,t=0,1,\cdots,q-1)\qquad(10)$$

3. 求 $\bar{Y}_{1,s,t}(z)$ 的逆变换，

$$Y_{1,m,n}(z)\equiv\frac{1}{q^2}\sum_{s=0}^{q-1}\sum_{t=0}^{q-1}\bar{Y}_{1,s,t}(z)z^{-(ms+nt)}\bmod M(z)\quad(m,n=0,1,\cdots,q-1)\qquad(11)$$

以上计算过程的示意图为



在实际应用中，因 $[h_{i,j,k}]_{q\times q\times q}$ 可预先给定，故计算 $Y_{1,m,n}(z)$ 只需一个正变换和一个逆变换及 q^2 个以 $M(z)$ 为模的多项式乘积。

由上可知，计算 $q\times q\times q$ 型的三維循环卷积，因多项式变换本身不需乘法，(7) 式的计算也不需乘法（将 $\frac{1}{q}$ 转移到 $\{h_{i,j,k}\}$ 中去即可），故只有 $q(q+1)$ 个以 $M(z)$ 为模的多项式乘积（其中计算 $Y_{1,m,n}(z)$ 需 q^2 个，$Y_{2,m,n}$ 需 q 个）需要乘法。由 Winograd 定理[4]知，计算一个多项式乘积（模 $M(z)$）至少需要 $2q-3$ 次乘法。因此，计算 $q\times q\times q$ 型的三維循环卷积共需 $q(2q^2-q-3)$ 个乘法，比直接用(1)计算所需 q^6 次乘法少得多。

下面我们讨论二維多项式变换的实现条件。

三、二维多项式变换

我们先来证明第二节中指出的，当 q 为奇素数时，(8)和(9)为一对互逆变换且具有 CCP.

定理 2 在定义 3 所述的条件下，(8) 和 (9) 为一对互逆变换且具有 CCP.

证明 因 $M(z)$ 不可约，故 $(z,M(z))=1$，从而 z^{-1} 存在。将 (9) 代入 (8) 中有

$$\bar{H}_{s,t}(z)\equiv\sum_{j=0}^{q-1}\sum_{k=0}^{q-1}\left\{\frac{1}{q^2}\sum_{m=0}^{q-1}\sum_{n=0}^{q-1}z^{m(s-j)+n(t-k)}\right\}\bar{H}_{j,k}(z)\bmod M(z)$$

欲证 (8) 和 (9) 为一对互逆变换，必须且只需证明

$$S\equiv\frac{1}{q^2}\sum_{m=0}^{q-1}\sum_{n=0}^{q-1}z^{mj+nk}\equiv\begin{cases}1, j\equiv 0 \bmod q \text{ 且 } k\equiv 0 \bmod q\\ 0, \text{否则}\end{cases}\bmod M(z)\qquad(12)$$

当 $j\equiv 0 \bmod q$ 且 $k\equiv 0 \bmod q$，(12) 显然成立。否则，不妨设 $j=aq+t$（a 为整数，$1\leqslant t\leqslant q-1$），由于

$$(z^t-1)\sum_{m=0}^{q-1}z^{mt}=z^{tq}-1\equiv 0 \bmod M(z)$$

而 $(z^t-1)\not\equiv 0 \bmod M(z)$，又$M(z)$不可约，故 $((z^t-1),M(z))=1$，从而必有

$$\sum_{m=0}^{q-1}z^{mt}\equiv 0 \bmod M(z),$$

于是

$$S=\frac{1}{q^2}\sum_{n=0}^{q-1}\sum_{m=0}^{q-1}z^{nk+mj}\equiv\frac{1}{q^2}\sum_{n=0}^{q-1}z^{nk}\cdot\left\{\sum_{m=0}^{q-1}z^{mt}\right\}\equiv 0 \bmod M(z)$$

同理可证 $k\not\equiv 0 \bmod q$ 的情况。可见 (8)、(9) 为一对互逆变换。下证 (8) 和 (9) 具有 CCP.

$$\begin{aligned}\bar{Y}_{s,t}(z)&\equiv\sum_{m=0}^{q-1}\sum_{n=0}^{q-1}Y_{m,n}(z)z^{ms+nt}\\&\equiv\sum_{j=0}^{q-1}\sum_{k=0}^{q-1}\left\{\sum_{m=0}^{q-1}\sum_{n=0}^{q-1}H_{<m-j>q,<n-k>q}(z)z^{ms+nt}\right\}X_{j,k}(z) \bmod M(z)\end{aligned}$$

记 $m-j=u, n-k=v$. 因 $H_{<u+q>q,<v+q>q}(z)\equiv H_{<u>q,<v>q}(z)\bmod M(z)$

则 $\sum_{m=0}^{q-1}\sum_{n=0}^{q-1}H_{<m-j>q,<n-k>q}(z)z^{ms+nt}\equiv\sum_{u=-j}^{q-j-1}\sum_{v=-k}^{q-k-1}H_{<u>q,<v>q}(z)z^{(u+j)s+(v+k)t} \bmod M(z)$

故 $\bar{Y}_{s,t}(z)\equiv\bar{H}_{s,t}(z)\bar{X}_{s,t}(z)\bmod M(z)$ $(s,t=0,1,\cdots,q-1)$. 证完。

下面将定义 3 推广到下列三种情况。

(一) q 是复合数。此时，z^q-1 在有理数域中可分解为若干个互异割圆多项式之积，$z^q-1=\prod_{i=1}^{p}M_{d_i}(z)$, $M_{d_i}(z)$ 的主系数为 1，$d_i(i=1,2,\cdots,p)$为 q 的因子（包括 1 和 q）. $M_{d_i}(z)$的次数为 d_i 的Euler 函数$\varphi(d_i)$[5], 记$Y_{i,m,n}(z)\equiv Y_{m,n}(z)\bmod M_{d_i}(z)$ $(i=1,2,\cdots,p;\ m,n=0,1,\cdots,q-1)$，由孙子定理而得

$$Y_{m,n}(z)\equiv\sum_{i=1}^{p}Y_{i,m,n}(z)M_i'(z)M_i(z)\bmod(z^q-1) \tag{13}$$

其中 $M_i(z)=(z^q-1)/M_{d_i}(z)$, $M_i'(z)M_i(z)\equiv 1\bmod M_{d_i}(z)$

$$Y_{i,m,n}(z)\equiv\sum_{u=0}^{q-1}\sum_{v=0}^{q-1}H_{i,<m-u>q,<n-v>q}(z)X_{i,u,v}(z)\bmod M_{d_i}(z)$$

$$H_{i,m,n}(z)\equiv H_{m,n}(z)\bmod M_{d_i}(z),\quad X_{i,m,n}(z)\equiv X_{m,n}(z)\bmod M_{d_i}(z)$$

$(i=1,2,\cdots,p;\ m,n=0,1,\cdots,q-1)$

用二維多项式变换计算 $Y_{i,m,n}(z)$, $i=1,2,\cdots,p$（因 $M_{d_i}(z)$ 不可约，故二維多项式变换存在。但在此处假定除 $z-1$ 和 $z+1$ 外，均能以 $M_{d_i}(z)$ 为模定义一个 $q\times q$ 型的二維多项式变换），全部算出 $Y_{i,m,n}(z)$后，由 (13) 式便得 $Y_{m,n}(z)$.

(二) $q=N_1p$，这里 p 为奇素数，$(N_1,p)=1$.

定理 3 设 $q=N_1p$，p 为奇素数，$(N_1,p)=1$, $[H_{j,k}(z)]_{p\times q}$ (或$[H_{j,k}(z)]_{q\times q}$)为多项式矩阵，则

$$\bar{H}_{s,t}(z)\equiv\sum_{j=0}^{p-1}\sum_{k=0}^{q-1}H_{j,k}(z)z^{sj}(\omega z)^{tk}\bmod M(z) \tag{14}$$

$$H_{j,k}(z)\equiv\frac{1}{pq}\sum_{s=0}^{p-1}\sum_{t=0}^{q-1}\bar{H}_{s,t}(z)z^{-js}(\omega z)^{-kt}\bmod M(z) \tag{15}$$

$(j,s=0,1,\cdots,p-1;\ k,t=0,1,\cdots,q-1)$

或
$$\overline{H}_{s,t}(z)\equiv\sum_{j=0}^{q-1}\sum_{k=0}^{q-1}H_{j,k}(z)(\omega z)^{sj+tk}\bmod M(z) \tag{16}$$

$$H_{j,k}(z)\equiv\frac{1}{q^2}\sum_{s=0}^{q-1}\sum_{t=0}^{q-1}\overline{H}_{s,t}(z)(\omega z)^{-(js+kt)}\bmod M(z) \tag{17}$$

$(j,k,s,t=0,1,\cdots,q-1)$

为一对具有 CCP 的互逆变换。其中 $\omega=e^{-j2\pi/N_1}$，$M(z)=(z^q-1)/(z-1)$.

证明 因 $M(z)$ 不可约，故 $(z,M(z))=1$，从而 z^{-1} 存在。将 (15) 代入(14)中，欲使

$$\overline{H}_{s,t}(z)\equiv\sum_{u=0}^{p-1}\sum_{v=0}^{q-1}\left\{\frac{1}{pq}\sum_{j=0}^{p-1}\sum_{k=0}^{q-1}z^{j(s-u)}(\omega z)^{k(t-v)}\right\}\overline{H}_{u,v}(z)\bmod M(z)$$

成立的充分必要条件是

$$S=\frac{1}{pq}\sum_{j=0}^{p-1}\sum_{k=0}^{q-1}z^{jm}(\omega z)^{kn}\equiv\begin{cases}1,\ m\equiv0\bmod p\ \text{且}\ n\equiv0\bmod q\\ 0,\ \text{否则}\end{cases}\bmod M(z) \tag{18}$$

第一式显然成立，对于第二式，若 $m\not\equiv0\bmod p$，则 $m=ap+t$ (a为整数，$1\leqslant t\leqslant p-1$)，由 $(z^t-1,M(z))=1$ 及

$$(z^t-1)\sum_{j=0}^{p-1}z^{jm}\equiv(z^t-1)\sum_{j=0}^{p-1}z^{jt}\equiv z^{tp}-1\equiv0\bmod M(z)$$

而知 $\sum_{j=0}^{p-1}z^{mj}\equiv0\bmod M(z)$，于是 $S=0\bmod M(z)$.

若 $n\not\equiv0\bmod q$，则 $n=aq+t$ (a 为整数，$t=1,2,\cdots,q-1$)，因 $(N_1,p)=1$，故对 $k=0,1,\cdots,q-1$ 可作素因子变换：

$$k\longleftrightarrow(k_1,k_2),\quad k_1\equiv k\bmod N_1\quad(k_1=0,1,\cdots,N_1-1)$$
$$k_2\equiv k\bmod p\quad(k_2=0,1,\cdots,p-1)$$

由孙子定理有 $k\equiv k_1a_1p+k_2a_2N_1\bmod q$，其中 $a_1p\equiv1\bmod N_1$，$a_2N_1\equiv1\bmod p$，于是

$$\sum_{k=0}^{q-1}(\omega z)^{kn}\equiv\sum_{k=0}^{q-1}(\omega z)^{kt}\equiv\sum_{k_1=0}^{N_1-1}\omega^{tk_1}\sum_{k_2=0}^{p-1}z^{tk_2}\bmod M(z)$$

由于 $t\equiv0\bmod N_1$ 和 $t\equiv0\bmod p$ 不可能同时成立 (否则，因 $(N_1,p)=1$ 而有 $t\equiv0\bmod N_1p$)，又 ω 是 N_1 阶单位根，故 $\sum_{k=0}^{q-1}(\omega z)^{kn}\equiv0\bmod M(z)$. 从而 $S=0\bmod M(z)$. 可见 (18)式成立。仿定理 2 可证 (14) 和 (15) 具有 CCP.

同理可证 (16) 和(17)为一对具有 CCP 的互逆变换，只是相应于(18)式的是下式：

$$S=\frac{1}{q^2}\sum_{j=0}^{q-1}\sum_{k=0}^{q-1}(\omega z)^{mj+nk}\equiv\begin{cases}1,\ m\equiv0\bmod q\ \text{且}\ n\equiv0\bmod q\\ 0,\ \text{否则}\end{cases}\bmod M(z) \tag{19}$$

定理 3 证完。

推论 设 $M(z)=(z^q-1)/(z-1)$，$[H_{j,k}(z)]$ 为 $p\times2p$ 型 (或$2p\times2p$ 型)多项式矩阵，p为奇素数，则

$$\overline{H}_{s,t}(z)\equiv\sum_{j=0}^{p-1}\sum_{k=0}^{2p-1}H_{j,k}(z)z^{sj}(-z)^{tk}\bmod M(z)$$

$$H_{j,k}(z)\equiv\frac{1}{2p^2}\sum_{s=0}^{p-1}\sum_{t=0}^{2p-1}\overline{H}_{s,t}(z)z^{-js}(-z)^{-kt}\bmod M(z)$$

$$(s,j=0,1,\cdots,p-1;\ t,k=0,1,\cdots,2p-1)$$

或
$$\overline{H}_{s,t}(z)\equiv\sum_{j=0}^{2p-1}\sum_{k=0}^{2p-1}H_{j,k}(z)z^{sj}(-z)^{tk}\bmod M(z)\quad(s,t=0,1,\cdots,2p-1)$$

$$H_{j,k}(z)\equiv\frac{1}{4p^2}\sum_{s=0}^{2p-1}\sum_{t=0}^{2p-1}\overline{H}_{s,t}(z)z^{-js}(-z)^{-kt}\bmod M(z)$$

$$(j,k=0,1,\cdots,2p-1)$$

为一对具有 CCP 的互逆变换。

（三） 模 $M(z)$ 为可约多项式的情况。

定义 5 设 $M(z)$ 为有理数域上一多项式，$[H_{j,k}(z)]_{M\times N}$ 是多项式矩阵，称

$$\overline{H}_{s,t}(z)\equiv\sum_{j=0}^{M-1}\sum_{k=0}^{N-1}H_{j,k}(z)(\alpha z^c)^{sj}(\beta z^d)^{tk}\bmod M(z)\tag{20}$$

$$(s=0,1,\cdots,M-1;\ t=0,1,\cdots,N-1)$$

为 $[H_{j,k}(z)]$ 的（模 $M(z)$）二維多项式变换。其逆为

$$H_{j,k}(z)\equiv\frac{1}{MN}\sum_{s=0}^{M-1}\sum_{t=0}^{N-1}\overline{H}_{s,t}(z)(\alpha z^c)^{-sj}(\beta z^d)^{-tk}\bmod M(z)\tag{21}$$

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

其中 α、β 为复常数，c、d 为自然数。

定理 4 当且仅当

$$(\alpha z^c)^M\equiv 1\bmod M(z),\ (\beta z^d)^N\equiv 1\bmod M(z)\tag{22}$$

$$S=\frac{1}{MN}\sum_{j=0}^{M-1}\sum_{k=0}^{N-1}(\alpha z^c)^{js}(\beta z^d)^{kt}\equiv\begin{cases}1,\ s\equiv 0\bmod M\ \text{且}\ t\equiv 0\bmod N\\ 0,\ \text{否则}\end{cases}\bmod M(z)\tag{23}$$

时，(20)、(21) 为一对互逆变换且具有 CCP.

证明 将 (21) 代入 (20) 中，欲使

$$\overline{H}_{s,t}(z)\equiv\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\left\{\frac{1}{MN}\sum_{j=0}^{M-1}\sum_{k=0}^{N-1}(\alpha z^c)^{j(s-m)}(\beta z^d)^{k(t-n)}\right\}\overline{H}_{m,n}(z)\bmod M(z)$$

成立的充分必要条件是

$$S=\frac{1}{MN}\sum_{j=0}^{M-1}\sum_{k=0}^{N-1}(\alpha z^c)^{js}(\beta z^d)^{kt}\equiv\begin{cases}1,\ s\equiv 0\bmod M\ \text{且}\ t\equiv 0\bmod N\\ 0,\ \text{否则}\end{cases}\bmod M(z)\tag{24}$$

又当 (20)、(21) 为一对互逆变换时，在 (24) 中取 $s=1,t=0$，并两边乘 αz^c-1 而得 $(\alpha z^c)^M\equiv 1\bmod M(z)$；取 $s=0$，$t=1$，并两边乘 βz^d-1 而得 $(\beta z^d)^N\equiv 1\bmod M(z)$.

若 (22) 成立，仿定理 2 可证 (20)、(21) 具有 CCP.

定理证完。

定理 5 设 $M(z)=p_1^{l_1}(z)\cdots p_s^{l_s}(z)$，其中 $p_i(z)(i=1,2,\cdots,s)$ 为互异的不可约多项式，当且仅当

1° $(\alpha z^c)^M \equiv 1 \bmod M(z)$，$(\beta z^d)^N \equiv 1 \bmod M(z)$；

2° $(\alpha z^c)^M \equiv 1 \bmod p_i(z)$，$(\beta z^d)^N \equiv 1 \bmod p_i(z)$ $(i=1,2,\cdots,s)$

且M、N分别是使上述式子成立的最小正整数时，(20) 和 (21) 为一对互逆变换且具有 CCP. 当 $M(z)$ 为不可约多项式时，1° 包含 2°.

证明 设 (20)、(21) 为一对互逆变换，则 (22) 成立，且有

$(\alpha z^c)^u \not\equiv 1 \bmod M(z)$，$(\beta z^d)^v \not\equiv 1 \bmod M(z)$ $(u=1,2,\cdots,M-1;\ v=1,2,\cdots,N-1)$. 若不然，设有某 $u(1 \leqslant u \leqslant M-1)$ 使 $(\alpha z^c)^u \equiv 1 \bmod M(z)$，则在 (23) 中取$t=0$而得 $1 \equiv 0 \bmod M(z)$，矛盾! 同样讨论(βz^d). 于是 1° 成立。

从 (22)、(23) 有 $(\alpha z^c)^M \equiv 1 \bmod p_i(z)$，$(\beta z^d)^N \equiv 1 \bmod p_i(z)$.

$$\frac{1}{MN}\sum_{j=0}^{M-1}\sum_{k=0}^{N-1}(\alpha z^c)^{ju}(\beta z^d)^{kv} \equiv \begin{cases} 1, & u \equiv 0 \bmod M \text{ 且 } v \equiv 0 \bmod N \\ 0, & \text{否则} \end{cases} \bmod p_i(z)$$

$(i=1,2,\cdots,s)$

同样可证得 $(\alpha z^c)^u \not\equiv 1 \bmod p_i(z)$，$(\beta z^d)^v \not\equiv 1 \bmod p_i(z)$ $(u=1,2,\cdots,M-1;\ v=1,2,\cdots,N-1)$. 此即证明了必要性。

又由 1° 知 (22) 成立，当 $u \equiv 0 \bmod M$ 且 $v \equiv 0 \bmod N$时，由 1° 则有

$$\frac{1}{MN}\sum_{j=0}^{M-1}\sum_{k=0}^{N-1}(\alpha z^c)^{ju}(\beta z^d)^{kv} \equiv 1 \bmod M(z)$$

其次，因 $p_i(z)(i=1,2,\cdots,s)$ 不可约，故$(p_i(z), (\alpha z^c)^u - 1)=1$. 因此 $(M(z), (\alpha z^c)^u - 1)=1$，由于$(\alpha z^c)^{uN} - 1 \equiv [(\alpha z^c)^u - 1]\sum_{j=0}^{M-1}(\alpha z^c)^{ju} \equiv 0 \bmod M(z)$，故

$$\sum_{j=0}^{M-1}(\alpha z^c)^{ju} \equiv 0 \bmod M(z) \quad (u=1,2,\cdots,M-1)$$

同理可得出 $\sum_{k=0}^{N-1}(\beta z^d)^{kv} \equiv 0 \bmod M(z)$ $(v=1,2,\cdots,N-1)$. 则 (23) 的第二式成立。据定理 4 充分性得证。

定理 6 设 $M(z)=p_1^{l_1}(z)\cdots p_s^{l_s}(z)$，$p_i(z)(i=1,2,\cdots,s)$ 为互异的不可约多项式，当且仅当$(\alpha z^c)^M \equiv 1 \bmod p_i^{l_i}(z)$，$(\beta z^d)^N \equiv 1 \bmod p_i^{l_i}(z)(i=1,2,\cdots,s)$，且$M$，$N$是分别使这些等式成立的正整数时，(20)、(21)为一对具有 CCP 的互逆变换。

证明 设 (20)、(21) 为具有 CCP 的互逆变换，则有 $(\alpha z^c)^M \equiv 1 \bmod M(z)$，从而 $(\alpha z^c)^M \equiv 1 \bmod p_i^{l_i}(z)$，且有 $(\alpha z^c)^u \not\equiv 1 \bmod p_i^{l_i}(z)(i=1,2,\cdots,s;\ 1 \leqslant u \leqslant M-1)$. 否则，由 $(\alpha z^c)^u \equiv 1 \bmod p_i^{l_i}(z)(1 \leqslant u \leqslant M-1)$ 则有 $(\alpha z^c)^u \equiv 1 \bmod p_i(z)$，与定理 6 矛盾!

同理可得 $(\beta z^d)^N \equiv 1 \bmod p_i^{l_i}(z)$ 且 $(\beta z^d)^v - 1 \bmod p_i^{l_i}(z)(i=1,2,\cdots,s;\ 1 \leqslant v \leqslant N-1)$

反之，因 $p_i^{l_i}(z)(i=1,2,\cdots,s)$两两互质，故$(\alpha z^c)^M\equiv 1 \bmod M(z)$，$(\beta z^d)^N\equiv 1 \bmod M(z)$且$(\alpha z^c)^u\not\equiv 1 \bmod M(z)$，$(\beta z^d)^v\not\equiv 1 \bmod M(z)(u=1,2,\cdots,M-1;\ v=1,2,\cdots,N-1)$，否则将与条件矛盾。

又有$(\alpha z^c)^M\equiv 1 \bmod p_i(z)$，$(\alpha z^c)^u\not\equiv 1 \bmod p_i(z)(i=1,2,\cdots,s;\ u=1,\cdots,M-1)$. 否则由$(\alpha z^c)^{u_0}\equiv 1 \bmod p_{i_0}(z)(1\leqslant i_0\leqslant s, 1\leqslant u_0\leqslant M-1)$而得$(\alpha z^c)^{Mu_0}-1=[(\alpha z)^{u_0}-1]\sum_{j=0}^{M-1}(\alpha z^c)^{ju_0}\equiv 0 \bmod p_i^{l_i}(z)$ (25)

从而$[(\alpha z^c)^{u_0}-1]\sum_{j=0}^{M-1}(\alpha z^c)^{ju_0}\equiv 0 \bmod p_{i_0}(z)$，此时必有$\sum_{j=0}^{M-1}(\alpha z^c)^{ju_0}\not\equiv 0 \bmod p_{i_0}(z)$，若不然，则有$M\equiv 0 \bmod M(z)$，这不可能！又因$p_{i0}(z)$不可约，则$(p_{i0}(z),\sum_{j=0}^{M-1}(\alpha z^c)^{ju_0})=1$，于是$(p_{i_0}^{l_{i_0}}(z),\sum_{j=0}^{M-1}(\alpha z^c)^{ju_0})=1$. 由(25)则得$(\alpha z^c)^{u_0}\equiv 1 \bmod p_{i_0}^{l_{i_0}}(z)$，矛盾！同理可证$(\beta z^d)^N\equiv 1 \bmod p_i(z)$，且$(\beta z^d)^v\not\equiv 1 \bmod p_i(z)(i=1,2,\cdots,s;\ 1\leqslant v\leqslant N-1)$. 充分性得证。定理证完。

定理5的条件2°与下述条件等价：

2°′存在多项式$\alpha_u(z)$，$\beta_v(z)(u=1,2,\cdots,M-1;\ v=1,2,\cdots,N-1)$使得$\alpha_u(z)[(\alpha z^c)^u-1]\equiv 1 \bmod M(z)$，$\beta_v(z)[(\beta z^d)^v-1]\equiv 1 \bmod M(z)$.

事实上，由定理5的2°，对于$M(z)$的任一不可约多项式因子$p(z)$，$(\alpha z^c)^u\not\equiv 1 \bmod p(z)$，$(\beta z^d)^v\not\equiv 1 \bmod p(z)$，从而$((\alpha z^c)^u-1, M(z))=1$，$((\beta z^d)^v-1, M(z))=1$，于是$[(\alpha z^c)^u-1]^{-1}$及$[(\beta z^d)^v-1]^{-1}$存在，记$\alpha_u(z)=[(\alpha z^c)^u-1]^{-1}$，$\beta_v(z)=[(\beta z^d)^v-1]^{-1}$，$(u=1,2,\cdots,M-1;\ v=1,2,\cdots,N-1)$. 2°′成立。

反之，因$\sum_{j=0}^{M-1}(\alpha z^c)^{ju}\equiv \alpha_u(z)[(\alpha z^c)^u-1]\sum_{j=0}^{M-1}(\alpha z^c)^{ju}$

$$\equiv \alpha_u(z)[(\alpha z^c)^{Mu}-1]\equiv 0 \bmod M(z)$$

同理有$\sum_{k=0}^{N-1}(\beta z^d)^{kv}\equiv 0 \bmod M(z)(u=1,2,\cdots,M-1;\ v=1,2,\cdots,N-1)$. 又由定理5的1°及定理4得知定理5的2°成立。

若从矩阵角度考虑，(20)、(21)的矩阵形式是

$$[\boldsymbol{H}_{s,t}(z)]_{M\times N}\equiv T_M(z)[H_{j,k}(z)]_{M\times N}T_N(z) \bmod M(z)$$

$$[H_{j,k}(z)]_{M\times N}\equiv V_M(z)[\boldsymbol{H}_{s,t}]_{M\times N}V_N(z) \bmod M(z)$$

其中

$$T_M(z)\equiv\begin{Bmatrix}1 & 1 & 1 & \cdots & 1\\ 1 & \alpha z^c & (\alpha z^c)^2 & \cdots & (\alpha z^c)^{M-1}\\ 1 & (\alpha z^c)^2 & (\alpha z^c)^4 & \cdots & (\alpha z^c)^{2(M-1)}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ 1 & (\alpha z^c)^{M-1} & (\alpha z^c)^{2(M-1)} & \cdots & (\alpha z^c)^{(M-1)^2}\end{Bmatrix} \bmod M(z)$$

$$T_N(z)\equiv\begin{Bmatrix}1 & 1 & 1 & \cdots & 1\\ 1 & \beta z^d & (\beta z^d)^2 & \cdots & (\beta z^d)^{N-1}\\ 1 & (\beta z^d)^2 & (\beta z^d)^4 & \cdots & (\beta z^d)^{2(N-1)}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ 1 & (\beta z^d)^{N-1} & (\beta z^d)^{2(N-1)} & \cdots & (\beta z^d)^{(N-1)^2}\end{Bmatrix}\bmod M(z)$$

$$V_M(z)\equiv\frac{1}{M}\begin{Bmatrix}1 & 1 & 1 & \cdots & 1\\ 1 & (\alpha z^c)^{-1} & (\alpha z^c)^{-2} & \cdots & (\alpha z^c)^{-(M-1)}\\ 1 & (\alpha z^c)^{-2} & (\alpha z^c)^{-4} & \cdots & (\alpha z^c)^{-2(M-1)}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ 1 & (\alpha z^c)^{-(M-1)} & (\alpha z^c)^{-2(M-1)} & \cdots & (\alpha z^c)^{-(M-1)^2}\end{Bmatrix}\bmod M(z)$$

$$V_N(z)\equiv\frac{1}{N}\begin{Bmatrix}1 & 1 & 1 & \cdots & 1\\ 1 & (\beta z^d)^{-1} & (\beta z^d)^{-2} & \cdots & (\beta z^d)^{-(N-1)}\\ 1 & (\beta z^d)^{-2} & (\beta z^d)^{-4} & \cdots & (\beta z^d)^{-2(N-1)}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ 1 & (\beta z^d)^{-(N-1)} & (\beta z^d)^{-2(N-1)} & \cdots & (\beta z^d)^{-(N-1)^2}\end{Bmatrix}\bmod M(z)$$

要证(20)、(21)为互逆变换，必须且只需证明 $T_MV_M\equiv I_{M\times M}\bmod M(z)$及 $T_NV_N\equiv I_{N\times N}\bmod M(z)$

定理 7 设 $M(z)=p_1^{l_1}(z)\cdots p_s^{l_s}(z)$，当且仅当

1° $(\alpha z^c)^M\equiv 1\bmod M(z)$，$(\beta z^d)^N\equiv 1\bmod M(z)$；

2° $(p_i(z),(\alpha z^c)^k-(\alpha z^c)^m)=1\quad(0\leqslant m<k\leqslant M-1,i=1,2,\cdots,s)$

$(p_i(z),(\beta z^d)^j-(\beta z^d)^l)=1\quad(0\leqslant l<j\leqslant N-1,i=1,2,\cdots,s)$

时，(20)、(21)为一对具有 CCP 的互逆变换。

证明 因 $|T_M(z)|=\prod\limits_{0\leqslant m<k\leqslant M-1}[(\alpha z^c)^k-(\alpha z^c)^m]\bmod M(z)$，由 2° 有 $(M(z),(\alpha z^c)^k-(\alpha z^c)^m)=1(0\leqslant m<k\leqslant M-1)$，故$[(\alpha z^c)^k-(\alpha z^c)^m]^{-1}$存在，于是$|T_M(z)|^{-1}$，从而 $T_M^{-1}(z)$ 存在。同理，$T_N^{-1}(z)$ 存在。

反之，设 (20)、(21) 为一对互逆变换，即$[T_M(z)]^{-1}$存在，从而$(M(z),(\alpha z^c)^k-(\alpha z^c)^m)=1$ $(0\leqslant m<k\leqslant M-1)$，于是 $(p_i(z),(\alpha z^c)^k-(\alpha z^c)^m)=1$ $(0\leqslant m<k\leqslant M-1;\ i=1,2,\cdots,s)$

同理可得 $(p_i(z),(\beta z^d)^j-(\beta z^d)^l)=1$ $(0\leqslant l<j\leqslant N-1,i=1,2,\cdots,s)$

以上证明了 $T_M^{-1}(z)$、$T_N^{-1}(z)$ 存在的充分必要条件是 1°、2° 成立。下证 $T_M(z)V_M(z)=I_{M\times M}\bmod M(z)$.

设 $T_M(z)V_M(z)=[c_{ij}(z)]_{M\times M}$，只需证

$$c_{ij}(z)\equiv\frac{1}{M}\sum_{k=0}^{M-1}(\alpha z^c)^{k(i-j)}\equiv\begin{cases}1 & i\equiv j\bmod M\\ 0 & i\not\equiv j\bmod M\end{cases}\bmod M(z)$$

由 1°，当 $i\equiv j\bmod M$时，有 $c_{ij}(z)\equiv 1\bmod M$. 当 $i\not\equiv j\bmod M$时，不难证得

$$x^{tM}-1\equiv\prod_{m=0}^{M-1}[x^t-(\alpha z^c)^{tm}]\bmod M(z)\qquad(t=1,2,\cdots,M-1)$$

比较系数而得 $\sum_{m=0}^{M-1}(\alpha z^{c})^{mt}\equiv 0 \bmod M(z)\quad (t=1,2,\cdots,M-1)$.

仿此可证 $T_N(z)V_N(z)\equiv I_{N\times N} \bmod M(z)$. 证完。

定理 8 若以 z^d 为根，多项式 $M(z)$ 为模可构成 $N\times N$ 的多项式方阵的二維多项式变换，则以 $M(z)$ 为模，(αz^d) 为根可构成 $N_1N\times N_1N$ 的多项式方阵的二維多项式变换，其中 $\alpha=e^{-i2\pi/N_1}$，$(N_1,N)=1$ 以 $M(z)$ 为模，z^d、αz^d 为根可构成 $N\times N_1N$ 型的多项式变换。

证明 由定理 3 而得。证完。

四、多维多项式变换

定义 6 设 K 一維多项式矩阵 $[H_{m,n,\cdots,l}(z)]_{M\times N\times\cdots\times L}$，$M(z)$ 为一多项式，则称

$$Y_{m,n,\cdots,l}(z)\equiv\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\cdots\sum_{l=0}^{L-1}H_{<m-i>M,<n-j>N,\cdots,<l-k>L}(z)X_{i,j,\cdots,k}(z)\cdot \bmod M(z)$$

为 $[H_{m,n,\cdots,l}(z)]$ 与 $[X_{m,n,\cdots,l}(z)]$ 的 K 一維循环卷积。称

$$\boldsymbol{H}_{r,s,\cdots,t}(z)\equiv\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\cdots\sum_{l=0}^{L-1}H_{m,n,\cdots,l}(z)(\alpha z^{a})^{mr}(\beta z^{b})^{ns}\cdots(\gamma z^{c})^{lt} \bmod M(z) \quad (26)$$

为 $[H_{m,n,\cdots,l}(z)]$ 的 K 一維多项式变换，其中 $\alpha,\beta,\cdots,\gamma$ 为复常数，$(\alpha z^{a})^{M}\equiv 1 \bmod M(z)$，$(\beta z^{b})^{N}\equiv 1 \bmod M(z),\cdots,(\gamma z^{c})^{L}\equiv 1 \bmod M(z)$. 其逆变换定义作

$$H_{m,n,\cdots,l}(z)\equiv\frac{1}{MN\cdots L}\sum_{r=0}^{M-1}\sum_{s=0}^{N-1}\cdots\sum_{t=0}^{L-1}\boldsymbol{H}_{r,s,\cdots,t}(z)(\alpha z^{a})^{-mr}(\beta z^{b})^{-ns}\cdots(\gamma z^{c})^{-lt} \bmod M(z) \quad (27)$$

$(r,m=0,1,\cdots,M-1;\ s,n=0,1,\cdots,N-1,\ \cdots\cdots,\ t,l=0,1,\cdots,L-1)$

类似于二維多项式变换，我们可得到 (26) 和 (27) 为具有 CCP 的互逆变换的充分必要条件如下：

定理 9 当且仅当

$$(\alpha z^{a})^{M}\equiv 1 \bmod M(z),\ (\beta z^{b})^{N}\equiv 1 \bmod M(z),\ \cdots,(\gamma z^{c})^{L}\equiv 1 \bmod M(z),$$

$$S=\frac{1}{MN\cdots L}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\cdots\sum_{l=0}^{L-1}(\alpha z^{a})^{mr}(\beta z^{b})^{ns}\cdots(\gamma z^{c})^{lt}$$

$$\equiv\begin{cases}1, & r\equiv 0 \bmod M,\ s\equiv 0 \bmod N,\ \cdots,\ t\equiv 0 \bmod L\\ 0, & \text{否则}\end{cases} \bmod M(z)$$

时，(26)、(27) 为一对互逆变换，且具有 CCP.

定理 10 设 $M(z)=p_1(z)^{l_1}\cdots p_s(z)^{l_s}$，$p_i(z)(i=1,2,\cdots,s)$ 是互异的不可约多项式，则当且仅当

1° $(\alpha z^{a})^{M}\equiv 1 \bmod M(z)$，$(\beta z^{b})^{N}\equiv 1 \bmod M(z),\cdots,(\gamma z^{c})^{L}\equiv 1 \bmod M(z)$，且 $M,N,\cdots,L$ 分别是使这些等式成立的最小正整数。

2° $(\alpha z^{a})^{M}\equiv 1 \bmod p_i(z)$，$(\beta z^{b})^{N}\equiv 1 \bmod p_i(z),\cdots,(\gamma z^{c})^{L}\equiv 1 \bmod p_i(z)$ $(i=1,2,\cdots,s)$，且 $M,N,\cdots,L$ 分别是使这些等式成立的最小正整数时，(26) 和 (27) 为一对具有 CCP 的互逆变换。

定理 11 设 $M(z)=p_1(z)^{l_1}\cdots p_s(z)^{l_s}$，$p_i(z)$ $(i=1,2,\cdots,s)$ 为互异的不可约多项式，则当且仅当

$(\alpha z^a)^M\equiv 1 \bmod p_i(z)^{l_i}$，$(\beta z^b)^N\equiv 1 \bmod p_i(z)^{l_i}$，$\cdots$，$(\gamma z^c)^L\equiv 1 \bmod p_i(z)^{l_i}$，$(i=1,2,\cdots,s)$ 时，(26)、(27) 为一对互逆变换且具有 CCP.

定理 12 设 $M(z)$ 为多项式，则当且仅当

1°$(\alpha z^a)^M\equiv 1 \bmod M(z)$，$(\beta z^b)^N\equiv 1 \bmod M(z)$，$\cdots$，$(\gamma z^c)^L\equiv 1 \bmod M(z)$，且 M，N，$\cdots$，L 分别是使这些等式成立的最小正整数；

2°存在多项式 $\alpha_r(z)(r=1,2,\cdots,M-1)$，$\beta_s(z)$ $(s=1,2,\cdots,N-1)$，$\cdots$，$\gamma_t(z)$ $(t=1,2,\cdots,L-1)$，使得

$\alpha_r(z)[(\alpha z^a)^r-1]\equiv 1 \bmod M(z)$，$\beta_s(z)[(\beta z^b)^s-1]\equiv 1 \bmod M(z)$，$\cdots$，

$\gamma_t(z)[(\gamma z^c)^t-1]\equiv 1 \bmod M(z)(r=1,2,\cdots,M-1;\ s=1,2,\cdots,N-1;\ \cdots;\ r=1,2,\cdots,L-1)$ 时，(26) 和 (27) 为一对具有 CCP 的互逆变换。

若从矩阵角度考虑，则 (26) 的变换矩阵为

$$T_M(z)\equiv\begin{Bmatrix}1 & 1 & 1 & \cdots & 1\\ 1 & \alpha z^a & (\alpha z^a)^2 & \cdots & (\alpha z^a)^{M-1}\\ 1 & (\alpha z^a)^2 & (\alpha z^a)^4 & \cdots & (\alpha z^a)^{2(M-1)}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ 1 & (\alpha z^a)^{M-1} & (\alpha z^a)^{2(M-1)} & \cdots & (\alpha z^a)^{(M-1)^2}\end{Bmatrix}\bmod M(z)$$

$$\vdots$$

$$T_L(z)\equiv\begin{Bmatrix}1 & 1 & 1 & \cdots & 1\\ 1 & (\gamma z^c) & (\gamma z^c)^2 & \cdots & (\gamma z^c)^{L-1}\\ 1 & (\gamma z^c)^2 & (\gamma z^c)^4 & \cdots & (\gamma z^c)^{2(L-1)}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ 1 & (\gamma z^c)^{L-1} & (\gamma z^c)^{2(L-1)} & \cdots & (\gamma z^c)^{(L-1)^2}\end{Bmatrix}\bmod M(z).$$

$$[\boldsymbol{H}_{r,s,\cdots,t}(z)]_{M\times\cdots\times L}\equiv T_M(z)\cdots T_L(z)[H_{m,n,\cdots,l}(z)]_{M\times\cdots\times L}\bmod M(z)\qquad(28)$$

上式右端表示 $T_M(z)$ 对 $[H_{m,n,\cdots,l}(z)]_{M\times N\times\cdots\times L}$ 的第 1 个坐标进行变换，$\cdots$，$T_L(z)$ 对最后一个坐标进行变换。

同样，(27)式可改写为

$$[H_{m,n,\cdots,l}(z)]_{M\times\cdots\times L}\equiv V_M(z)\cdots V_L(z)[\boldsymbol{H}_{r,s,\cdots,t}(z)]_{M\times\cdots\times L}\bmod M(z).\qquad(29)$$

其中 $V_M(z),\cdots,V_L(z)$ 类似于二維变换的矩阵形式。

定理 13 设 $M(z)=p_1(z)^{l_1}\cdots p_s(z)^{l_s}$，则当且仅当

1° $(\alpha z^a)^M\equiv 1 \bmod M(z)$，$(\beta z^b)^N\equiv 1 \bmod M(z)$，$\cdots$，$(\gamma z^c)^L\equiv 1 \bmod M(z)$；

2° $(p_i(z),(\alpha z^a)^k-(\alpha z^a)^m)=1$ $(0\leqslant m<k\leqslant M-1)$

$(p_i(z),(\beta z^b)^k-(\beta z^b)^m)=1$ $(0\leqslant m<k\leqslant N-1)$ $(i=1,2,\cdots,s)$

$(p_i(z),(\gamma z^c)^k-(\gamma z^c)^m)=1$ $(0\leqslant m<k\leqslant L-1)$

时，(26) 和 (27) 为一对具有 CCP 的互逆变换。

定理 9 ～13的证明可仿二維情形。从略。

五、结束语

我们已详细讨论了二維及多維多项式变换的实现条件以及用二維多项式变换计算三維循环卷积的方法。如何将多项式变换算法在计算机上实现，有待进一步研究。

参考文献

[1] 蒋增荣，数论变换，上海科技出版社，1980.8.

[2] 蒋增荣，多项式变换及其在卷积计算中的应用，国防科技大学学报，1980年第3期。

[3] H.J.Nussbaumer, P.Quandalle, "Computation of Convolutions and Discreter Fourier Transforms by Polynomial Transforms", IBM J.RES. DEVELOP, Vol22, No2, MAR 1978.

[4] 蒋增荣、沙基昌，Winograd 富里叶变换算法(WFTA)与多项式变换第一章§4，国防科技大学资料室。

[5] 杜德利著，周仲良译，基础数论，上海科技出版社，1980.9.

Two-dimensional and Multi-dimensional Polynomial Transforms

Luo Jian-shu Dai Xi--ying

Abstract

In this paper, we put forward algorithm to compute digital cyclic convolutions using two-dimensional polynomial transforms, and indicated the number of arithmetic operations required to compute three-dimensional cyclic convolutions by two-dimensional polynomial transforms. Moreover, the paper discussed in detail on the conditions of the two-dimensional polynomial transforms and spread it to multi-dimensional polynomial transforms.