有限域上快速分块Jacket变换

黄成荣
(广西经贸职业技术学院信息工程系 南宁 530021)

摘 要 提出了一种在有限域上的简单上闭链分块逆Jacket变换(CBIJT)。为将高阶的上闭链逆Jacket矩阵(CBIJM)因式分解成单位矩阵和低阶稀疏矩阵,考虑运用带来快速变换的连续结构来减少计算负荷。采用类似的递归方式分析两个CBIJT,即单维和双维CBIJT。这两个CBIJT为单位矩阵和低阶CBIJT的多重Kronecker积。

关键词 元素逆矩阵,Jacket矩阵,有限域
中图法分类号 TN911 **文献标识码** A

Fast Construction of Block Jacket Transform over Finite Field

HUANG Cheng-rong
(Department of Information Engineering, Guangxi Economic Trade Polytechnic, Nanning 530021, China)

Abstract We constructed anovel cocyclic block-wise inverse Jacket transform(CBIJT) with a fast transform. To factorize the large-size cocyclic block-wise inverse Jacket matrix(CBIJM) into several low-orderidentitymatrices and sparse matrices, we achieved a successive architecture that leads to a fast transform while reducing computational load. Two kinds of the CBIJTs, named one-dimensional and two dimensional CBIJTs, were designed with a similar recursive fashion, which refers the above-mentioned multi-fold product of identity matrices and CBIJTs.

Keywords Element-inverse matrix, Jacket matrix, Finite field

1 引言

离散正交变换,比如离散傅里叶变换(DFT)和Walsh-Hadamard变换(WHT),在图像处理、特征选择、信号处理、数据压缩和编码等许多领域都有广泛运用[1,2]。基于DFT和WHT的正交性开发出了大众正交矩阵,这些矩阵被称为Jacket矩阵[3-5],更多细节可参考文献[6-9]。

定义1 一个$n\times n$的方矩阵$J_n=(\alpha_{ij})_{n\times n}$称为元素级逆Jacket矩阵,若其逆矩阵可由元素级逆运算得到,即$J_n^{-1}=\frac{1}{n}(\alpha_{ij}^{-1})_{n\times n}^{\mathrm{T}}$,$\forall i,j\in\{0,1,\cdots,n-1\}$,其中上标T代表转置。

Hadamard矩阵、DFT矩阵等均属于Jacket矩阵家族。

最近有研究得到n阶块级逆矩阵$[J]_n$,其中元素级逆Jacket矩阵J_n的复单位$\exp^{\sqrt{-1}(2\pi/p)}$被适当的矩阵单元替代[8-10]。

在数据编码和处理的许多应用中,上闭链矩阵发挥了重要作用[7,11]。

定义2 若G为一个r阶有限群,其操作为$\circ$,C是t阶Abelian群,则上闭链为映射$\phi:G\times G\to C$,且满足下式:

$$\phi(a,b)\phi(a\circ b,c)=\phi(a,b\circ c)\phi(b,c) \tag{1}$$

其中,$a,b,c\in G$,一个行a和列b可由固定阶位置(a,b)的元$\phi(a,b)\in C$索引的方矩阵$M(\phi)=(\phi(a,b))_{a,b\in G}$称作一个上闭链矩阵。若$\phi(1,1)=1$,则该矩阵为可做标准使用的归一化上闭链矩阵[11]。

由于生成自Hadamard矩阵,Jacket矩阵继承了Hadamard矩阵的优点,同时矩阵元不需要被限制为'±1'。然而,在目前的文献中,上闭链块矩阵并没有得到太多的重视,当前并没有上闭链块级逆Jacket矩阵(CBIJM)。本文将给出广义上闭链块Jacket矩阵,而且将考虑快速上闭链块级逆Jacket变换(CBIJT)。CBIJM不仅是值得关注的理论问题,而且在信号序列变换、数据处理、信号处理和编码学中都有许多实际应用。

2 上闭链块级逆Jacket变换

在逆矩阵的简单运算方面,Jacket矩阵得到了广泛运用[4-7]。本节中将看到,元素级逆Jacket矩阵可以推广到CBIJT的构造中。

对于可以被分区为$p\times p$块矩阵的p阶的单维块矩阵$[J]_p$,可以通过下面的变换将矢量x变换为另一个矢量y:

$$y=[J]_p x \tag{2}$$

为得到CBIJT,用α表示一个矩阵单元,其中给定质数p有$\alpha^p=I_p$。本文中,为简单起见,用I_p表示$p\times p$单位矩阵。令α为大小2×2的方矩阵:

$$\alpha=\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix} \tag{3}$$

容易证明$\alpha^2=I_2$。事实上,由于存在块级逆Jacket矩阵[8-10],矩阵α会被引入。可以看到高阶块Jacket矩阵$[J]_2$,$s\triangleq\alpha^{\otimes s}=\underbrace{\alpha\otimes\alpha\cdots\otimes\alpha}_{s}$实质上也是一个CBIJM,其中$\otimes$表示Kro-

本文受广西高等学校科研项目(20010YB190)资助。
黄成荣(1964—),男,副教授,主要研究方向为无线通信技术,E-mail:hchengrong@163.com。

necker 积。

接下来将讨论基于大小为 $p\times p$ 的矩阵单元 α 的广义块级逆 Jacket 矩阵$[J]_{p^s}$的上闭链性。特别地对于给定质数 p,定义置换矩阵单元 $\alpha^h=[e_{i,j}]_p$,

$$e_{i,j}=\begin{cases}1, & i=\langle j+h\rangle_p\\ 0, & i\neq\langle j+h\rangle_p\end{cases} \tag{4}$$

其中,$\langle j+h\rangle_p=j+h \bmod p,\forall i,j,h\in Z_p$。可以看到$\{\alpha^h:h\in Z_p\}$组成一个传统矩阵乘法的 Abelian 群。即上述具有矩阵单元 α 的 Abelian 群可被重写为$\{I,\alpha,\alpha^2,\cdots,\alpha^{p-1}\}$。

例 1　设 $p=3$,则有

$$I_3=\alpha^0=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix},\alpha^1=\begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix},$$

$$\alpha^2=\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix} \tag{5}$$

明显可知,具有乘法操作$\langle a\cdot b\rangle$的 $Z_p\equiv\{0,1,\cdots,p-1\}$为 p 阶有限域。对于$\forall a,x\in Z_p$,定义一个 Z_p 上的乘法函数 $f_a(x)$,即:

$$f_a(x)=\langle a\cdot x\rangle_p \tag{6}$$

通过链接 p 个矩阵 $\alpha^{h_i},\forall h_i\in Z_p$,定义一个大小为 $p\times p^2$ 的块矩阵:

$$[\beta]\overset{\triangle}{=}[\alpha^{h_0},\alpha^{h_1},\cdots,\alpha^{h_{p-1}}] \tag{7}$$

由此得到:

$$[\beta_a]\overset{\triangle}{=}[\alpha^{f_a(h_0)},\alpha^{f_a(h_1)},\cdots,\alpha^{f_a(h_{p-1})}]$$
$$=[\alpha^{\langle a\cdot h_0\rangle_p},\alpha^{\langle a\cdot h_1\rangle_p},\cdots,\alpha^{\langle a\cdot h_{p-1}\rangle_p}] \tag{8}$$

引理 1　$\forall a,b\in Z_p$,分块矩阵$[\beta_a]$和$[\beta_b]$,有:

$$[\beta_a]\cdot[\beta_b]^{\mathrm{T}}=\begin{cases}pI, & \langle a+b\rangle_p=0\\ 0, & \langle a+b\rangle_p\neq0\end{cases} \tag{9}$$

证明:如果 $a=0$,那么$[\beta_0]=[I,I,\cdots,I]$,并且$[\beta_0]\cdot[\beta_0]^{\mathrm{T}}=pI$。如果$\langle a+b\rangle_p=0,\forall a,b\in Z_p$,那么 $f_a(h_i)+f_b(h_i)=\langle ah_i\rangle_p+\langle bh_i\rangle_p=\langle(a+b)h_i\rangle_p=0$ 因此,容易验证:

$$[\beta_a]\cdot[\beta_b]^{\mathrm{T}}=\sum_{i=1}^{p}\alpha^{f_a(h_i)+f_b(h_i)}=pI$$

但是如果$\langle a+b\rangle_p\neq0$,那么对于 $0<\langle a+b\rangle_p<P$

$$\{0,\langle a+b\rangle_p,\langle 2(a+b)\rangle_p,\cdots,\langle(p-1)(a+b)\rangle_p\}=Z_p \tag{10}$$

因此

$$[\beta_a]\cdot[\beta_b]^{\mathrm{T}}=\sum_{i=0}^{p-1}\alpha^i, \tag{11}$$

因为 $\alpha^p-I=0$ 且 $\alpha\neq I$。可以证明$\sum_{i=1}^{p-1}\alpha^2$ 是 0。

本质上在有限域$\{0,I,\alpha\}$有零个元素。

2.1　分块 Jacket 逆矩阵

文献[8-10]中,Lee 等扩展了元素级逆 Jacket 矩阵以设计块级逆 Jacket 矩阵。

定义 3　一个 $np\times np$ 块矩阵$[J]_n=([\alpha_{ij}]_p)_{np\times np}$被称为 n 阶块级逆 Jacket 矩阵,如果$[J]_n^{-1}=\frac{1}{c}([\alpha_{ij}]^{-1})^{\mathrm{T}}_{np\times np}$,其中 c 为归一化值且$[\alpha_{ij}]_{p\times p}$表示一个大小为 $p\times p$ 的矩阵单元。

定义 4　对于一个给定的素数 p,设 α 是一个 $p\times p$ 矩阵单元,则 $\alpha^p=I$ 且$[\beta]=[\alpha^0,\alpha^1,\cdots,\alpha^{p-1}]$。

规定

$$[J]_p=\begin{bmatrix}\alpha^0&\alpha^0&\cdots&\alpha^0\\ \alpha^0&\alpha^1&\cdots&\alpha^{p-1}\\ \alpha^0&\alpha^2&\cdots&\alpha^{2(p-1)}\\ \vdots&\vdots&\ddots&\vdots\\ \alpha^0&\alpha^{p-1}&\cdots&\alpha^{(p-1)(p-1)}\end{bmatrix} \tag{12}$$

它的逆

$$[J]_p^{-1}=\begin{bmatrix}\alpha^0&\alpha^0&\cdots&\alpha^0\\ \alpha^0&\alpha^{\langle-1\rangle_p}&\cdots&\alpha^{\langle-(p-1)\rangle_p}\\ \alpha^0&\alpha^{\langle-2\rangle_p}&\cdots&\alpha^{\langle-2(p-1)\rangle}\\ \vdots&\vdots&\ddots&\vdots\\ \alpha^0&\alpha^{\langle-(p-1)\rangle_p}&\cdots&\alpha^{\langle-(p-1)(p-1)\rangle_p}\end{bmatrix} \tag{13}$$

因此$[J]_p\cdot[J]_p^{-1}=[J]_p^{-1}\cdot[J]_p=I$。

块级逆 Jacket 矩阵首次由 Lee 和 Hou[6] 提出,以在有限域中证明块 Jacket 矩阵的存在。接下来将看到该块级逆 Jacket 矩阵也是上闭链的。

定理 1　令 $G=Z_p$,其中有操作 $a\circ b=\langle a+b\rangle_p,\forall a,b\in Z_p$,且有传统乘法 $C=\{\alpha^i:i\in Z_p\}$。则式(12)中的块级逆 Jacket 矩阵$[J]_p$ 为归一化上闭链块矩阵,该矩阵的行和列均由递增阶(即 $0\prec1\prec\cdots\prec p-1$)在$(a,b)$位置的元 $\phi(a,b)$的 G 索引。

证明:根据式(12)中分块 Jacket 逆矩阵$[J]_p$,有 $\phi(a,b)=\alpha^{\langle a\cdot b\rangle_p}$。$\forall c\in Z_p$,有

$$\phi(a,b)\phi(a\circ b,c)=\alpha^{\langle a\cdot b\rangle_p}\cdot\alpha^{\langle(a+b)c\rangle_p}=\alpha^{\langle a\cdot b+(a+b)\cdot c\rangle_p} \tag{14}$$

另一方面,

$$\phi(a,b\circ c)\phi(b,c)=\alpha^{\langle a\cdot(b+c)\rangle_p}\cdot\alpha^{\langle b+c\rangle_p}=\alpha^{\langle a\cdot(b+c)+b\cdot c\rangle_p} \tag{15}$$

结合式(14) 和式(15),有

$$\phi(a,b)\phi(a\circ b,c)=\phi(a,b\circ c)\phi(b,c) \tag{16}$$

因此,Jacket 矩阵$[J]_p$ 是一个上闭链块矩阵。

2.2　p^s 阶上闭链块级逆 Jacket 矩阵

为得到高阶上闭链块级逆 Jacket 矩阵$[J]_{p^s}$,对任意质数 p 和非负数 s,给出如下引理[11]:

引理 2　令 A,B,C,D 为适当大小的矩阵,则

$$(A\otimes B)\cdot(C\otimes D)=(A\cdot C)\otimes(B\cdot D)$$
$$(A\otimes B)^{-1}=(A^{-1}\otimes B^{-1}) \tag{17}$$
$$(A\otimes B)^{\mathrm{T}}=(A^{\mathrm{T}}\otimes B^{\mathrm{T}})$$

定理 2　对于质数 p,令$[A]_p=[\alpha_{i,j}]_p$,$[B]_p=[\gamma_{s,t}]_p$ 为两个 p 阶上闭链块级逆 Jacket 矩阵,对应矩阵单元 α 和 γ 使得 $\alpha^p=I$ 和 $\gamma^p=I,\forall i,j,s,t\in Z$。则 2 重 Kronecker 乘积矩阵

$$[J]_{p^2}=[A]_p\otimes[B]_p \tag{18}$$

为一个阶为 p^2 的上闭链块级逆 Jacket 矩阵。

证明:因为 $a_{sj}\prec a_{si}$ 和$[B]_p=[\gamma_{s,t}]_p$ 均为块级逆 Jacket 矩阵,求逆如下:

$$[A]_p^{-1}=\frac{1}{p}[\alpha_{i,j}^{-1}]_p^{\mathrm{T}},[B]_p^{-1}=\frac{1}{p}[\gamma_{s,t}^{-1}]_p^{\mathrm{T}} \tag{19}$$

令$[A]_p\otimes[B]_p=[\sigma_{ip+s,jp+t}]_{p^2}$

其中,$\sigma_{ip+s,jp+t}=\alpha_{i,j}\cdot\gamma_{s,t}$表示两个矩阵的传统乘积。因此得到可直接由式(18)中初始块矩阵$[J]_{p^2}$之上的块级逆运算得出的逆矩阵$[J]_{p^2}^{-1}$。

$$[J]_{p^2}^{-1}=([A]_p[B]_p)^{-1}=([A]_p^{-1}\otimes[B]_p^{-1})^{-1}$$
$$=\frac{1}{p^2}[\alpha_{i,j}^{-1}\cdot\gamma_{s,t}^{-1}]_{p^2}^{\mathrm{T}}$$

$$=\frac{1}{p^2}[\sigma_{ip^{-1}+s,jp+t}]_{p^2}^{\mathrm{T}} \tag{20}$$

这意味着$[J]_{p^2}$是一个分块 Jacket 矩阵。

接下来将看到矩阵$[J]_{p^2}$为一个行和列均索引过的上闭链矩阵。设$[A]_p$和$[B]_p$为分别在Z_p索引过的上闭链：

$$\begin{cases}\alpha_{s1}\prec\alpha_{s2}\prec\cdots\prec\alpha_{sp},(\alpha_{sj}\in Z_p,\forall j\in Z_p)\\ b_{s1}\prec b_{s2}\prec\cdots\prec b_{sp},(b_{sk}\in Z_p,\forall k\in Z_p)\end{cases} \tag{21}$$

其中，$s\in\{r,c\}$，a_{rj}和a_{cj}表示块矩阵$[A]_p$的第j行和第j列索引，b_{rk}和b_{ck}表示块矩阵$[B]_p$的第k列和第k行索引，‘$\prec$’表示递增阶。则对于Z_{p^2}之上的p^2阶块矩阵$[J]_{p^2}$，其行列索引阶可定义为：

如果$a_{sj}\prec a_{si}$，$a_{sj}=a_{si}$，$b_{sk}\prec b_{sh}$，则

$$a_{sj}b_{sk}\prec a_{si}b_{sh} \tag{22}$$

基于$[J]_p$的$[J]_{p^2}$元定义为：

$$\phi_{p^2}(a_{ri}b_{rh},a_{cj}b_{ck})=\phi_p(a_{ri},a_{cj})\cdot\phi_p(b_{rh},b_{ck}) \tag{23}$$

对于$[A]_p$，$[B]_p$中的元$\phi_p(a_i,a_j)$，$\phi_p(b_h,b_k)$，$\forall a_i,a_j,a_l\in Z_p$，$\forall b_h,b_k,b_t\in Z_p$，有

$$\phi_p(a_i,a_j)\phi_p(a_i\circ a_j,a_l)=\phi_p(a_i,a_j\circ a_l)\phi_p(a_j,a_l) \tag{24}$$

$$\phi_p(b_h,b_k)\phi_p(b_h\circ b_k,b_t)=\phi_p(b_h,b_k\circ b_t)\phi_p(b_k,b_t) \tag{25}$$

表 1　$[J]_4$中索引与元的对应关系

$\vec{a}/\vec{b}\circ$		00	01	10	11
$\circ a\backslash b$		0	1	2	3
00	0	$\alpha^0\alpha^0\alpha^0\alpha^0$		$\alpha^0\alpha^0\alpha^0\alpha^0$	
01	1	$\alpha^0\alpha^0\alpha^0\alpha^1$		$\alpha^0\alpha^0\alpha^0\alpha^1$	
10	2	$\alpha^0\alpha^0\alpha^0\alpha^0$		$\alpha^1\alpha^0\alpha^1\alpha^0$	
11	3	$\alpha^0\alpha^0\alpha^0\alpha^1$		$\alpha^1\alpha^0\alpha^1\alpha^1$	

容易证明：

$$\phi_{p^2}(a_ib_h,a_jb_k)\phi_{p^2}(a_ib_h,a_jb_k\circ a_lb_t)=\phi_{p^2}(a_ib_h,a_jb_k\circ a_lb_t)\phi_{p^2}(a_jb_k,a_lb_t) \tag{26}$$

因此可见块矩阵$[J]_{p^2}$也是一个式(22)中索引阶的上闭链块矩阵，该引理完成证明。

推论 1　对任意质数p和非负数s，令

$$[J]_{p^s}=\underbrace{[J]_p\otimes[J]_p\otimes\cdots\otimes[J]_p}_{s} \tag{27}$$

则s重块矩阵$[J]_{p^s}$为一个p^s阶的 CBIJM。

注意到任意非负数s和质数p均存在于s重块 Jacket 矩阵$[J]_{p^s}$中。

表 2　$N=p^s$快速算法复杂度

	方向法	快速算法
ADD	$(N-1)N$	$sp^s(p-1)$
MUL	N^2	$sp^{s-1}(p-1)^2$

其中，ADD 和 MUL 分别代表加法和乘法。此外，基于分解算法的 4 阶块 Jacket 矩阵$[J]_4$可被重写为：

$$[J]_4=[J]_2\otimes[J]_2=(I_2\otimes[J]_2)([J]_2\otimes I_2) \tag{28}$$

其中，I_2表示大小为 2 × 2 的单位矩阵，简单描述了快速算法，即

$$\begin{bmatrix}\alpha^0&\alpha^0&\alpha^0&\alpha^0\\ \alpha^0&\alpha^1&\alpha^0&\alpha^1\\ \alpha^0&\alpha^0&\alpha^1&\alpha^1\\ \alpha^0&\alpha^1&\alpha^1&\alpha^0\end{bmatrix}=\begin{bmatrix}\alpha^0&\alpha^0&0&0\\ \alpha^0&\alpha^1&0&0\\ 0&0&\alpha^0&\alpha^0\\ 0&0&\alpha^0&\alpha^1\end{bmatrix}\times\begin{bmatrix}\alpha^0&0&\alpha^0&0\\ 0&\alpha^0&0&\alpha^0\\ \alpha^0&0&\alpha^1&0\\ 0&\alpha^0&0&\alpha^1\end{bmatrix} \tag{29}$$

从运算方面来说(即加法和乘法)，直接计算和快速变换的比较在表 2 中给出。从该表中可见，$N=4$时，若采用直接计算则需要 12 次加法和 16 次乘法，但如果采用快速变换算法，加法和乘法的次数可分别减少为 8 次和 4 次。给出的算法明显在计算效率上比直接计算更优。此外，若$p=4$，$s=2$时，则

$$\alpha^0=\begin{bmatrix}1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1\end{bmatrix},\alpha=\begin{bmatrix}0&0&0&1\\ 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\end{bmatrix},$$

$$\alpha^2=\begin{bmatrix}0&0&1&0\\ 0&0&0&1\\ 1&0&0&0\\ 0&1&0&0\end{bmatrix},\alpha^3=\begin{bmatrix}0&1&0&0\\ 0&0&1&0\\ 0&0&0&1\\ 1&0&0&0\end{bmatrix}, \tag{30}$$

从而有 4 阶块 Jacket 矩阵$[J]_4$：

$$[J]_4=\begin{bmatrix}\alpha^0&\alpha^0&\alpha^0&\alpha^0\\ \alpha^0&\alpha^1&\alpha^2&\alpha^3\\ \alpha^0&\alpha^2&\alpha^0&\alpha^2\\ \alpha^0&\alpha^3&\alpha^2&\alpha^1\end{bmatrix} \tag{31}$$

得到 2 重块 Jacket 矩阵$[J]_{4^2}=[J]_4\otimes[J]_4$，即

$$[J]_{4^2}=\begin{bmatrix}
\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^0\\
\alpha^0&\alpha^1&\alpha^2&\alpha^3&\alpha^0&\alpha^1&\alpha^2&\alpha^3&\alpha^0&\alpha^1&\alpha^2&\alpha^3&\alpha^0&\alpha^1&\alpha^2&\alpha^3\\
\alpha^0&\alpha^2&\alpha^0&\alpha^2&\alpha^0&\alpha^2&\alpha^0&\alpha^2&\alpha^0&\alpha^2&\alpha^0&\alpha^2&\alpha^0&\alpha^2&\alpha^0&\alpha^2\\
\alpha^0&\alpha^3&\alpha^2&\alpha^1&\alpha^0&\alpha^3&\alpha^2&\alpha^1&\alpha^0&\alpha^3&\alpha^2&\alpha^1&\alpha^0&\alpha^3&\alpha^2&\alpha^1\\
\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^1&\alpha^1&\alpha^1&\alpha^1&\alpha^2&\alpha^2&\alpha^2&\alpha^2&\alpha^3&\alpha^3&\alpha^3&\alpha^3\\
\alpha^0&\alpha^1&\alpha^2&\alpha^3&\alpha^1&\alpha^2&\alpha^3&\alpha^0&\alpha^2&\alpha^3&\alpha^0&\alpha^1&\alpha^3&\alpha^0&\alpha^1&\alpha^2\\
\alpha^0&\alpha^2&\alpha^0&\alpha^2&\alpha^1&\alpha^3&\alpha^1&\alpha^3&\alpha^2&\alpha^0&\alpha^2&\alpha^0&\alpha^3&\alpha^1&\alpha^3&\alpha^1\\
\alpha^0&\alpha^3&\alpha^2&\alpha^1&\alpha^1&\alpha^0&\alpha^3&\alpha^2&\alpha^2&\alpha^1&\alpha^0&\alpha^3&\alpha^3&\alpha^2&\alpha^1&\alpha^0\\
\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^2&\alpha^2&\alpha^2&\alpha^2&\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^2&\alpha^2&\alpha^2&\alpha^2\\
\alpha^0&\alpha^1&\alpha^2&\alpha^3&\alpha^2&\alpha^3&\alpha^0&\alpha^1&\alpha^2&\alpha^3&\alpha^0&\alpha^1&\alpha^2&\alpha^3&\alpha^0&\alpha^1\\
\alpha^0&\alpha^2&\alpha^0&\alpha^2&\alpha^2&\alpha^0&\alpha^2&\alpha^0&\alpha^2&\alpha^0&\alpha^2&\alpha^0&\alpha^2&\alpha^0&\alpha^2&\alpha^0\\
\alpha^0&\alpha^3&\alpha^2&\alpha^1&\alpha^2&\alpha^1&\alpha^0&\alpha^3&\alpha^2&\alpha^1&\alpha^0&\alpha^3&\alpha^2&\alpha^1&\alpha^0&\alpha^3\\
\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^3&\alpha^3&\alpha^3&\alpha^3&\alpha^2&\alpha^2&\alpha^2&\alpha^2&\alpha^1&\alpha^1&\alpha^1&\alpha^1\\
\alpha^0&\alpha^1&\alpha^2&\alpha^3&\alpha^3&\alpha^0&\alpha^1&\alpha^2&\alpha^2&\alpha^3&\alpha^0&\alpha^1&\alpha^1&\alpha^2&\alpha^3&\alpha^0\\
\alpha^0&\alpha^2&\alpha^0&\alpha^2&\alpha^3&\alpha^1&\alpha^3&\alpha^1&\alpha^2&\alpha^0&\alpha^2&\alpha^0&\alpha^1&\alpha^3&\alpha^0&\alpha^3\\
\alpha^0&\alpha^3&\alpha^2&\alpha^1&\alpha^3&\alpha^2&\alpha^1&\alpha^0&\alpha^2&\alpha^1&\alpha^0&\alpha^3&\alpha^1&\alpha^0&\alpha^3&\alpha^2
\end{bmatrix} \tag{32}$$

索引矩阵I_{4^2}为：

$$I_{16}=\begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&2&3&0&1&2&3&0&1&2&3&0&1&2&3\\
0&2&0&2&0&2&0&2&0&2&0&2&0&2&0&2\\
0&3&2&1&0&3&2&1&0&3&2&1&0&3&2&1\\
0&0&0&0&1&1&1&1&2&2&2&2&3&3&3&3\\
0&1&2&3&1&2&3&0&2&3&0&1&3&0&1&2\\
0&2&0&2&1&3&1&3&2&0&2&0&3&1&3&1\\
0&3&2&1&1&0&3&2&2&1&0&3&3&2&1&0\\
0&0&0&0&2&2&2&2&0&0&0&0&2&2&2&2\\
0&1&2&3&2&3&0&1&0&1&2&3&2&3&0&1\\
0&2&0&2&2&0&2&0&0&2&0&2&2&0&2&0\\
0&3&2&1&2&1&0&3&0&3&2&1&2&1&0&3\\
0&0&0&0&3&3&3&3&2&2&2&2&1&1&1&1\\
0&1&2&3&3&0&1&2&2&3&0&1&1&2&3&0\\
0&2&0&2&3&1&3&1&2&0&2&0&1&3&0&3\\
0&3&2&1&3&2&1&0&2&1&0&3&1&0&3&2
\end{bmatrix}\bmod 4 \tag{33}$$

该矩阵为一阶 4 进制 Reed-Mull 码的生成矩阵。2 重块 Jacket 矩阵$[J]_{4^2}$可被分解为：

$$[J]_{4^2}=[J]_4\otimes[J]_4=(I_4\cdot[J]_4)\otimes([J]_4\cdot I_4)$$
$$=(I_4\otimes[J]_4)([J]_4\otimes I_4) \tag{34}$$

参见式(35)以及图 1 的信号流图。

$[J]_{4^2}=$

$$\begin{bmatrix}
\alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
\alpha^0 & \alpha^1 & \alpha^2 & \alpha^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
\alpha^0 & \alpha^2 & \alpha^0 & \alpha^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
\alpha^0 & \alpha^3 & \alpha^2 & \alpha^1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & \alpha^0 & \alpha^1 & \alpha^2 & \alpha^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & \alpha^0 & \alpha^2 & \alpha^0 & \alpha^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & \alpha^0 & \alpha^3 & \alpha^2 & \alpha^1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^0 & \alpha^1 & \alpha^2 & \alpha^3 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^0 & \alpha^2 & \alpha^0 & \alpha^2 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^0 & \alpha^3 & \alpha^2 & \alpha^1 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^0 & \alpha^1 & \alpha^2 & \alpha^3\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^0 & \alpha^2 & \alpha^0 & \alpha^2\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^0 & \alpha^3 & \alpha^2 & \alpha^1
\end{bmatrix}\times$$

$$\begin{bmatrix}
\alpha^0 & 0 & 0 & 0 & \alpha^0 & 0 & 0 & 0 & \alpha^0 & 0 & 0 & 0 & \alpha^0 & 0 & 0 & 0\\
0 & \alpha^0 & 0 & 0 & 0 & \alpha^0 & 0 & 0 & 0 & \alpha^0 & 0 & 0 & 0 & \alpha^0 & 0 & 0\\
0 & 0 & \alpha^0 & 0 & 0 & 0 & \alpha^0 & 0 & 0 & 0 & \alpha^0 & 0 & 0 & 0 & \alpha^0 & 0\\
0 & 0 & 0 & \alpha^0 & 0 & 0 & 0 & \alpha^0 & 0 & 0 & 0 & \alpha^0 & 0 & 0 & 0 & \alpha^0\\
\alpha^0 & 0 & 0 & 0 & \alpha^1 & 0 & 0 & 0 & \alpha^2 & 0 & 0 & 0 & \alpha^3 & 0 & 0 & 0\\
0 & \alpha^0 & 0 & 0 & 0 & \alpha^1 & 0 & 0 & 0 & \alpha^2 & 0 & 0 & 0 & \alpha^3 & 0 & 0\\
0 & 0 & \alpha^0 & 0 & 0 & 0 & \alpha^1 & 0 & 0 & 0 & \alpha^2 & 0 & 0 & 0 & \alpha^3 & 0\\
0 & 0 & 0 & \alpha^0 & 0 & 0 & 0 & \alpha^1 & 0 & 0 & 0 & \alpha^2 & 0 & 0 & 0 & \alpha^3\\
\alpha^0 & 0 & 0 & 0 & \alpha^2 & 0 & 0 & 0 & \alpha^0 & 0 & 0 & 0 & \alpha^2 & 0 & 0 & 0\\
0 & \alpha^0 & 0 & 0 & 0 & \alpha^2 & 0 & 0 & \alpha^0 & \alpha^0 & 0 & 0 & 0 & \alpha^2 & 0 & 0\\
0 & 0 & \alpha^0 & 0 & 0 & 0 & \alpha^2 & 0 & 0 & 0 & \alpha^0 & 0 & 0 & 0 & \alpha^2 & 0\\
0 & 0 & 0 & \alpha^0 & 0 & 0 & 0 & \alpha^2 & 0 & 0 & 0 & \alpha^0 & 0 & 0 & 0 & \alpha^2\\
\alpha^0 & 0 & 0 & 0 & \alpha^3 & 0 & 0 & 0 & \alpha^2 & 0 & 0 & 0 & \alpha^1 & 0 & 0 & 0\\
0 & \alpha^0 & 0 & 0 & 0 & \alpha^3 & 0 & 0 & 0 & \alpha^2 & 0 & 0 & 0 & \alpha^1 & 0 & 0\\
0 & 0 & \alpha^0 & 0 & 0 & 0 & \alpha^3 & 0 & 0 & 0 & \alpha^2 & 0 & 0 & 0 & \alpha^1 & 0\\
0 & 0 & 0 & \alpha^0 & 0 & 0 & 0 & \alpha^3 & 0 & 0 & 0 & \alpha^2 & 0 & 0 & 0 & \alpha^1
\end{bmatrix} \tag{35}$$

一般地，2^s 阶块逆 Jacket 矩阵$[J]_{2^s}$可被如下的分解算法推广：

$$[J]_{2^s}=[J]_{2^{s-1}}\otimes[J]_2=\prod_{i=1}^{s}(I_{2^{s-i}}\otimes[J]_{2^{i-1}}) \tag{36}$$

其中，I_{2^i}表示大小为 $2^i\times 2^i$ 的单位矩阵，简单表示为 $I_{2^0}=1$。

图 1(a)和图 1(b)分别表示前向和逆向的 Jacket 变换。

推论 2 基于任意数 p 上的 p 阶块级逆 Jacket 矩阵$[J]_p$，p^s 阶 s 重块级逆 Jacket 矩阵可由以下递归公式构建：

$$[J]_{p^s}=\prod_{i=1}^{s}(I_{p^{s-i}}\otimes[J]_p\otimes I_{p^{i-1}}) \tag{37}$$

其中，s 是一个非负整数。

证明：对索引 s 进行归纳。$s=1$ 时明显为真，即$[J]_{p^1}=[J]_p$。对于接下来的值，假定以下前提对于 s 为真，即对 $\forall i\in\{1,2,\cdots,s\}$有以下假定：

$$[J]_{p^s}=\prod_{i=1}^{s}(I_{p^{s-i}}\otimes[J]_p\otimes I_{p^{i-1}}) \tag{38}$$

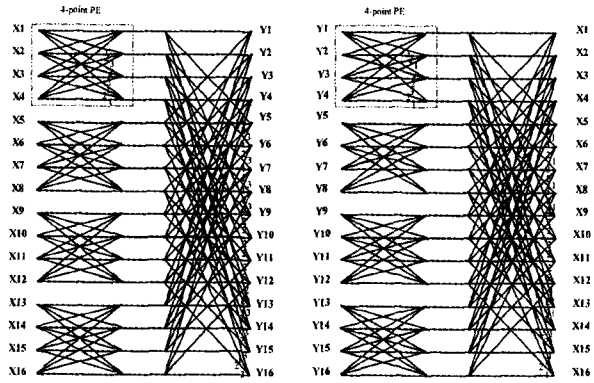
则对于 $s+1$ 也成立。事实上，通过引入基于 Kronecker 积特性可以得到：

$$[J]_{p^{s+1}}=[J]_p\otimes I_{p^s}=([J]_p\otimes I_p)\otimes(I_p\cdot[J]_{p^s})$$
$$=([J]_p\otimes I_{p^s})(I_p\otimes[J]_{p^s}) \tag{39}$$

结合式(38)和式(40)得到：

$$[J]_{p^{s+1}}=\prod_{i=1}^{s+1}(I_{p^{s-i}}[J]_p\otimes I_{p^{i-1}}) \tag{40}$$

则该推论证明完成。



(a)Forward Jacket Transform　　(b)Inverse Jacket Transform

图 1　一维 2 重上闭链块 Jacket 变换$[J]_{16}$的信号流图

2.3　低密度上闭链块级逆 Jacket 矩阵

接下来考虑 s 重 CBIJM $[J]_{p^s}$ 中的 1 的密度。基于之前提到的 CBIJM $[J]_p$，可知式(4)中矩阵$[J]_p$的矩阵单元 α 为 $p^2\times p^2$ 大小的单位矩阵。1 的数量为在每个矩阵单元 α^h 中的 p，$\forall\alpha^h$，$h\in Z_p$，则 α^h 中 1 的密度为：

$$\rho(\alpha^h)=\frac{p}{p^2}=\frac{1}{p} \tag{41}$$

因此$[J]_p$ 中 1 的密度计算公式为：

$$\rho([J]_p)=\rho(\alpha^h)=\frac{1}{p} \tag{42}$$

且 s 重矩阵$[J]_{p^s}$中 1 的密度是：

$$\rho([J]_{p^s})=\rho([J]_p)=\frac{1}{p} \tag{43}$$

更大的矩阵阶 p 意味着 CBIJM $[J]_p$ 和 s 重 CBIJM $[J]_{p^s}$ 中更小的 1 密度。

容易得知 α，$[J]_2$ 和 $[J]_{2^2}$ 中的 1 密度均为 1/2，即 $\rho([J]_{2^2})=\rho([J]_2)=\rho(\alpha)=1/2$。一般地，对于任意数 p，有 $\rho([J]_{p^2})=\rho([J]_p)=\rho(\alpha)=1/p$，如表 3 所列。

表 3　矩阵单元 α，CBIJM $[J]_p$ 和 s 重 CBIJM $[J]_{p^s}$ 的密度

	2	3	5	7	11
α	1/2	1/3	1/5	1/7	1/11
$[J]_p$	1/2	1/3	1/5	1/7	1/11
$[J]_{p^s}$	1/2	1/3	1/5	1/7	1/11

3　有限域上的上闭链块级逆 Jacket 矩阵

本节中，考虑有限域 $GF(2^m)$ 上的 CBIJM 的推广，以及得到对于 $p=2^{m-1}$ 的高阶 CBIJM。

令 α 为 $GF(2^m)$ 之上的矩阵单元，且 $\alpha^{2^{m-1}}=I$ 和 $\alpha\neq I$。则得到引理如下。

引理 3

$$\sum_{i=0}^{2^m-2}\alpha^{ir}=\begin{cases}(2^m-1)I, & \text{for } r=0\\ 0, & \text{for } 1\leqslant r\leqslant 2^m-2\end{cases} \tag{44}$$

证明：显然 $\sum_{i=0}^{2^m-2}\alpha^{ir}$ 包含 2^m-1 项。若 $r=0$，则 $\sum_{i=0}^{2^m-2}\alpha^{ir}$ 为 2^m-1 个单位矩阵之和，则第一个等式得到证明。现在考虑 $1\leqslant r\leqslant 2^m-2$ 且 $\alpha^r\neq I$，即，$\alpha^r-I\neq 0$ 的情况。因为 $\alpha^{2^m-1}=I$，则有 $\alpha^{r(2^m-1)}=I$ 且 $0=\alpha^{r(2^m-1)}-I=(\alpha^r-I)\sum_{i=0}^{2^m-1}\alpha^{ir}$，则 $\sum_{i=0}^{2^m-2}\alpha^{ir}=0$，证明完成。

定理 3 令 $[J]_{2^m-1}\overset{\triangle}{=}[\alpha^{ij}]_{2^m-1}$ 为 $GF(2^m)$ 之上的 (2^m-1) 阶块矩阵，$\forall i,j\in Z_{2^m-1}$，其中 α 为 $(2^m-1)\times(2^m-1)$ 大小的矩阵单元，且满足 $\alpha^{2^m-1}=I$ 和 $\alpha=I$。则块矩阵 $[J]_{2^m-1}$ 是一个 CBIJM。

证明：根据 (2^m-1) 阶块矩阵 $[J]_{2^m-1}$ 的定义，令 $[J]_{2^m-1}^{-1}=\frac{1}{2^m-1}[\alpha^{\langle -ij\rangle_{2^m-1}}]_{2^m-1}^{\mathrm{T}}$，利用引理 3 简单的计算，它可以验证 $[J]_{2^m-1}[J]_{2^m-1}^{-1}=[J]_{2^m-1}^{-1}[J]_{2^m-1}=I$。

可见块矩阵 $[J]_{2^m-1}$ 为块级逆 Jacket 矩阵。为证明其为一个 CBIJM，令 $\phi(i,j)$ 为位置 (i,j) 之上的元，其中行和列的阶在 Z_{2^m-1} 之上从 0 到 2^m-2，对于 $i,j,h,k\in Z_{2^m-1}$，有

$$\begin{aligned}&\phi(i,j)=\alpha^{\langle i\cdot j\rangle_{2^m-1}}\\ &\phi(i,j\circ h)=\alpha^{\langle i\cdot(i+j)\rangle_{2^m-1}}\\ &\phi(i,j)\phi(h,k)=\alpha^{\langle i\cdot j+h\cdot k\rangle_{2^m-1}}\end{aligned} \tag{45}$$

从而

$$\begin{aligned}\phi(i,j\circ k)\phi(j,k)&=\alpha^{\langle i\cdot(j+k)\rangle_{2^m-1}}\alpha^{\langle j\cdot k\rangle_{2^m-1}}\\ &=\alpha^{\langle i\cdot j+i\cdot k+j\cdot k\rangle_{2^m-1}}\end{aligned} \tag{46}$$

且

$$\begin{aligned}\phi(i,j)\phi(i\circ j,k)&=\alpha^{\langle i\cdot j\rangle_{2^m-1}}\alpha^{\langle(j+j)\cdot k\rangle_{2^m-1}}\\ &=\alpha^{\langle i\cdot j+i\cdot k+j\cdot k\rangle_{2^m-1}}\end{aligned} \tag{47}$$

容易验证

$$\phi(i,j\circ k)\phi(j,k)=\phi(i,j)\phi(i\circ j,k) \tag{48}$$

表明块矩阵 $[J]_{2^m-1}$ 是 $GF(2^m)$ 上的一个 CBIJM。

例 2 考虑 $GF(2^3)$ 之上本原多项式为 $x^3+x+1=0$ 的 7 阶块矩阵。令 α 为任意矩阵单元使得 $\alpha^7=I$ 和 $\alpha=I$。则 $GF(2^3)$ 之上的任意矩阵单元 β 可以被二进制矢量 (b_0,b_1,b_2) 表示，$\forall b_i\in\{0,1\}$ 且 $i\in\{0,1,2\}$，$\beta=b_0+b_1\alpha+b_2\alpha^2$。

由表 4 可知，在 $GF(2^3)$ 之上式(48)成立。

表 4 二进制表示的 $GF(2^3)$

g\h	012	3	456
0	$\alpha^0\alpha^0\alpha^0\alpha^0\alpha^0\alpha^0\alpha^0$		
1	$\alpha^0\alpha^1\alpha^2\alpha^3\alpha^4\alpha^5\alpha^6$		
2	$\alpha^0\alpha^2\alpha^4\alpha^6\alpha^1\alpha^3\alpha^5$		
3	$\alpha^0\alpha^3\alpha^6\alpha^2\alpha^5\alpha^1\alpha^4$		
4	$\alpha^0\alpha^4\alpha^1\alpha^5\alpha^2\alpha^6\alpha^3$		
5	$\alpha^0\alpha^5\alpha^3\alpha^1\alpha^6\alpha^4\alpha^2$		
6	$\alpha^0\alpha^6\alpha^5\alpha^4\alpha^3\alpha^2\alpha^1$		

$[J]_7$ 及 $[J]_7^{-1}$ 为

$$[J]_7=\begin{bmatrix}\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^0\\ \alpha^0&\alpha^1&\alpha^2&\alpha^3&\alpha^4&\alpha^5&\alpha^6\\ \alpha^0&\alpha^2&\alpha^4&\alpha^6&\alpha^1&\alpha^3&\alpha^5\\ \alpha^0&\alpha^3&\alpha^6&\alpha^2&\alpha^5&\alpha^1&\alpha^4\\ \alpha^0&\alpha^4&\alpha^1&\alpha^5&\alpha^2&\alpha^6&\alpha^3\\ \alpha^0&\alpha^5&\alpha^3&\alpha^1&\alpha^6&\alpha^4&\alpha^2\\ \alpha^0&\alpha^6&\alpha^5&\alpha^4&\alpha^3&\alpha^2&\alpha^1\end{bmatrix} \tag{49}$$

$$[J]_7^{-1}=\frac{1}{7}\begin{bmatrix}\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^0\\ \alpha^0&\alpha^6&\alpha^5&\alpha^4&\alpha^3&\alpha^2&\alpha^1\\ \alpha^0&\alpha^5&\alpha^3&\alpha^1&\alpha^6&\alpha^4&\alpha^2\\ \alpha^0&\alpha^4&\alpha^1&\alpha^5&\alpha^6&\alpha^2&\alpha^3\\ \alpha^0&\alpha^3&\alpha^6&\alpha^2&\alpha^5&\alpha^1&\alpha^4\\ \alpha^0&\alpha^2&\alpha^4&\alpha^6&\alpha^1&\alpha^3&\alpha^5\\ \alpha^0&\alpha^1&\alpha^2&\alpha^3&\alpha^4&\alpha^5&\alpha^6\end{bmatrix} \tag{50}$$

$$\begin{aligned}[J]_{p^{2s}}&=([J]_{p^s}\otimes I_{p^s})(I_{p^s}\otimes[J]_{p^s})\\ &=([J]_{p^{s-1}}\otimes I_p\otimes I_{p^s})(I_{p^{s-1}}\otimes[J]_p\otimes I_{p^s})(I_{p^s}\otimes\\ &\quad[J]_{p^{s-1}}\otimes I_p)(I_{p^s}\otimes I_{p^{s-1}}\otimes[J]_p)\end{aligned} \tag{51}$$

根据表 5 中给出的矩阵索引映射，容易得出式(49)中的矩阵 $[J]_7$ 为 $GF(2^3)$ 之上的 7 阶 CBIJM。

表 5 二进制表示的 $GF(2^3)$

元素	二进制表示
α^0	(0 0 0)
α^1	(1 0 0)
α^2	(0 1 0)
α^3	(1 1 0)
α^4	(0 1 1)
α^5	(1 1 1)
α^6	(1 0 1)

4 二维快速上闭链块 Jacket 变换

上一节考虑了一维 CBIJT，现在扩展到二维 CBIJM。二维 CBIJT 的快速算法可由文献[8]中的二维块级逆矩阵得到 $Y=[J]_{p^s}X[J]_{p^s}^{\mathrm{T}}$。

其可由列级拉直矢量 X 变换表示为：

$vec(Y)=([J]_{p^s}\otimes[J]_{p^s})vec(X)$

换言之，如果 $X=(x_0,x_1,\cdots,x_{p^s-1})$，那么 $vec(X)=(x_0^{\mathrm{T}},x_1^{\mathrm{T}},\cdots,x_{p^s-1}^{\mathrm{T}})^{\mathrm{T}}$，其中 x_i 为 X 的第 i^{th} 列，$\forall i\in Z_{p^s}$。则二维 CBIJT 的快速算法可由 2 重一维 CBIJT 求得，即 $[J]_{p^{2s}}=[J]_{p^s}\otimes[J]_{p^s}$。

根据 $[J]_{p^s}\otimes[J]_{p^s}$ 的快速算法，可得式(51)中表示的二维 CBIJT 快速算法。

即二维 CBIJT 与基于一维 CBIJT 分解的稀疏矩阵分解相关。可设计出用于减少计算负荷的连续架构，该架构通过低复杂度的方法分解二维 CBIJM 到低阶稀疏矩阵，以达到快速变换的目的。

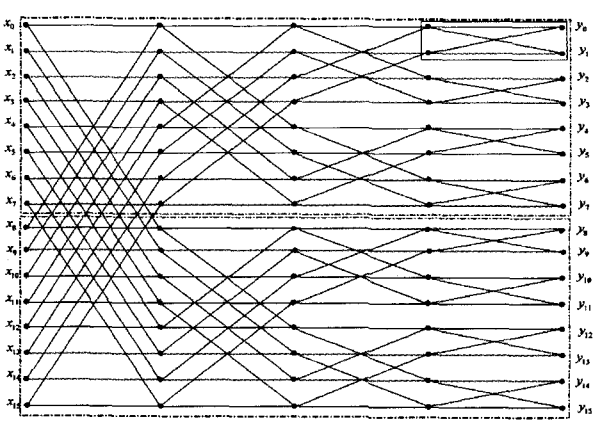


图 2 二维 2 重 4 阶 CBIJM $[J]16$ 的信号流图

例 3 考虑 2 维 4 阶 CBIJM

$[J]_{2^4}=[J]_{2^2}\otimes[J]_{2^2}$

$$=([J]_2\otimes I_2\otimes I_4)(I_2\otimes[J]_2\otimes I_4)\cdot(I_4\otimes[J]_2\otimes I_2)(I_4\otimes I_2[J]_2) \quad (52)$$

由上一节得知块矩阵$[J]_{2^2}$为一个可由快速算法构建的4阶CBIJM。因此，二维4阶CBIJT可以由基于2重4阶CBIJT的快速算法设计得到，如图2所示。

结束语 本文提出了一个设计快速一维和二维CBIJT的简单方法。该方法可以简单而清晰地将一个高阶CBIJM分解为多个低阶CBIJM。此分解算法对适当的矩阵单元α在单元有限域$GF(2^{p^s})$上的(p^s)阶CBIJM有效。同时这些结果对于其他以递归式开发基于稀疏矩阵的二维快速CBIJM也有借鉴价值。由于其架构的特殊连续性，可以考虑应用于区组设计(CD)和低密度校验(LDPC)之中。

参考文献

[1] Ahmed N, RaoK R. Orthogonal Transforms for Digital Signal Processing[M]. Springer-Verlag New York, Inc. Secaucus, NJ, USA, 1975

[2] Lee M H. The Center Weighted Hadamard Transform[J]. IEEE Trans. Circuits Syst, 1989, 36(9): 1247-1249

[3] Lee M H, Borrisov Y L. On Jacket transforms over finite fields [J]. IEEE Inter. Symp. Infor. Theory, 2009: 2803-2807

[4] Lee M H. A new reverse jacket transform and its fast algorithm [J]. IEEE Trans. Circuits and Systems II, AnalogDigit. Signal Process, 2000, 47(1): 39-47

[5] Lee M H, Rajan B S, Park J Y. A generalized reverse Jacket transform[J]. IEEE Trans. Circuits and Systems, 2001, 48(7): 684-690

[6] Lee M H, Guo Y. A Novel Construction of Jacket Matrix from Characters on finite Abelian Group[J]. IET ElectronicsLetters, 2010, 46

[7] Chen Z, Lee M H, Zeng G. Fast cocyclic Jacket transform[J]. IEEE Trans. Signal Processing, 2008, 56(5): 2143-2148

[8] Lee M H, Hou J. Fast block inverse Jacket transform[J]. IEEE Signal Process. Lett., 2006, 13(4): 461-464

[9] Zeng G, Lee M H. A generalized reverse block Jacket transform [J]. IEEE Trans. Circuits and Systems, 2008, 55(6): 1589-1600

[10] Lee M H, Zhang X D. Fast Block Center Weighted Hadamard Transform[J]. IEEE Trans. Circuit & Systems, 2007, 54(12): 2741-2745

[11] Horadam K J, Udaya P. Cocyclic Hadamard Codes [J]. IEEE Trans. Infor. Theory, 2000, 46(4): 1545-1550

(上接第190页)

用户的满意度、节约了通信的信令开销，进而提高了通信系统的QoS。

对图5分析如下：

其示出实验数据空间一定的情况下本文算法与传统算法的运行时间对比结果，本文所需要的时间比传统算法所需要的时间短，当数据量增大时，本文的这种优势会更明显。这样降低了预测所需要的时间，进一步降低了掉话率，提高了通信服务质量。

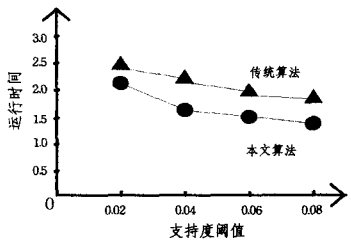


图5 支持度阈值与运行时间对比图

结束语 本文在研究现有位置预测的基础上提出了基于频繁轨迹挖掘的预测方案，将该方案应用于蜂窝移动通信系统的越区切换中，并通过对仿真结果图的分析得出结论：本文所提出的方案优于传统方案，提高了通信系统的整体质量，在实际通信实践中具有指导意义，它为未来解决小蜂窝、频繁切换、支持大量用户与多媒体应用的问题提供了新的思路。另外，该方案在实际应用中还有若干问题有待解决，如，当数据规模较为庞大时如何使存储以及读取效率更高，在历史移动轨迹数据更新时如何高效更新频繁轨迹集合，此问题有待进一步研究。

参考文献

[1] Becvar Z, Mach P. Adaptive hysteresis margin for handover in femtocell networks[C]// 2010 6th International Conference on Wireless and Mobile Communications (ICWMC). IEEE, 2010: 256-261

[2] Singhrova A, Prakash N. Vertical handoff decision algorithm for improved quality of service in heterogeneous wireless networks [J]. IET Communications, 2012, 6(2): 211-223

[3] 魏垚. 蜂窝移动通信系统物理小区识别自组织技术研究[D]. 北京：北京邮电大学，2013

[4] Piro G, Grieco L A, Boggia G, et al. Simulating LTE Cellular Systems: An Open-Source Framework [J]. IEEE Transactions on Vehicular Technology, 2011, 60(2): 498-513

[5] Jara A J, Silva R M, Silva J S, et al. Mobile IP-Based Protocol for Wireless Personal Area Networks in Critical Environments [J]. Wireless Personal Communications, 2011, 61(4): 711-737

[6] Ramanathan P, Agrawal P, Kishore S, et al. Dynamic resource allocation schemes during handoff for mobile multimedia wireless networks[J]. IEEE Journal on Selected Areas in Communications, 1999, 17(7): 1270-1283

[7] 李小文，等. TD-SCDMA第三代移动通信系统、信令及实现[M]. 北京：人民邮电出版社，2006

[8] 刘雪洁，刘衍珩，李奇. 移动环境下基于策略的信道资源管理研究[J]. 计算机科学，2009(4): 97-100

[9] 宁国勤，张静，刘干，朱光喜. 异构分层无线网络中基于业务QoS保证的切换策略研究[J]. 计算机科学，2010(1): 83-86

[10] Song Li-bo, Kotz D, Jain R, et al. Evaluating location predictors with extensive Wi-Fi mobility data [C] // INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies. 2004, 2: 1414-1424

[11] Jeong B, Shin S, Jang I, et al. A Smart Handover Decision Algorithm Using Location Prediction for Hierarchical Macro/Femto-Cell Networks[C]// 2011 IEEE Vehicular Technology Conference. [v. 3]. 2011: 1759-1763

[12] Chen S-M, Sue P-J. Constructing concept maps for adaptive learning systems based on data mining techniques[J]. Expert Systems with Application, 2013, 40(7): 2746-2755

[13] Tsukamoto K, Kashihara S, Taenaka Y, et al. An efficient handover decision method based on frame retransmission and data rate for multi-rate WLANs[J]. Ad hoc Networks, 2013, 11(1): 324-338