sponds to the introduction of a second parameter, both being correlated by a ratio of approximately 4:1.

Qualitatively, the narrow Gaussian models primary extinction and the four-times-wider Gaussian models secondary extinction. There is no physical reason for the constraint of the ratio of 4:1 for the half-widths of the two Gaussians as imposed by the assumption of a Lorentzian mosaic distribution. The model should become much more flexible if the ratio of the half-widths is a free parameter in some fixed limits. Additionally the relative normalization of the two Gaussians can be introduced as a free parameter under the natural constraint that the sum of the two must normalize to 1.

References

BACHMANN, R., KOHLER, H., SCHULZ, H. & WEBER, H.-P. (1985). *Acta Cryst.* A**41**, 35-40.
BECKER, P. J. & COPPENS, P. (1974). *Acta Cryst.* A**30**, 129-147, 148-153.
BECKER, P. & DUNSTETTER, F. (1984). *Acta Cryst.* A**40**, 241-251.
BOEHM, J. M., PRAGER, P. R. & BARNEA, Z. (1974). *Acta Cryst.* A**30**, 335-337.
BOURRET, A., THIBAULT-DESSAUX, J. & SEIDMANN, D. N. (1984). *J. Appl. Phys.* **55**, 825-836.
DEMARCO, J. J. & WEISS, R. J. (1965). *Acta Cryst.* **19**, 68-72.
GRAF, H. A. & SCHNEIDER, J. R. (1986). *Phys. Rev. B*, **34**, 8629-8638.
JAMES, F. & ROSS, M. (1975). *Comput. Phys. Commun.* **10**, 343-367.
KATO, N. (1976). *Acta Cryst.* A**32**, 453-457, 458-466.
KATO, N. (1979). *Acta Cryst.* A**35**, 9-16.
KATO, N. (1980*a*). *Acta Cryst.* A**36**, 171-177.
KATO, N. (1980*b*). *Acta Cryst.* A**36**, 763-769, 770-778.
MAZZONE, G. (1981). *Acta Cryst.* A**37**, 391-397.
PONCE, F. A. & HAHN, H. (1984). In *Electron Microscopy of Materials, Mater. Res. Soc. Proc.*, Vol. 31, edited by W. KRAKOW, D. A. SMITH & L. W. HOBBS, p. 153. New York: North Holland.
SCHNEIDER, J. R. (1977). *Acta Cryst.* A**33**, 235-243.
SCHNEIDER, J. R. (1983). *J. Cryst. Growth*, **65**, 660-671.
SCHNEIDER, J. R., GONÇALVES, O. D., ROLLASON, A. J., BONSE, U., LAUER, J. & ZULEHNER, W. (1988). *Nucl. Instrum. Methods Phys. Res.* B**29**, 661-674.
SCHNEIDER, J. R. & GRAF, H. A. (1986). *J. Cryst. Growth*, **74**, 191-202.
SCHNEIDER, J. R., JØRGENSEN, J. E. & SHIRANE, G. (1986). *Phase Transitions*, **8**, 17-34.
SCHNEIDER, J. R. & KRETSCHMER, H. R. (1985). *Z. Naturwiss.* **72**, 249-259.
TEMPELHOFF, K., GLEICHMANN, R., SPIEGELBERG, F. & WRUCH, D. (1979). *Phys. Status Solidi A*, **56**, 213-223.
ZACHARIASEN, W. H. (1967). *Acta Cryst.* **23**, 558-564.

Acta Cryst. (1988). A**44**, 467-478

Evaluating Finite Fourier Transforms that Respect Group Symmetries

BY L. AUSLANDER

Department of Mathematics, CUNY Graduate Center, 33 West 42 St, New York, NY 10036, USA

R. W. JOHNSON

Department of Computer Science, CUNY Graduate Center, 33 West 42 St, New York, NY 10036, USA

AND M. VULIS

Department of Computer Science, CCNY, Convent Ave at 138th St, New York, NY 10031, USA

(*Received 28 February 1987; accepted 12 February 1988*)

Abstract

A general method for producing efficient algorithms to evaluate finite Fourier transforms that fully utilize symmetry to reduce both computing time and space requirements is described. The method is applicable to all space groups. The resulting algorithms retain the '$N \log N$' behavior of the fast Fourier transform while reducing the size of the data to approximately an asymmetric unit. The algorithm for the $p3$ and $P3$ groups is shown.

0108-7673/88/040467-12$03.00

I. Introduction

The standard method for efficiently computing three-dimensional finite Fourier transforms is by Cooley-Tukey and Good-Thomas algorithms. Ten Eyck (1973) in his pioneering work on crystallographic fast Fourier transforms showed how certain groups of crystallographic symmetries could be combined with such algorithms to reduce the computational burden. There are two main features of the Ten Eyck algorithms: (1) the groups of symmetries must carry the sample points onto themselves; and (2) when we reduce the finite Fourier transform to the asymmetric unit, they can still be evaluated by the above efficient algorithms. Ten Eyck pointed out that his methods will not work for general crystallographic groups.

Basically the Cooley–Tukey and Good–Thomas algorithms use the additive properties of the integers. In recent years, starting with an idea of Rader (1968), Winograd (1978) has developed new algorithms for efficiently computing finite Fourier transforms based on the 'multiplicative' properties of the integers. In this paper we will show how multiplicative algorithms match with crystallographic symmetry groups to produce efficient finite Fourier transforms when restricted to the asymmetric unit for $P3$. In subsequent papers we will show how these algorithms can be made to work for all crystallographic groups.

Our approach is based on standard ideas used in the study of crystal symmetries: groups acting on spaces, equivalent points and asymmetric units. The essential new ingredient in our approach is to introduce what we call multiplicative groups M (these come from the multiplicative properties of the integers), an ordering of the elements of M, a group CM built from the group $P3$ and M, and tensor skew-circulant matrices. In an extremely abridged form our method consists of finding equivalent points and an asymmetric unit for the group CM acting on the sample points. This information, combining with the ordering on M, enables us to structure the finite Fourier transform restricted to the $P3$ asymmetric unit so that it breaks into blocks of tensor skew-circulant matrices which by Winograd theory can be computed efficiently.

In this paper we will carry out this program in two stages. Stage 1 will treat the two-dimensional space group $p3$ acting on 5×5 points, which although a toy example does let us show in a simple setting many of our ideas. Stage 2 will consist of a treatment of $P3$ acting on $60\times 60\times 60$ points. We have chosen a presentation of stage 2 that shows all of the ideas in our approach, but we have omitted many of the technical details that are necessary when one really writes computer code. The technical computer coding ideas will be presented in a subsequent paper.

II. Tensor skew-circulant matrices

The essential feature of Winograd-type algorithms is that they efficiently compute the product of a tensor skew-circulant matrix and a vector. A 4×4 skew-circulant matrix is defined as a matrix of the form

$$M=\begin{pmatrix} m_1 & m_2 & m_3 & m_4\\ m_2 & m_3 & m_4 & m_1\\ m_3 & m_4 & m_1 & m_2\\ m_4 & m_1 & m_2 & m_3\end{pmatrix}.$$

An $n\times n$ skew-circulant matrix is of the form

$$N=\begin{pmatrix} a_1 & a_2 & \dots & a_{n-1} & a_n\\ a_2 & a_3 & \dots & a_n & a_1\\ \vdots & \vdots & & \vdots & \vdots\\ a_n & a_1 & \dots & a_{n-2} & a_{n-1}\end{pmatrix}.$$

Thus, if X and Y are n-vectors and N is skew-circulant, there is an efficient algorithm to perform the linear computation: $Y=NX$.

But even more is true. For instance if M and N are as above, then the $4n\times 4n$ matrix written in $n\times n$ block form as

$$\begin{pmatrix} m_1N & m_2N & m_3N & m_4N\\ m_2N & m_3N & m_4N & m_1N\\ m_3N & m_4N & m_1N & m_2N\\ m_4N & m_1N & m_2N & m_3N\end{pmatrix}$$

is called the tensor product of M and N and denoted by $M\otimes N$. Similarly, we may form $M\otimes N\otimes S$ also. If M, N and S are skew-circulant, we will call such matrices tensor skew-circulant. The essential point is that there exist efficient algorithms for evaluating tensor skew-circulant matrices operating on vectors.

In this paper we will encounter only three types of tensor skew-circulant matrices. We will now pause to discuss these examples. Let B and C be 2×2 skew-circulant matrices

$$B=\begin{pmatrix} b_1 & b_2\\ b_2 & b_1\end{pmatrix} \quad\text{and}\quad C=\begin{pmatrix} c_1 & c_2\\ c_2 & c_1\end{pmatrix},$$

and let M be a 4×4 skew-circulant matrix as above. In this paper we will encounter $B\otimes C$, $B\otimes M$ or $C\otimes M$, and $B\otimes C\otimes M$.

We will write them out in detail so that when they arise in the rest of the paper they can be readily recognized. We have

$$B\otimes C=\begin{pmatrix} b_1C & b_2C\\ b_2C & b_1C\end{pmatrix}=\begin{pmatrix} b_1c_1 & b_1c_2 & b_2c_1 & b_2c_2\\ b_1c_2 & b_1c_1 & b_2c_2 & b_2c_1\\ b_2c_1 & b_2c_2 & b_1c_1 & b_1c_2\\ b_2c_2 & b_2c_1 & b_1c_2 & b_1c_1\end{pmatrix},$$

which can be seen to consist of four 2×2 skew-circulant blocks arranged in a skew-circulant pattern. Similarly,

$$C\otimes M=\begin{pmatrix} c_1M & c_2M\\ c_2M & c_1M\end{pmatrix}$$

$$=\begin{pmatrix} c_1m_1 & c_1m_2 & c_1m_3 & c_1m_4 & c_2m_1 & c_2m_2 & c_2m_3 & c_2m_4\\ c_1m_2 & c_1m_3 & c_1m_4 & c_1m_1 & c_2m_2 & c_2m_3 & c_2m_4 & c_2m_1\\ c_1m_3 & c_1m_4 & c_1m_1 & c_1m_2 & c_2m_3 & c_2m_4 & c_2m_1 & c_2m_2\\ c_1m_4 & c_1m_1 & c_1m_2 & c_1m_3 & c_2m_4 & c_2m_1 & c_2m_2 & c_2m_3\\ c_2m_1 & c_2m_2 & c_2m_3 & c_2m_4 & c_1m_1 & c_1m_2 & c_1m_3 & c_1m_4\\ c_2m_2 & c_2m_3 & c_2m_4 & c_2m_1 & c_1m_2 & c_1m_3 & c_1m_4 & c_1m_1\\ c_2m_3 & c_2m_4 & c_2m_1 & c_2m_2 & c_1m_3 & c_1m_4 & c_1m_1 & c_1m_2\\ c_2m_4 & c_2m_1 & c_2m_2 & c_2m_3 & c_1m_4 & c_1m_1 & c_1m_2 & c_1m_3\end{pmatrix}$$

consists of four 4×4 skew-circulant blocks in a skew-circulant pattern. $B\otimes M$ exhibits the same pattern. Finally,

$$B\otimes C\otimes M=\begin{pmatrix} b_1C\otimes M & b_2C\otimes M\\ b_2C\otimes M & b_1C\otimes M\end{pmatrix}$$

$$=\begin{pmatrix} b_1c_1M & b_1c_2M & b_2c_1M & b_2c_2M\\ b_1c_2M & b_1c_1M & b_2c_2M & b_2c_1M\\ b_2c_1M & b_2c_2M & b_1c_1M & b_1c_2M\\ b_2c_2M & b_2c_1M & b_1c_2M & b_1c_1M\end{pmatrix},$$

which is a skew-circulant pattern of four 8×8 blocks each of which is a skew-circulant pattern of four 4×4 blocks, each of which is the 4×4 skew-circulant matrix b_ic_jM.

We will now see how skew-circulant matrices can be found in finite Fourier transform matrices. Consider the finite Fourier transform matrix $F(5)$ on five points relative to the standard basis. Explicitly, if we let $\omega=e^{2\pi i/5}$, then

$$F(5)=\begin{pmatrix} 1&1&1&1&1\\ 1&\omega&\omega^2&\omega^3&\omega^4\\ 1&\omega^2&\omega^4&\omega&\omega^3\\ 1&\omega^3&\omega&\omega^4&\omega^2\\ 1&\omega^4&\omega^3&\omega^2&\omega\end{pmatrix}.$$

This matrix has no apparent skew-circulant pattern, but if we permute rows and columns, *i.e.* reorder the basis vectors, then we obtain a matrix which has a large skew-circulant piece. To be precise, if we permute the fourth and fifth columns and rows, we obtain a matrix $F_p(5)$ given by

$$F_p(5)=\begin{pmatrix} 1&1&1&1&1\\ 1&\omega&\omega^2&\omega^4&\omega^3\\ 1&\omega^2&\omega^4&\omega^3&\omega\\ 1&\omega^4&\omega^3&\omega&\omega^2\\ 1&\omega^3&\omega&\omega^2&\omega^4\end{pmatrix}.$$

Now a skew-circulant matrix is evident as the lower right-hand 4×4 submatrix.

III. Finite Fourier transforms on 5 and 5×5 points

To simplify notation we will use Z_n to denote the integers modulo n, $Z_n\times Z_n$ to denote ordered pairs (a,b) with a, $b\in Z_n$, and $Z_n\times Z_n\times Z_n$ to denote ordered triples (a,b,c) with a, b, $c\in Z_n$.

In this section we will consider Z_5 and $Z_5\times Z_5$. For a, $b\in Z_5$, we may form $a+b\in Z_5$ and $a\times b\in Z_5$. We say that $a\in Z_5$ is a unit provided there exists a b in Z_5 such that $a\times b=1$ in Z_5. The set of units in Z_5 will be denoted by $U(5)$. Clearly, $1\in U(5)$ and because $2\times 3\equiv 1 \pmod 5$, $2,3\in U(5)$, and because $4\times 4\equiv 1 \pmod 5$, $4\in U(5)$. Thus $U(5)$ consists of the elements 1, 2, 3, 4 or all of the non-zero elements of Z_5 and one checks that $U(5)$ forms an Abelian group under multiplication. Furthermore, we have 1, 2, $2^2\equiv 4 \pmod 5$, $2^3\equiv 3 \pmod 5$, $2^4\equiv 1 \pmod 5$, and so the element 2 multiplicatively generates $U(5)$, and its powers 1, 2, 2^2, 2^3 form an ordering of $U(5)$.

We define the action of the group $U(5)$ on Z_5 as follows: for $u\in U(5)$ and $a\in Z_5$ define $u(a)=u\times a\equiv ua \pmod 5$. Using this action we say that a, $b\in Z_5$ are equivalent if there is a $u\in U(5)$ such that $a=u(b)$ and write $[a]$ for the set of points equivalent to a in Z_5. Since $u(0)=0$ for all $u\in U(5)$, $[0]=0$. By the discussion above $[1]=1$, 2, 4, 3, so that Z_5 is the disjoint union of the sets $[0]$ and $[1]$, and hence the two points 0 and 1 form an asymmetric unit for the group $U(5)$ acting on Z_5.

Since we have an ordering on the group $U(5)$, the sets $[a]$ in Z_5 are naturally ordered by $U(5)$ by simply applying the elements $u\in U(5)$ in order to the element $a\in Z_5$. $[a]=2^0(a)$, $2^1(a)$, $2^2(a)$, $2^3(a)$ or a, $2a$, $4a$, $3a$. (Not all of these elements need be distinct as in the case of $[0]=0$, 0, 0, 0 or simply 0.) Since our objective is to find a matrix form of the five-point Fourier transform we need to extend this ordering to the whole of Z_5. Since 0, 1 is an asymmetric unit for $U(5)$ acting on Z_5, $[0]$, $[1]$ is a listing of all the elements of Z_5 with each ordered by Z_5. Thus we obtain the ordered listing of Z_5, 0, 1, 2×1, $2^2\times 1$, $2^3\times 1$ or 0, 1, 2, 4, 3.

This ordering of Z_5 provides a matrix form of the finite Fourier transform. Again, letting $\omega=e^{2\pi i/5}$, we have the result that the matrix entry of the a row and b column is ω^{ab}. Thus in this ordering we have

$$F_p(5)=\begin{array}{c} \\ 0\\ 1\\ 2\\ 2^2\\ 2^3\end{array}\begin{array}{c} \begin{array}{ccccc} 0 & 1 & 2 & 2^2 & 2^3\end{array}\\ \begin{pmatrix} \omega^{0\times 0} & \omega^{0\times 1} & \omega^{0\times 2} & \omega^{0\times 2^2} & \omega^{0\times 2^3}\\ \omega^{1\times 0} & \omega^{1\times 1} & \omega^{1\times 2} & \omega^{1\times 2^2} & \omega^{1\times 2^3}\\ \omega^{2\times 0} & \omega^{2\times 1} & \omega^{2\times 2} & \omega^{2\times 2^2} & \omega^{2\times 2^3}\\ \omega^{2^2\times 0} & \omega^{2^2\times 1} & \omega^{2^2\times 2} & \omega^{2^2\times 2^2} & \omega^{2^2\times 2^3}\\ \omega^{2^3\times 0} & \omega^{2^3\times 1} & \omega^{2^3\times 2} & \omega^{2^3\times 2^2} & \omega^{2^3\times 2^3}\end{pmatrix}\end{array}$$

and evaluating all the expressions modulo 5 we obtain

$$F_p(5)=\begin{array}{c} \\ 0\\ 1\\ 2\\ 4\\ 3\end{array}\begin{array}{c} \begin{array}{ccccc} 0 & 1 & 2 & 4 & 3\end{array}\\ \begin{pmatrix} \omega^0&\omega^0&\omega^0&\omega^0&\omega^0\\ \omega^0&\omega^1&\omega^2&\omega^4&\omega^3\\ \omega^0&\omega^2&\omega^4&\omega^3&\omega^1\\ \omega^0&\omega^4&\omega^3&\omega^1&\omega^2\\ \omega^0&\omega^3&\omega^1&\omega^2&\omega^4\end{pmatrix}\end{array}=\begin{pmatrix} 1&1&1&1&1\\ 1&\omega&\omega^2&\omega^4&\omega^3\\ 1&\omega^2&\omega^4&\omega^3&\omega\\ 1&\omega^4&\omega^3&\omega&\omega^2\\ 1&\omega^3&\omega&\omega^2&\omega^4\end{pmatrix}$$

which has a 4×4 skew-circulant submatrix in the lower right-hand corner.

Thus we see that by introducing the ordered multiplicative group $U(5)$ and studying the equivalent points and an asymmetric unit for the action of this group on Z_5, we can rewrite $F(5)$ as a matrix with a large skew-circulant block.

It is easier to see the patterns in the various forms of the finite Fourier transform matrix if in displaying it we drop the root of unity ω and simply show the exponents. So we will write

$$\hat{F}(5)=\begin{pmatrix}0&0&0&0&0\\0&1&2&3&4\\0&2&4&1&3\\0&3&1&4&2\\0&4&3&2&1\end{pmatrix}$$

and our new form,

$$\hat{F}_p(5)=\begin{pmatrix}0&0&0&0&0\\0&1&2&4&3\\0&2&4&3&1\\0&4&3&1&2\\0&3&1&2&4\end{pmatrix}.$$

Let us now consider the two-dimensional finite Fourier transform $F(5,5)$ on $Z_5\times Z_5$. If $X(a,b)$, a, $b\in Z_5\times Z_5$ is the input and $Y(c,d)$, c, $d\in Z_5\times Z_5$ is the output then

$$Y(c,d)=\sum_{(a,b)\in Z_5\times Z_5}\exp[(2\pi i/5)(ac+bd)]X(a,b).$$

To view this as a matrix operating on a 25-vector requires that we choose a basis, *i.e.* order the elements of $Z_5\times Z_5$. We will now carry out the above construction in this two-dimensional case. First, we will introduce an ordered multiplicative group $M=U(5)$ acting on $Z_5\times Z_5$, and then determine its equivalent points and asymmetric unit. Finally, we will establish an ordering on $Z_5\times Z_5$ that yields skew-circulant blocks in the matrix representing the Fourier transform on $Z_5\times Z_5$.

For $u\in U(5)$ and $(a,b)\in Z_5\times Z_5$ define

$$m_u=\begin{pmatrix}u&0\\0&u\end{pmatrix}$$

and let

$$m_u(a,b)=\begin{pmatrix}u&0\\0&u\end{pmatrix}\begin{pmatrix}a\\b\end{pmatrix}=\begin{pmatrix}ua&0\\0&ub\end{pmatrix}$$

where all arithmetic operations are performed modulo 5. Since, for u_1, $u_2\in U(5)$

$$m_{u_1}m_{u_2}=\begin{pmatrix}u_1&0\\0&u_1\end{pmatrix}\begin{pmatrix}u_2&0\\0&u_2\end{pmatrix}=\begin{pmatrix}u_1u_2&0\\0&u_1u_2\end{pmatrix}=m_{u_1u_2},$$

the set M of m_u of all $u\in U(5)$ is an ordered group acting on $Z_5\times Z_5$. In fact, it is just another way of writing $U(5)$ so that it acts in two dimensions.

We will now describe a construction that will help us study the action of groups on sets and select asymmetric units. This will produce a table of elements of the set organized in such a way that the action of the group can easily be seen. Table 1 shows the action of M on $Z_5\times Z_5$.

Table 1. *The action of the group M on $Z_5\times Z_5$*

		m_1	m_2	m_4	m_3
$\begin{bmatrix}0\\0\end{bmatrix}$	=	$\begin{pmatrix}0\\0\end{pmatrix}$			
$\begin{bmatrix}0\\1\end{bmatrix}$	=	$\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}0\\2\end{pmatrix}$	$\begin{pmatrix}0\\4\end{pmatrix}$	$\begin{pmatrix}0\\3\end{pmatrix}$
$\begin{bmatrix}1\\0\end{bmatrix}$	=	$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}2\\0\end{pmatrix}$	$\begin{pmatrix}4\\0\end{pmatrix}$	$\begin{pmatrix}3\\0\end{pmatrix}$
$\begin{bmatrix}1\\1\end{bmatrix}$	=	$\begin{pmatrix}1\\1\end{pmatrix}$	$\begin{pmatrix}2\\2\end{pmatrix}$	$\begin{pmatrix}4\\4\end{pmatrix}$	$\begin{pmatrix}3\\3\end{pmatrix}$
$\begin{bmatrix}1\\2\end{bmatrix}$	=	$\begin{pmatrix}1\\2\end{pmatrix}$	$\begin{pmatrix}2\\4\end{pmatrix}$	$\begin{pmatrix}4\\3\end{pmatrix}$	$\begin{pmatrix}3\\1\end{pmatrix}$
$\begin{bmatrix}1\\4\end{bmatrix}$	=	$\begin{pmatrix}1\\4\end{pmatrix}$	$\begin{pmatrix}2\\3\end{pmatrix}$	$\begin{pmatrix}4\\1\end{pmatrix}$	$\begin{pmatrix}3\\2\end{pmatrix}$
$\begin{bmatrix}1\\3\end{bmatrix}$	=	$\begin{pmatrix}1\\3\end{pmatrix}$	$\begin{pmatrix}2\\1\end{pmatrix}$	$\begin{pmatrix}4\\2\end{pmatrix}$	$\begin{pmatrix}3\\4\end{pmatrix}$

Each row in the table contains the set of points equivalent to the first element of that row, ordered by the group M. That is, we obtain the row by letting each element of M: m_1, m_2, m_4, m_3 act on the first point. For example, the row labelled by

$$\begin{bmatrix}1\\2\end{bmatrix}=m_1\begin{pmatrix}1\\2\end{pmatrix}=\begin{pmatrix}1\\2\end{pmatrix},\quad m_2\begin{pmatrix}1\\2\end{pmatrix}=\begin{pmatrix}2\\4\end{pmatrix},\quad m_4\begin{pmatrix}1\\2\end{pmatrix}=\begin{pmatrix}4\\3\end{pmatrix},$$
$$m_3\begin{pmatrix}1\\2\end{pmatrix}=\begin{pmatrix}3\\1\end{pmatrix}.$$

The entire table is created by repeatedly selecting elements not already included and forming the row corresponding to their equivalent points, until every point in $Z_5\times Z_5$ has been included. Finally note that only the first occurrence of an element in a row is listed. See, for example, the first row in Table 1.

Since every element in $Z_5\times Z_5$ appears in the table and each row consists of all the elements equivalent to the element in the first column, it follows that an asymmetric unit may be constructed by choosing one element from each row. By a slight abuse of notation we write

$$\begin{bmatrix}a\\b\end{bmatrix}$$

for the set of points equivalent under M to

$$\begin{pmatrix}a\\b\end{pmatrix}.$$

Since M is an ordered group, each of the sets

$$\begin{bmatrix}a\\b\end{bmatrix}$$

is ordered as in the one-dimensional case and if

$$\begin{pmatrix}a\\b\end{pmatrix}\neq\begin{pmatrix}0\\0\end{pmatrix},$$

we have

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} 2a \\ 2b \end{pmatrix}, \begin{pmatrix} 4a \\ 4b \end{pmatrix}, \begin{pmatrix} 3a \\ 3b \end{pmatrix}.$$

It remains to construct an ordered asymmetric unit to give an order to $Z_5 \times Z_5$ and then to show the resulting Fourier transform matrix.

Before doing this, let us introduce the notation

$$B_p\left(\begin{bmatrix} c \\ d \end{bmatrix}; \begin{bmatrix} a \\ b \end{bmatrix}\right) = B_p(c, d; a, b)$$

for the submatrix of the Fourier transform $F_p(5, 5)$ matrix that transforms the sample points corresponding to the ordered set of equivalent points

$$\begin{bmatrix} a \\ b \end{bmatrix}$$

to those of

$$\begin{bmatrix} c \\ d \end{bmatrix}.$$

We can calculate these blocks as follows: since the equivalent sets are ordered by $M = m_1, m_2, m_4, m_3$ we have, in general, for

$$\begin{pmatrix} a \\ b \end{pmatrix} \text{ and } \begin{pmatrix} c \\ d \end{pmatrix} \text{ both not } \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

if $\omega = e^{2\pi i/5}$ *and* $\eta = \omega^{ac+bd}$,

$$B_p(c, d; a, b) = \begin{pmatrix} \eta^1 & \eta^2 & \eta^4 & \eta^3 \\ \eta^2 & \eta^4 & \eta^3 & \eta^1 \\ \eta^4 & \eta^3 & \eta^1 & \eta^2 \\ \eta^3 & \eta^1 & \eta^2 & \eta^4 \end{pmatrix},$$

which is indeed skew-circulant. This is perhaps clearer if we write

$$\hat{B}_p(c, d; a, b) = \begin{pmatrix} 1 & 2 & 4 & 3 \\ 2 & 4 & 3 & 1 \\ 4 & 3 & 1 & 2 \\ 3 & 1 & 2 & 4 \end{pmatrix}.$$

The remaining cases are given by

$$\hat{B}_p(0, 0; a, b) = (0\,0\,0\,0), \begin{pmatrix} a \\ b \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix};$$

and

$$\hat{B}_p(c, d; 0, 0) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix};$$

and, finally,

$$\hat{B}_p(0, 0; 0, 0) = (0).$$

Thus no matter how we choose the asymmetric unit, we will end up with a block skew-circulant matrix. However, the space $Z_5 \times Z_5$ itself is ordered lexicographically not only in counting order but also as we constructed in the beginning of this section using M. Our choice of an asymmetric unit is fully defined by taking in each set of equivalent points the smallest as a representative, obtaining

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ 4 \end{bmatrix}, \begin{bmatrix} 1 \\ 3 \end{bmatrix}.$$

The full matrix of $\hat{F}_p$ is shown in Fig. 1.

Thus we have verified that the ordered multiplicative group $M \cong U(5)$ acting on $Z_5 \times Z_5$ enables us to order the elements of $Z_5 \times Z_5$ so that when the finite Fourier transform on $Z_5 \times Z_5$ is written as a matrix relative to this basis it breaks into blocks that are skew-circulant.

IV. A toy example

We will now present a toy example to show that Winograd-type algorithms offer the potential for computing finite Fourier transforms that respect crystallographic symmetries. Consider the two-dimensional space group $p3$ given in *International Tables for Crystallography* (1983) with equivalent positions given by

$$x, y; \bar{y}, x - y; \bar{x} + y, \bar{x}$$

and sample with five points in each dimension. The action of $p3$ on $Z_5 \times Z_5$ is given in matrix form by

$$\begin{pmatrix} a \\ b \end{pmatrix}; \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix}; \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix}$$

where all arithmetic operations are taken modulo 5. In particular, $-1 = 4$. We let

$$T = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

	0 0	0 0 0 0 1 2 4 3	1 2 4 3 0 0 0 0	1 2 4 3 1 2 4 3	1 2 4 3 2 4 3 1	1 2 4 3 4 3 1 2	1 2 4 3 3 1 2 4
(0,0)	0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
(0,1)	0	1 2 4 3	0 0 0 0	1 2 4 3	2 4 3 1	4 3 1 2	3 1 2 4
(0,2)	0	2 4 3 1	0 0 0 0	2 4 3 1	4 3 1 2	3 1 2 4	1 2 4 3
(0,4)	0	4 3 1 2	0 0 0 0	4 3 1 2	3 1 2 4	1 2 4 3	2 4 3 1
(0,3)	0	3 1 2 4	0 0 0 0	3 1 2 4	1 2 4 3	2 4 3 1	4 3 1 2
(1,0)	0	0 0 0 0	1 2 4 3	1 2 4 3	1 2 4 3	1 2 4 3	1 2 4 3
(2,0)	0	0 0 0 0	2 4 3 1	2 4 3 1	2 4 3 1	2 4 3 1	2 4 3 1
(4,0)	0	0 0 0 0	4 3 1 2	4 3 1 2	4 3 1 2	4 3 1 2	4 3 1 2
(3,0)	0	0 0 0 0	3 1 2 4	3 1 2 4	3 1 2 4	3 1 2 4	3 1 2 4
(1,1)	0	1 2 4 3	1 2 4 3	2 4 3 1	3 1 2 4	0 0 0 0	4 3 1 2
(2,2)	0	2 4 3 1	2 4 3 1	4 3 1 2	1 2 4 3	0 0 0 0	3 1 2 4
(4,4)	0	4 3 1 2	4 3 1 2	3 1 2 4	2 4 3 1	0 0 0 0	1 2 4 3
(3,3)	0	3 1 2 4	3 1 2 4	1 2 4 3	4 3 1 2	0 0 0 0	2 4 3 1
(1,2)	0	2 4 3 1	1 2 4 3	3 1 2 4	0 0 0 0	4 3 1 2	2 4 3 1
(2,4)	0	4 3 1 2	2 4 3 1	1 2 4 3	0 0 0 0	3 1 2 4	4 3 1 2
(4,3)	0	3 1 2 4	4 3 1 2	2 4 3 1	0 0 0 0	1 2 4 3	3 1 2 4
(3,1)	0	1 2 4 3	3 1 2 4	4 3 1 2	0 0 0 0	2 4 3 1	1 2 4 3
(1,4)	0	4 3 1 2	1 2 4 3	0 0 0 0	4 3 1 2	2 4 3 1	3 1 2 4
(2,3)	0	3 1 2 4	2 4 3 1	0 0 0 0	3 1 2 4	4 3 1 2	1 2 4 3
(4,1)	0	1 2 4 3	4 3 1 2	0 0 0 0	1 2 4 3	3 1 2 4	2 4 3 1
(3,2)	0	2 4 3 1	3 1 2 4	0 0 0 0	2 4 3 1	1 2 4 3	4 3 1 2
(1,3)	0	3 1 2 4	1 2 4 3	4 3 1 2	2 4 3 1	3 1 2 4	0 0 0 0
(2,1)	0	1 2 4 3	2 4 3 1	3 1 2 4	4 3 1 2	1 2 4 3	0 0 0 0
(4,2)	0	2 4 3 1	4 3 1 2	1 2 4 3	3 1 2 4	2 4 3 1	0 0 0 0
(3,4)	0	4 3 1 2	3 1 2 4	2 4 3 1	1 2 4 3	4 3 1 2	0 0 0 0

Fig. 1. The Fourier transform matrix $\hat{F}_p(5, 5)$ produced by the group M.

Table 2. *The action of the group CM on* $Z_5 \times Z_5$

	m_1	m_2	m_4	m_3
I, T, T^2	$\binom{0}{0}$			
I	$\binom{0}{1}$	$\binom{0}{2}$	$\binom{0}{4}$	$\binom{0}{3}$
T	$\binom{4}{4}$	$\binom{3}{3}$	$\binom{1}{1}$	$\binom{2}{2}$
T^2	$\binom{1}{0}$	$\binom{2}{0}$	$\binom{4}{0}$	$\binom{3}{0}$
I	$\binom{1}{2}$	$\binom{2}{4}$	$\binom{4}{3}$	$\binom{3}{1}$
T	$\binom{3}{4}$	$\binom{1}{3}$	$\binom{2}{1}$	$\binom{4}{2}$
T^2	$\binom{1}{4}$	$\binom{2}{3}$	$\binom{4}{1}$	$\binom{3}{2}$

Then

$$T^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad T^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I.$$

Hence $p3$ may be considered as the group of matrices I, T, T^2 operating on $Z_5 \times Z_5$.

In § III we introduced the multiplicative group M acting on $Z_5 \times Z_5$. Let CM be the group generated by all matrices in $p3$ and M. Because for all $u \in U(5)$,

$$Tm_u = m_u T,$$

we have that CM is an Abelian group of order 12. Explicitly every element of CM can be uniquely written as the product $m_u T^i$, where $u \in U(5)$ and $i = 0, 1, 2$. But the group CM acts on the set $Z_5 \times Z_5$ and so has equivalent points and asymmetric units. Table 2 describes the action of CM on $Z_5 \times Z_5$. In this table m_u, $u = 1, 2, 4, 3$ acts horizontally and I, T, T^2 acts vertically.

Notice that Table 2 implies that the set of points

$$\binom{0}{0}, \binom{0}{1}, \binom{0}{2}, \binom{0}{4}, \binom{0}{3}, \binom{1}{2}, \binom{2}{4}, \binom{4}{3}, \binom{3}{1}$$

is a $p3$-asymmetric unit that is carried onto itself by the action of M. In Fig. 2, we show the full $p3$ unit cell enclosing the space of sample points in $Z_5 \times Z_5$. The points have been labeled in the order we have developed and equivalent points have been given the same label. Points in the $p3$-asymmetric unit we have chosen are circled and the conventional asymmetric unit is outlined in the lower left-hand corner.

Fig. 2 has no obvious geometric interpretation; the order of the points has been chosen for arithmetic, not geometric reasons. We remark that the choice of the M-invariant $p3$-asymmetric unit on $Z_5 \times Z_5$ gives us yet another order of the space $Z_5 \times Z_5$ and hence another form of the Fourier-transform matrix. We keep our multiplicative order in the asymmetric unit, but for the other points we use the $p3$ symmetry to obtain their order. This gives us the following choice of the representatives and order of equivalence sets:

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 4 \\ 4 \end{bmatrix}, \begin{bmatrix} 3 \\ 4 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ and } \begin{bmatrix} 1 \\ 4 \end{bmatrix}.$$

The resulting Fourier transform matrix is shown (in exponent form) in Fig. 3. It is formed from 4×4 skew-circulant matrices since, as we showed in § III, the form of $B(c, d; a, b)$ does not depend on the choice of representatives,

$$\binom{a}{b} \text{ and } \binom{c}{d}.$$

But now for the payoff for all our efforts: since the input $X(c, d)$ is $p3$ symmetric, we need only compute the transform in the asymmetric unit. But by our choice of ordering in the sample space, the transform matrix reduces to a particularly nice form - blocks of skew-circulant matrices. To see this in general, we

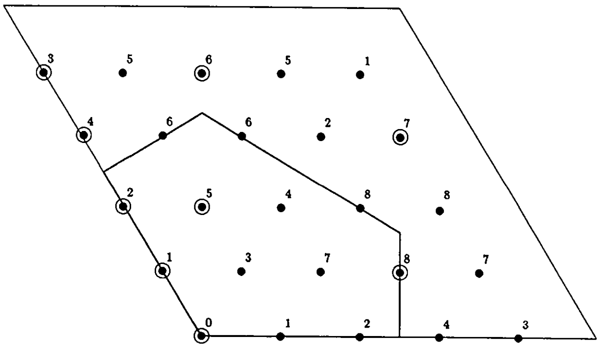

Fig. 2. The $p3$-asymmetric unit in $Z_5 \times Z_5$.

	0	0	0	0	0	1	2	4	3	4	3	1	2	3	1	2	4	1	2	4	3	1	2	4	3
	0	1	2	4	3	2	4	3	1	4	3	1	2	4	3	1	2	0	0	0	0	4	3	1	2
(0,0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
(0,1)	0	1	2	4	3	2	4	3	1	4	3	1	2	4	3	1	2	0	0	0	0	4	3	1	2
(0,2)	0	2	4	3	1	4	3	1	2	3	1	2	4	3	1	2	4	0	0	0	0	3	1	2	4
(0,4)	0	4	3	1	2	3	1	2	4	1	2	4	3	1	2	4	3	0	0	0	0	1	2	4	3
(0,3)	0	3	1	2	4	1	2	4	3	2	4	3	1	2	4	3	1	0	0	0	0	2	4	3	1
(1,2)	0	2	4	3	1	0	0	0	0	2	4	3	1	1	2	4	3	1	2	4	3	4	3	1	2
(2,4)	0	4	3	1	2	0	0	0	0	4	3	1	2	2	4	3	1	2	4	3	1	3	1	2	4
(4,3)	0	3	1	2	4	0	0	0	0	3	1	2	4	4	3	1	2	4	3	1	2	1	2	4	3
(3,1)	0	1	2	4	3	0	0	0	0	1	2	4	3	3	1	2	4	3	1	2	4	2	4	3	1
(4,4)	0	4	3	1	2	2	4	3	1	2	4	3	1	3	1	2	4	4	3	1	2	0	0	0	0
(3,3)	0	3	1	2	4	4	3	1	2	4	3	1	2	1	2	4	3	3	1	2	4	0	0	0	0
(1,1)	0	1	2	4	3	3	1	2	4	3	1	2	4	2	4	3	1	1	2	4	3	0	0	0	0
(2,2)	0	2	4	3	1	1	2	4	3	1	2	4	3	4	3	1	2	2	4	3	1	0	0	0	0
(3,4)	0	4	3	1	2	1	2	4	3	3	1	2	4	0	0	0	0	3	1	2	4	4	3	1	2
(1,3)	0	3	1	2	4	2	4	3	1	1	2	4	3	0	0	0	0	1	2	4	3	3	1	2	4
(2,1)	0	1	2	4	3	4	3	1	2	2	4	3	1	0	0	0	0	2	4	3	1	1	2	4	3
(4,2)	0	2	4	3	1	3	1	2	4	4	3	1	2	0	0	0	0	4	3	1	2	2	4	3	1
(1,0)	0	0	0	0	0	1	2	4	3	4	3	1	2	3	1	2	4	1	2	4	3	1	2	4	3
(2,0)	0	0	0	0	0	2	4	3	1	3	1	2	4	1	2	4	3	2	4	3	1	2	4	3	1
(4,0)	0	0	0	0	0	4	3	1	2	1	2	4	3	2	4	3	1	4	3	1	2	4	3	1	2
(3,0)	0	0	0	0	0	3	1	2	4	2	4	3	1	4	3	1	2	3	1	2	4	3	1	2	4
(1,4)	0	4	3	1	2	4	3	1	2	0	0	0	0	4	3	1	2	1	2	4	3	2	4	3	1
(2,3)	0	3	1	2	4	3	1	2	4	0	0	0	0	3	1	2	4	2	4	3	1	4	3	1	2
(4,1)	0	1	2	4	3	1	2	4	3	0	0	0	0	1	2	4	3	4	3	1	2	3	1	2	4
(3,2)	0	2	4	3	1	2	4	3	1	0	0	0	0	2	4	3	1	3	1	2	4	1	2	4	3

Fig. 3. The Fourier transform matrix $\hat{F}_p(5, 5)$ produced by the group M and $p3$.

choose the output at the set of M-equivalent points $[a, b]$,

$$\begin{aligned} Y(c, d) = B_p(c, d; 0, 0)X(0, 0) \\ + B_p(c, d; a, b)X(a, b) \\ + B_p(c, d; a', b')X(a', b') \\ + B_p(c, d; a'', b'')X(a'', b''), \end{aligned}$$

where

$$\begin{pmatrix} a' \\ b' \end{pmatrix} = T\begin{pmatrix} a \\ b \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} a'' \\ b'' \end{pmatrix} = T^2\begin{pmatrix} a \\ b \end{pmatrix}.$$

But $X(a, b) = X(a', b') = X(a'', b'')$ by $p3$ symmetry. Thus the matrix of the Fourier transform can be replaced by one in which the last four columns of blocks have been added to the first two, in pairs. Since the sum of skew-circulant blocks is again skew-circulant we obtain a matrix of such blocks. This reduces $F_p(5, 5)$ to a 25×9 matrix. The matrix can be further reduced by taking advantage of the $p3$ symmetry on output. A careful observation of the matrix in Fig. 3 shows that the Fourier transform maps the asymmetric unit of $p3$ to an asymmetric unit up to permutation. That is, after adding the columns as suggested, every output outside the asymmetric unit is equal to an output in the asymmetric unit. For example,

$$\begin{aligned} Y(1, 0) = 1 + 2(1 + \omega + \omega^4) + 2(1 + \omega^2 + \omega^3) \\ + (2\omega + \omega^3) + (\omega + 2\omega^2) + (2\omega^2 + \omega^4) \\ + (2\omega^3 + \omega^4) = Y(0, 4). \end{aligned}$$

It can be shown that this phenomenon occurs in general. With the help of these observations we have reduced, using $p3$ symmetry, a 25×25 matrix to a 9×9 matrix whose action on a vector can still be efficiently computed. We show the resulting matrix in Fig. 4.

This completes our study of small examples that illustrate our construction. In the next sections we turn our attention to the problem of structuring Fourier transforms on $60 \times 60 \times 60$ points that respect $P3$ symmetry. We will work this out in §§ V and VI. In § V we will study the Fourier transform on 60 points and introduce the multiplicative group $U(60)$ that we use instead of $U(5)$. In § VI we will see how our work on $Z_5 \times Z_5$ generalizes to a non-toy example.

V. The finite Fourier transform on 60 points

Our first task is to introduce a multiplicative group that plays the role of $U(5)$ for the finite Fourier transform on five points. Consider Z_{60} and all $a \in Z_{60}$ such that there exists a b with $a \times b = 1$ in Z_{60}. This set, denoted $U(60)$, is a group under multiplication in Z_{60} and is called the group of units. It can be shown that $U(60)$ consists of those elements in Z_{60} that are not divisible by 2, 3 or 5. Explicitly, $U(60)$ consists of

$$1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59.$$

In analogy with $U(5)$, this order is not the order we need to structure the finite Fourier transform matrix so as to maximize the number of tensor skew-circulant matrices. In the case of $U(60)$ we need three elements, 31, 41, and 37 to play the role of the multiplicative generator 2 in ordering $U(5)$. It is not obvious, but can easily be checked with a small calculation that (when all arithmetic is done modulo 60): (1) $31^2 = 1$; (2) $41^2 = 1$; (3) $37, 37^2 = 49, 37^3 = 13$, and $37^4 = 1$ are all distinct elements of Z_{60}; and (4) every element of $U(60)$ can be written uniquely as $(31)^\alpha(41)^\beta(37)^\gamma$ with $0 \le \alpha, \beta \le 1$ and $0 \le \gamma \le 3$. It

	$\binom{0}{0}$	$\binom{0}{1}$	$\binom{0}{2}$	$\binom{0}{4}$	$\binom{0}{4}$	$\binom{1}{2}$	$\binom{2}{4}$	$\binom{4}{3}$	$\binom{3}{1}$
(0,0)	1	3	3	3	3	3	3	3	3
(0,1)	1	$1+\omega+\omega^4$	$1+\omega^2+\omega^3$	$1+\omega+\omega^4$	$1+\omega^2+\omega^3$	$\omega^2+2\omega^4$	$2\omega^3+\omega^4$	$2\omega+\omega^3$	$\omega+2\omega^2$
(0,2)	1	$1+\omega^2+\omega^3$	$1+\omega+\omega^4$	$1+\omega^2+\omega^3$	$1+\omega+\omega^4$	$2\omega^3+\omega^4$	$2\omega+\omega^3$	$\omega+2\omega^2$	$\omega^2+2\omega^4$
(0,4)	1	$1+\omega+\omega^4$	$1+\omega^2+\omega^3$	$1+\omega+\omega^4$	$1+\omega^2+\omega^3$	$2\omega+\omega^3$	$\omega+2\omega^2$	$\omega^2+2\omega^4$	$2\omega^3+\omega^4$
(0,3)	1	$1+\omega^2+\omega^3$	$1+\omega+\omega^4$	$1+\omega^2+\omega^3$	$1+\omega+\omega^4$	$\omega+2\omega^2$	$\omega^2+2\omega^4$	$2\omega^3+\omega^4$	$2\omega+\omega^3$
(1,2)	1	$\omega+2\omega^2$	$\omega^2+2\omega^4$	$2\omega^3+\omega^4$	$2\omega+\omega^3$	$1+\omega+\omega^4$	$1+\omega^2+\omega^3$	$1+\omega+\omega^4$	$1+\omega^2+\omega^3$
(2,4)	1	$\omega^2+2\omega^4$	$2\omega^3+\omega^4$	$2\omega+\omega^3$	$\omega+2\omega^2$	$1+\omega^2+\omega^3$	$1+\omega+\omega^4$	$1+\omega^2+\omega^3$	$1+\omega+\omega^4$
(4,3)	1	$2\omega^3+\omega^4$	$2\omega+\omega^3$	$\omega+2\omega^2$	$\omega^2+2\omega^4$	$1+\omega+\omega^4$	$1+\omega^2+\omega^3$	$1+\omega+\omega^4$	$1+\omega^2+\omega^3$
(3,1)	1	$2\omega+\omega^3$	$\omega+2\omega^2$	$\omega^2+2\omega^4$	$2\omega^3+\omega^4$	$1+\omega^2+\omega^3$	$1+\omega+\omega^4$	$1+\omega^2+\omega^3$	$1+\omega+\omega^4$

Fig. 4. The Fourier transform matrix $F_p(5, 5)$ reduced to a $p3$-asymmetric unit.

follows from (4) that $U(60)$ is an Abelian group under multiplication with three generators.

Just as is the case with $U(5)$, we can use these generators to order $U(60)$ appropriately. Consider the correspondence

$$(\alpha, \beta, \gamma) \mapsto (31)^{\alpha}(41)^{\beta}(37)^{\gamma} \in U(60) \subset Z_{60}$$

with $0 \le \alpha$, $\beta \le 1$, $0 \le \gamma \le 3$. The triples (α, β, γ) are naturally ordered by the multi-radix counting order, namely

$$(0, 0, 0), (0, 0, 1), (0, 0, 2), (0, 0, 3), (0, 1, 0),$$
$$(0, 1, 1), (0, 1, 2), (0, 1, 3), (1, 0, 0), (1, 0, 1),$$
$$(1, 0, 2), (1, 0, 3), (1, 1, 0), (1, 1, 1), (1, 1, 2),$$
$$(1, 1, 3).$$

It is this order that we need in $U(60)$; computing the corresponding elements we have the order

$$1, 37, 49, 13, 41, 17, 29, 53, 31, 7, 19, 43, 11, 47, 59, 23.$$

We will now discuss equivalent points and asymmetric units for $U(60)$ acting on Z_{60} by multiplication in Z_{60}. In this case equivalent points may have 1, 2, 4, 8 or 16 elements, and different subgroups may be said to act on equivalent points. Let us introduce some notation for subgroups of $U(60)$:

$\langle 0, 0, 0\rangle$ denotes the subgroup 1,
$\langle 0, 1, 0\rangle$ the subgroup 1, 41,
$\langle 0, 0, 1\rangle$ the subgroup 1, 37, 49, 13,
$\langle 0, 1, 1\rangle$ the subgroup 1, 37, 49, 13, 41, 17, 29, 53,
$\langle 1, 0, 0\rangle$ the subgroup 1, 31,
$\langle 1, 1, 0\rangle$ the subgroup 1, 41, 31, 11,
$\langle 1, 0, 1\rangle$ the subgroup 1, 37, 49, 13, 31, 7, 19, 43,
$\langle 1, 1, 1\rangle$ $U(60)$.

Each point $a \in Z_{60}$ has one of these groups associated with it, the group of the point a, denoted by $G(a)$, carrying it effectively onto each of its equivalent points. For example, $0 \in Z_{60}$ has no other equivalent points and thus $G(0) = \langle 0, 0, 0\rangle$. Similarly, the point 1 is equivalent to all of $U(60)$ and thus $G(1) = \langle 1, 1, 1\rangle$. An intermediate case is $25 \in Z_{60}$ which is equivalent under multiplication by $U(60)$ to 5, 55, and 35. One verifies that $G(25) = \langle 1, 1, 0\rangle$. We remark that groups of equivalent points are the same, and thus $G(25) = G(5) = G(55) = G(35)$. The group of a point orders its equivalent points by using the order in $U(60)$. For example, if we choose 25 as the representative of the points 25, 5, 55, and 35, then we can order these points as follows: since $G(25) = \langle 1, 1, 0\rangle = 1, 41, 31, 11$ [this is the order in $U(60)$], we have the result that $1 \times 25 = 25$, $41 \times 25 = 5$, $31 \times 25 = 55$, $11 \times 25 = 35$ is the correct order in $[25] = 25, 5, 55, 35$, the set of equivalent points of 25. This method gives us a way to order Z_{60} and thus to produce a finite Fourier matrix.

By constructing a table as in § III we choose an asymmetric unit. It can be verified that 0, 1, 6, 10, 16, 21, 25, 30, 36, 40, 45, 46 is one. Now we order these elements by using the order of their associated groups.

$$0,\ G(0) = \langle 0, 0, 0\rangle$$
$$30,\ G(30) = \langle 0, 0, 0\rangle$$
$$40,\ G(40) = \langle 0, 1, 0\rangle$$
$$10,\ G(10) = \langle 0, 1, 0\rangle$$
$$36,\ G(36) = \langle 0, 0, 1\rangle$$
$$6,\ G(6) = \langle 0, 0, 1\rangle$$
$$16,\ G(16) = \langle 0, 1, 1\rangle$$
$$46,\ G(46) = \langle 0, 1, 1\rangle$$
$$45,\ G(45) = \langle 1, 0, 0\rangle$$
$$25,\ G(25) = \langle 1, 1, 0\rangle$$
$$21,\ G(21) = \langle 1, 0, 1\rangle$$
$$1,\ G(1) = \langle 1, 1, 1\rangle.$$

Notice that we have now completely ordered Z_{60}. In fact we just list the classes of equivalent points:

$$Z_{60} = [0], [30], [40], [10], [36], [6], [16], [46], [45], [25], [21], [1].$$

Now, let $B(b;\, a)$, as in the toy example, denote the block in the Fourier transform matrix corresponding to that part of the transform which takes the points in $[a]$ into those in $[b]$. We shall see that all $B(b;\, a)$ are tensor skew-circulant matrices or repetitions of tensor skew-circulant matrices.

We note that if $|G(a)|$ denotes the order of the group $G(a)$ then the number of points in $[a]$ is $|G(a)|$ since $G(a)$ acts effectively. Thus, $B(b;\, a)$ is a $|G(b)| \times |G(a)|$ rectangular matrix. Furthermore, it can be verified that $B(a;\, b)$ is the transpose of $B(b;\, a)$.

In Fig. 5 we show the finite Fourier transform matrix on 60 points for the ordering just described. Actually, we show only the exponents of $\omega = e^{2\pi i/60}$, the 60th roots of unity. More precisely, if $F(60) = (\omega^{ij})0 \le i, j \le 59$ describes the finite Fourier transform matrix relative to the standard ordering then let $\hat{F}(60) = (ij)$ be the matrix of exponents. Then if we reorder the indices $0, \ldots, 59$ into $p(0), \ldots, p(59)$ we have $F_p(60) = (\omega^{p(i)p(j)})$ and $\hat{F}_p(60) = (p(i)p(j))$ where all arithmetic is done modulo 60. Thus Fig. 5 is the matrix $\hat{F}_p(60)$, with $p(*)$ the ordering induced by the group $U(60)$.

We shall be content in this discussion to state that $\hat{F}_p(60)$ has the desired property that it consists of blocks $\hat{B}_p(a;b)$ that are tensor skew-circulant, and to discuss several examples. First notice that Fig. 5 has been labeled in the first row and column by the elements in their new order. Thus the element in the upper left-hand corner is $0\times 0=0$, the lower left-hand corner is $23\times 0=0$, the upper right $0\times 23=0$ and the lower right $23\times 23=49$.

Furthermore, the sets of equivalent points have been separated by additional space so that it is easier to see that, for example, the element 25 is a member of the asymmetric unit and its equivalence set $[25]=25, 5, 55, 35$. If we look in the column labeled 25 and the row labeled 25 we see the block

$$\hat{B}_p(25;25)=\begin{pmatrix}25 & 5 & 55 & 35\\ 5 & 25 & 35 & 55\\ 55 & 35 & 25 & 5\\ 35 & 55 & 5 & 25\end{pmatrix}.$$

It is clear that this is tensor skew-circulant; in fact, we have

$$\hat{B}_p(25;25)=\begin{pmatrix}25 & 55\\ 55 & 25\end{pmatrix}\otimes\begin{pmatrix}25 & 5\\ 5 & 25\end{pmatrix}.$$

Another case on the diagonal is the block $\hat{B}_p(21;21)$ for the set of equivalent points $[21]=25, 57, 9, 33, 51, 27, 39, 3$. We have

$$\hat{B}_p(21;21)=\begin{pmatrix}21 & 57 & 9 & 33 & 51 & 27 & 39 & 3\\ 57 & 9 & 33 & 21 & 27 & 39 & 3 & 51\\ 9 & 33 & 21 & 57 & 39 & 3 & 51 & 27\\ 33 & 21 & 57 & 9 & 3 & 51 & 27 & 39\\ 51 & 27 & 39 & 3 & 21 & 57 & 9 & 33\\ 27 & 39 & 3 & 51 & 57 & 9 & 33 & 21\\ 39 & 3 & 51 & 27 & 9 & 33 & 21 & 57\\ 3 & 51 & 27 & 39 & 33 & 21 & 57 & 9\end{pmatrix}$$

$$\hat{B}_p(21;21)=\begin{pmatrix}21 & 51\\ 51 & 21\end{pmatrix}\otimes\begin{pmatrix}21 & 57 & 9 & 33\\ 57 & 9 & 33 & 21\\ 9 & 33 & 21 & 57\\ 33 & 21 & 57 & 9\end{pmatrix}.$$

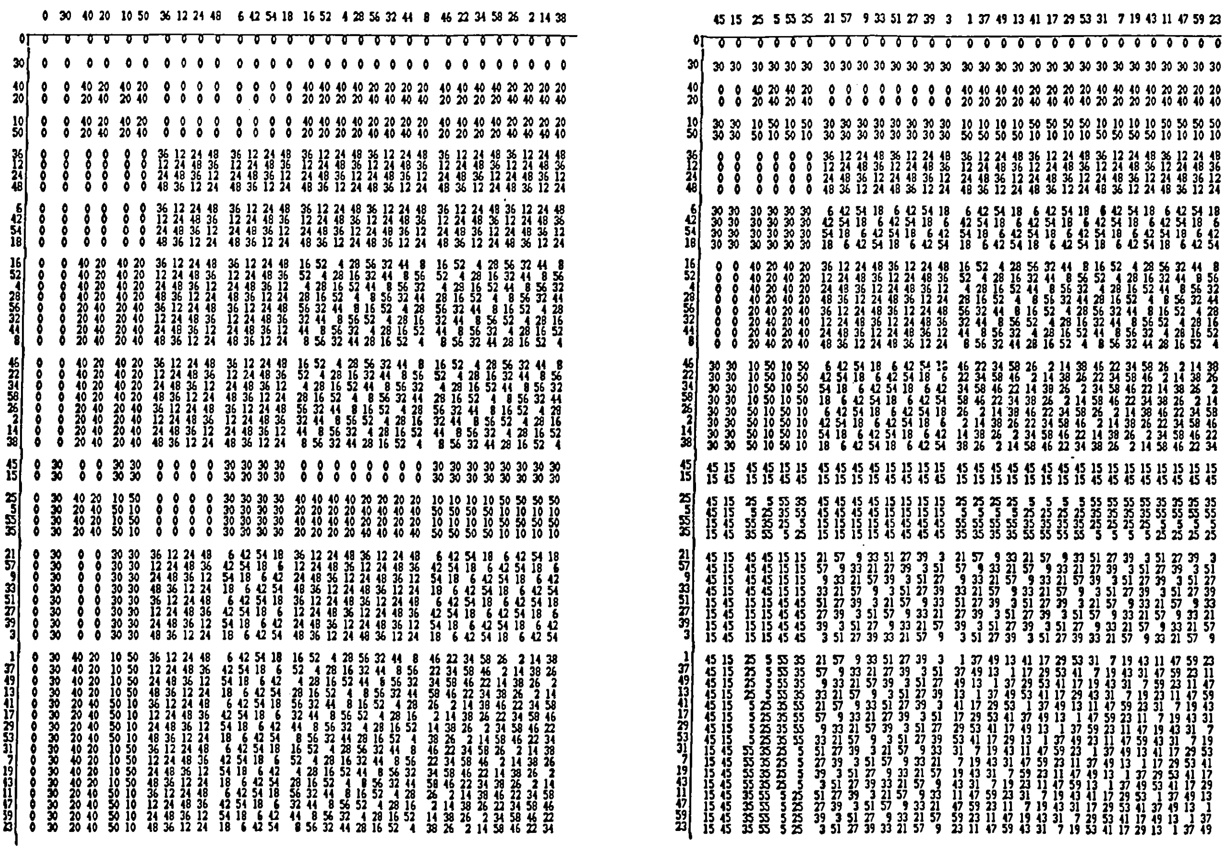

Fig. 5. The Fourier transform matrix $\hat{F}_p(60)$ produced by the group M.

And finally, on the diagonal, the set of points equivalent to 1,

$U(60)=[1]=1, 37, 49, 13, 31, 7, 19, 43, 41, 17, 29, 53, 11, 47, 59, 23$

$$\hat{B}_p(1;1)=\begin{pmatrix}1 & 31\\ 31 & 1\end{pmatrix}\otimes\begin{pmatrix}1 & 41\\ 41 & 1\end{pmatrix}\otimes\begin{pmatrix}1 & 37 & 49 & 13\\ 37 & 49 & 13 & 1\\ 49 & 13 & 1 & 37\\ 13 & 1 & 37 & 49\end{pmatrix}.$$

The off-diagonal blocks are also made up of repetitions of tensor skew-circulant matrices. This repetition is the result of the fact that the groups of the points are not the same and a precise prescription of this phenomenon is beyond the scope of this paper. Suffice it to say that the patterns discernible by the eye in Fig. 5 are perfectly regular and can be coded in a program to compute the Fourier transform efficiently on 60 points.

VI. Symmetry on $60\times60\times60$ points.

Until now everything in this paper has been constructive and explicit. Since $60\times60\times60=216\,000$, to list our constructions explicitly for a problem of this size is impossible. Even though our methods will reduce this problem by the threefold symmetry of $P3$, we still must deal with approximately $216\,000/3=72\,000$ points. We will therefore adopt an existential discussion, pointing out that certain objects exist, and continue to state their properties.

In the actual computer program for the calculation, each of these objects has to be constructed by an algorithm. Since this requires considerable technical discussion, we have delayed it to a second paper.

Putting together the suggestive ideas of the preceding sections, for the case of 60 points in three dimensions, we must investigate the ordering induced by $U(60)$ on $Z_{60}\times Z_{60}\times Z_{60}$, and the effect of the symmetry group $P3$ on that ordering.

We let $P3$ be the three-dimensional space group given in *International Tables for Crystallography* (1983) with equivalent positions given by

$$x, y, z;\ \bar{y}, x-y, z;\ y-x, \bar{x}, z.$$

$P3$ can be written as the matrix group $\{1, T, T^2\}$ acting on

$$\begin{pmatrix}a\\ b\\ c\end{pmatrix}$$

in $Z_{60}\times Z_{60}\times Z_{60}$, where

$$T=\begin{pmatrix}0 & -1 & 0\\ 1 & -1 & 0\\ 0 & 0 & 1\end{pmatrix}.$$

Furthermore, we must extend $U(60)$ to act in 3-space; so for $u\in U(60)$ we consider u acting as

$$m_u=\begin{pmatrix}u & 0 & 0\\ 0 & u & 0\\ 0 & 1 & 1\end{pmatrix}.$$

The set m_u such that $u\in U(60)=M$ is now an ordered group as in § III. Then $Tm_u=m_uT$ for all $u\in U(60)$. Let CM be the Abelian group m_u, Tm_u, T^2m_u of $3\times16=48$ elements. As a group acting in $Z_{60}\times Z_{60}\times Z_{60}$, CM has an asymmetric unit. This asymmetric unit can be enlarged to a $P3$-asymmetric unit A which is M invariant. The fact that A is M invariant means that when we restrict the finite Fourier transform matrix to A it will be made up of large tensor skew-circulant blocks.

A can be chosen so that it is the disjoint union of A_0 and A_1, $A=A_0\vee A_1$, where A_0 are the fixed points under $P3$ and A_1 are those points moved by $P3$. Further, A_0 and A_1 are M invariant, *i.e.* $M(A_0)=A_0$ and $M(A_1)=A_1$.

Now we can view M acting as a group on A_0 and A_1 and as such it has asymmetric units in each space. But this action has been described in § V; *i.e.* each asymmetric unit is described by a certain number of points and their groups. Let us write $A_{0,\langle\alpha,\beta,\gamma\rangle}$ for those points whose groups are $\langle\alpha,\beta,\gamma\rangle$ in an asymmetric unit for M in A_0, and, similarly, $A_{1,\langle\alpha,\beta,\gamma\rangle}$ in A_1. Now, as we saw in § V, M orders Z_{60}. Using this order, we can order $Z_{60}\times Z_{60}\times Z_{60}$ lexicographically. As subsets of $Z_{60}\times Z_{60}\times Z_{60}$, $A_{0,\langle\alpha,\beta,\gamma\rangle}$ and $A_{1,\langle\alpha,\beta,\gamma\rangle}$ are ordered. And, as before, we order the subgroups $\langle 0,0,0\rangle$, $\langle 0,1,0\rangle$, $\langle 0,0,1\rangle,\ldots,\langle 1,1,1\rangle$.

Since $Z_{60}\times Z_{60}\times Z_{60}=A_0\vee A_1\vee T(A_1)\vee T^2(A_1)$, just as in § IV, the whole space is ordered if we agree that $A_0<A_1<T(A_1)<T^2(A_1)$. With this order we have defined the finite Fourier transform matrix on $60\times60\times60$ points. It is clear that it will restrict to a transform of $A_0\vee A_1$ to $A_0\vee A_1$ that respects $P3$ symmetry and that the resulting blocks will be the sums of three blocks corresponding to I, T, T^2.

It remains only to sketch a proof that each of the blocks is tensor skew-circulant or a repetition of tensor skew-circulant matrices. As in § V, we shall only discuss blocks near the diagonal, but as in the case of $F_p(60)$, the other blocks, while more difficult to discuss (we need to introduce a lot of new notation), are in fact easy to compute because of the repetitions in their structure.

Let us extend our notation for blocks: if

$$\begin{bmatrix} a \\ b \\ c \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

are equivalence classes in A_0 or A_1 under the action of M, let $B_p(x, y, z; a, b, c)$ be the block in the finite Fourier transform matrix $F_p(60\times 60\times 60)$ corresponding to that part of the transform which carries the set of points

$$\begin{bmatrix} a \\ b \\ c \end{bmatrix} \quad \text{to} \quad \begin{bmatrix} x \\ y \\ z \end{bmatrix}.$$

Let $\hat{B}_p(x, y, z; a, b, c)$ be the corresponding block of exponents.

Our condition that $B_p(x, y, z; a, b, c)$ be near the diagonal is the requirement that the sample points have the same group, $G(a, b, c) = G(x, y, z)$. Suppose $G(a, b, c) = 1, g_1, \ldots, g_n$; then by our ordering we have

$$\begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{pmatrix} a \\ b \\ c \end{pmatrix}, g_1\begin{pmatrix} a \\ b \\ c \end{pmatrix}, \ldots, g_n\begin{pmatrix} a \\ b \\ c \end{pmatrix},$$

and

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}, g_1\begin{pmatrix} x \\ y \\ z \end{pmatrix}, \ldots, g_n\begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

With this notation we can explictly calculate the blocks $\hat{B}_p(x, y, z; a, b, c)$. We have

Now by our construction of the group $\langle\alpha, \beta, \gamma\rangle = G(a, b, c)$ the resulting matrix is tensor skew circulant. We shall be content to give three example calculations. For $\langle\alpha, \beta, \gamma\rangle = \langle 0, 1, 0\rangle = 1,\ 41$ we have

$$G = \begin{pmatrix} 1 & 41 \\ 41.41 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 41 \\ 41 & 1 \end{pmatrix},$$

(where all arithmetic is done modulo 60); for $\langle 1, 1, 0\rangle = 1, 41, 31, 11$,

$$\begin{pmatrix} 1 & 41 & 31 & 11 \\ 41 & 41.41 & 31.41 & 11.41 \\ 31 & 41.31 & 31.31 & 11.31 \\ 11 & 41.11 & 31.11 & 11.11 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 41 & 31 & 11 \\ 41 & 1 & 11 & 31 \\ 31 & 11 & 1 & 41 \\ 11 & 31 & 41 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 31 \\ 31 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 41 \\ 41 & 1 \end{pmatrix}.$$

And finally for $\langle 1, 1, 1\rangle = U(60)$ it can be verified that the matrix is given by

$$\begin{pmatrix} 1 & 31 \\ 31 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 41 \\ 41 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 37 & 49 & 13 \\ 37 & 49 & 13 & 1 \\ 49 & 13 & 1 & 37 \\ 13 & 1 & 37 & 49 \end{pmatrix}.$$

Let us summarize what we have achieved. For the case of the three-dimensional finite Fourier transform on $60\times 60\times 60$ points subject to the threefold crystal symmetry $P3$, we have introduced an order on the

$$\hat{B}_p(x, y, z; a, b, c) = \begin{array}{c|cccc} & \begin{pmatrix} a \\ b \\ c \end{pmatrix} & g_1\begin{pmatrix} a \\ b \\ c \end{pmatrix} & \cdots & g_n\begin{pmatrix} a \\ b \\ c \end{pmatrix} \\ \hline \begin{pmatrix} x \\ y \\ z \end{pmatrix} & ax+by+cz & g_1ax+g_1by+g_1cz & \cdots & g_nax+g_nby+g_ncz \\ \begin{pmatrix} g_1x \\ g_1y \\ g_1z \end{pmatrix} & ag_1x+bg_1y+cg_1z & g_1ag_1x+g_1bg_1y+g_1cg_1z & \cdots & g_nag_1x+g_nbg_1y+g_ncg_1z \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \begin{pmatrix} g_nx \\ g_ny \\ g_nz \end{pmatrix} & ag_nx+bg_ny+cg_nz & g_1ag_nx+g_1bg_ny+g_1cg_nz & \cdots & g_nag_nx+g_nbg_ny+g_ncg_nz \end{array}$$

$$= (ax+by+cz)\begin{pmatrix} 1 & g_1 & \cdots & g_n \\ g_1 & g_1g_1 & \cdots & g_1g_n \\ \vdots & \vdots & \vdots & \vdots \\ g_n & g_1g_n & \cdots & g_ng_n \end{pmatrix} = (ax+by+cz)G.$$

points, using a multiplicative group M, that produces a matrix of a particularly nice form. Further, it restricts to an asymmetric unit for $P3$ on the space reducing the size of the matrix by 1/9. Furthermore, the resulting matrix has the same tensor skew-circulant form as the big matrix and so can be used to compute the transform using the same efficient algorithms as the original transform.

As we have suggested earlier, the technical details in the resulting algorithm will be the subject of another paper where the construction of the asymmetric unit and all the blocks will be shown.

Summary

The finite Fourier transform on N data points is simply the evaluation of an $N \times N$ matrix times an N-vector to produce an N-vector result. The straightforward method of matrix multiplication requires a number of operations proportional to N^2. In terms of computer programming, the time required to compute the result, say $T_S(N)$, would quadruple if the input size were doubled. We can express this by writing $T_S(N) = CN^2$ where C is a constant depending, amongst many things, primarily on the machine on which the program is run and the coding of the program. Typical values of C are in the range of 40 μs for the VAX-11/785 to 400 ns for the CRAY X-MP. So even for moderate-size problems, say $N = 100$ to 10 000, the range of observed times is significant; measured in seconds to hours.

The remarkable aspect of the Fourier transform is that there exist 'fast' or 'efficient' methods which do the same evaluation in a time proportional to $N \log N$, or $T_F(N) = KN \log N$ where K is another constant, approximately the same as C. This means that using 'fast' methods reduces time costs for real problems by several orders of magnitude.

For problems in crystallography, the finite Fourier transform is run many times for the same space group on the same number of points. This problem has led to efforts to use the symmetry of the data to reduce N by the order of the group to save time and space in calculating the result. For groups built from $P2$ Ten Eyck (1973) was able to achieve both. Bantz & Zwick (1974) were able to use symmetry to reduce memory requirements for nearly all space groups.

The advantage of the approach presented in this paper is that we can use symmetry to reduce the data and still use an efficient $N \log N$ evaluation method. Although much work needs to be done to develop algorithms for all the space groups, the general method presented here shows that such algorithms exist. In principle, each group and each grid size leads to a different program. However, the methods presented in this paper enable us to generate these programs automatically. Moreover, by the very nature of the algorithms developed they can be naturally partitioned to calculate structures larger than available high-speed memory.

References

Bantz, D. A. & Zwick, M. (1974). *Acta Cryst.* A**30**, 257-260.
International Tables for Crystallography (1983). Vol. A, pp. 94, 480. Dordrecht: Reidel. (Present distributor Kluwer Academic Publishers, Dordrecht.)
Rader, C. M. (1968). *Proc. IEEE*, **5**, 1107-1108.
Ten Eyck, L. F. (1973). *Acta Cryst.* A**29**, 183-191.
Winograd, S. (1978). *Math. Comput.* **32**, 175-199.

Acta Cryst. (1988). A**44**, 478-481

Increasing the Size of Search Fragments for use in Patterson Method Calculations – the Partial-Fragment Rotation Function

By C. C. Wilson

Neutron Division, Rutherford Appleton Laboratory, Chilton, Didcot, Oxon OX11 0QX, England

(*Received 27 October* 1987; *accepted* 15 *February* 1988)

Abstract

A method is described of expanding a molecular fragment for use in Patterson search procedures by the rotation of part of a model about a bond direction with respect to a fixed fragment, allowing the removal of an important degree of freedom in the model. The function has been incorporated into a computer program and it has been found possible to orient very small partial fragments in this way. The consequent expansion of a search model should assist in structural solution.

Introduction

The basis of Patterson search techniques lies in the provision of a reasonable model fragment for comparison with the observed data. In the reciprocal-

0108-7673/88/040478-04$03.00