International Tables for Crystallography (2006). Vol. B, Section 1.3.4.3.4.3, pp. 76–79.

The equivalence of the two transposition formulae up to the intervening twiddle factors is readily established, using the relation

$$\mathbf{h}_2 \cdot [\mathbf{N}_2^{-1} \boldsymbol{\mu}_2(g, \mathbf{m}_1)] = \boldsymbol{\eta}_1(g, \mathbf{h}_2) \cdot (\mathbf{N}_1^{-1} \mathbf{m}_1) \bmod 1$$

which is itself a straightforward consequence of the identity

$$\mathbf{h} \cdot [\mathbf{N}^{-1} S_g(\mathbf{m})] = \mathbf{h} \cdot \mathbf{t}_g + (\mathbf{R}_g^T \mathbf{h}) \cdot (\mathbf{N}^{-1} \mathbf{m}).$$

To complete the characterization of the effect of symmetry on the Cooley–Tukey factorization, and of the economy of computation it allows, it remains to consider the possibility that some values of $\mathbf{m}_1$ may be invariant under some transformations $g \in G$ under the action $\mathbf{m}_1 \longmapsto S_g^{(1)}(\mathbf{m}_1)$.

Suppose that $\mathbf{m}_1$ has a non-trivial isotropy subgroup $G_{\mathbf{m}_1}$, and let $g \in G_{\mathbf{m}_1}$. Then each subarray $Y_{\mathbf{m}_1}$ defined by

$$Y_{\mathbf{m}_1}(\mathbf{m}_2) = Y(\mathbf{m}_1, \mathbf{m}_2) = \rho(\mathbf{m}_1 + \mathbf{N}_1 \mathbf{m}_2)$$

satisfies the identity

$$\begin{aligned} Y_{\mathbf{m}_1}(\mathbf{m}_2) &= Y_{S_g^{(1)}(\mathbf{m}_1)}[S_g^{(2)}(\mathbf{m}_2) + \boldsymbol{\mu}_2(g, \mathbf{m}_1)] \\ &= Y_{\mathbf{m}_1}[S_g^{(2)}(\mathbf{m}_2) + \boldsymbol{\mu}_2(g, \mathbf{m}_1)] \end{aligned}$$

so that the data for the transform on $\mathbf{m}_2$ have residual symmetry properties. In this case the identity satisfied by $\boldsymbol{\mu}_2$ simplifies to

$$\boldsymbol{\mu}_2(gg', \mathbf{m}_1) = S_g^{(2)}[\boldsymbol{\mu}_2(g', \mathbf{m}_1)] + \boldsymbol{\mu}_2(g, \mathbf{m}_1) \bmod \mathbf{N}_2\mathbb{Z}^3,$$

which shows that the mapping $g \longmapsto \boldsymbol{\mu}_2(g, \mathbf{m}_1)$ satisfies the Frobenius congruences (Section 1.3.4.2.2.3). Thus the internal symmetry of subarray $Y_{\mathbf{m}_1}$ with respect to the action of G on $\mathbf{m}_2$ is given by $G_{\mathbf{m}_1}$ acting on $\mathbb{Z}^3/\mathbf{N}_2\mathbb{Z}^3$ *via*

$$\mathbf{m}_2 \longmapsto S_g^{(2)}(\mathbf{m}_2) + \boldsymbol{\mu}_2(g, \mathbf{m}_1) \bmod \mathbf{N}_2\mathbb{Z}^3.$$

The transform on $\mathbf{m}_2$ needs only be performed for one out of $[G : G_{\mathbf{m}_1}]$ distinct arrays $Y_{\mathbf{m}_1}$ (results for the others being obtainable by the transposition formula), and this transforms is $G_{\mathbf{m}_1}$-symmetric. In other words, the following cases occur:

(i)	$G_{\mathbf{m}_1} = \{e\}$	maximum saving in computation (by $\lvert G\rvert$); $\mathbf{m}_2$-transform has no symmetry.
(ii)	$G_{\mathbf{m}_1} = G' < G$	saving in computation by a factor of $[G : G']$; $\mathbf{m}_2$-transform is G'-symmetric.
(iii)	$G_{\mathbf{m}_1} = G$	no saving in computation; $\mathbf{m}_2$-transform is G-symmetric.

The symmetry properties of the $\mathbf{m}_2$-transform may themselves be exploited in a similar way if $\mathbf{N}_2$ can be factored as a product of smaller decimation matrices; otherwise, an appropriate symmetrized DFT routine may be provided, using for instance the idea of 'multiplexing/demultiplexing' (Section 1.3.4.3.5). We thus have a recursive *descent procedure*, in which the deeper stages of the recursion deal with transforms on *fewer points*, or of *lower symmetry* (usually both).

The same analysis applies to the $\mathbf{h}_1$-transforms on the subarrays $Z_{\mathbf{h}_2}^*$, and leads to a similar descent procedure.

In conclusion, crystallographic symmetry can be fully exploited to reduce the amount of computation to the minimum required to obtain the unique results from the unique data. No such analysis was so far available in cases where the asymmetric units in real and reciprocal space are not parallelepipeds. An example of this procedure will be given in Section 1.3.4.3.6.5.

1.3.4.3.4.2. *Multidimensional Good factorization*

This procedure was described in Section 1.3.3.3.2.2. The main difference with the Cooley–Tukey factorization is that if $\mathbf{N} = \mathbf{N}_1\mathbf{N}_2 \ldots \mathbf{N}_{d-1}\mathbf{N}_d$, where the different factors are pairwise coprime, then the Chinese remainder theorem reindexing makes $\mathbb{Z}^3/\mathbf{N}\mathbb{Z}^3$ isomorphic to a direct sum.

$$\mathbb{Z}^3/\mathbf{N}\mathbb{Z}^3 \cong (\mathbb{Z}^3/\mathbf{N}_1\mathbb{Z}^3) \oplus \ldots \oplus (\mathbb{Z}^3/\mathbf{N}_d\mathbb{Z}^3),$$

where each p-primary piece is endowed with an induced $\mathbb{Z}G$-module structure by letting G operate in the usual way but with the corresponding modular arithmetic. The situation is thus more favourable than with the Cooley–Tukey method, since there is no interference between the factors (no 'carry'). In the terminology of Section 1.3.4.2.2.2, G acts *diagonally* on this direct sum, and results of a partial transform may be transposed by orbit exchange as in Section 1.3.4.3.4.1 but without the extra terms $\boldsymbol{\mu}$ or $\boldsymbol{\eta}$. The analysis of the symmetry properties of partial transforms also carries over, again without the extra terms. Further simplification occurs for all p-primary pieces with p other than 2 or 3, since all non-primitive translations (including those associated to lattice centring) disappear modulo p.

Thus the cost of the CRT reindexing is compensated by the computational savings due to the absence of twiddle factors and of other phase shifts associated with non-primitive translations and with geometric 'carries'.

Within each p-primary piece, however, higher powers of p may need to be split up by a Cooley–Tukey factorization, or carried out directly by a suitably adapted Winograd algorithm.

1.3.4.3.4.3. *Crystallographic extension of the Rader/Winograd factorization*

As was the case in the absence of symmetry, the two previous classes of algorithms can only factor the global transform into partial transforms on prime numbers of points, but cannot break the latter down any further. Rader's idea of using the action of the group of units $U(p)$ to obtain further factorization of a p-primary transform has been used in 'scalar' form by Auslander & Shenefelt (1987), Shenefelt (1988), and Auslander *et al.* (1988). It will be shown here that it can be adapted to the crystallographic case so as to take advantage also of the possible existence of n-fold cyclic symmetry elements ($n = 3$, 4, 6) in a two-dimensional transform (Bricogne & Tolimieri, 1990). This adaptation entails the use of certain rings of *algebraic* integers rather than ordinary integers, whose connection with the handling of cyclic symmetry will now be examined.

Let G be the group associated with a threefold axis of symmetry: $G = \{e, g, g^2\}$ with $g^3 = e$. In a standard trigonal basis, G has matrix representation

$$\mathbf{R}_e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{I}, \quad \mathbf{R}_g = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \quad \mathbf{R}_{g^2} = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$$

in real space,

$$\mathbf{R}_e^* = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{I}, \quad \mathbf{R}_g^* = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{R}_{g^2}^* = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

in reciprocal space. Note that

$$\mathbf{R}_{g^2}^* = [\mathbf{R}_{g^2}^{-1}]^T = \mathbf{R}_g^T,$$

and that

$$\mathbf{R}_g^T = \mathbf{J}^{-1}\mathbf{R}_g\mathbf{J}, \quad \text{where } \mathbf{J} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

so that $\mathbf{R}_g$ and $\mathbf{R}_g^T$ are conjugate in the group of 2×2 unimodular integer matrices. The group ring $\mathbb{Z}G$ is commutative, and has the structure of the polynomial ring $\mathbb{Z}[X]$ with the single relation $X^2 + X + 1 = 0$ corresponding to the minimal polynomial of $\mathbf{R}_g$. In the terminology of Section 1.3.3.2.4, the ring structure of $\mathbb{Z}G$ is obtained from that of $\mathbb{Z}[X]$ by carrying out polynomial addition and multiplication modulo $X^2 + X + 1$, then replacing X by any generator of G. This type of construction forms the very basis of algebraic number theory [see Artin (1944, Section IIc) for an illustration of this viewpoint], and $\mathbb{Z}G$ as just defined is isomorphic to the ring $\mathbb{Z}[\omega]$ of algebraic integers of the form $a + b\omega$ $[a, b \in \mathbb{Z}, \omega = \exp(2\pi i/3)]$ under the identification $X \leftrightarrow \omega$. Addition in this ring is defined component-wise, while multiplication is defined by

$$\begin{aligned}(a_1 + b_1\omega) \times (a_2 + b_2\omega) = (a_1a_2 - b_1b_2)& \\ + [(a_1 - b_1)b_2 + b_1a_2]\omega&.\end{aligned}$$

In the case of a fourfold axis, $G = \{e, g, g^2, g^3\}$ with $g^4 = e$, and

$$\mathbf{R}_g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \mathbf{R}_g^*, \quad \text{with again } \mathbf{R}_g^T = \mathbf{J}^{-1}\mathbf{R}_g\mathbf{J}.$$

$\mathbb{Z}G$ is obtained from $\mathbb{Z}[X]$ by carrying out polynomial arithmetic modulo $X^2 + 1$. This identifies $\mathbb{Z}G$ with the ring $\mathbb{Z}[i]$ of Gaussian integers of the form $a + bi$, in which addition takes place component-wise while multiplication is defined by

$$(a_1 + b_1i) \times (a_2 + b_2i) = (a_1a_2 - b_1b_2) + (a_1b_2 + b_1a_2)i.$$

In the case of a sixfold axis, $G = \{e, g, g^2, g^3, g^4, g^5\}$ with $g^6 = e$, and

$$\mathbf{R}_g = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{R}_g^* = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \quad \mathbf{R}_g^T = \mathbf{J}^{-1}\mathbf{R}_g\mathbf{J}.$$

$\mathbb{Z}G$ is isomorphic to $\mathbb{Z}[\omega]$ under the mapping $g \leftrightarrow 1 + \omega$ since $(1 + \omega)^6 = 1$.

Thus in all cases $\mathbb{Z}G \cong \mathbb{Z}[X]/P(X)$ where $P(X)$ is an irreducible quadratic polynomial with integer coefficients.

The actions of G on lattices in real and reciprocal space (Sections 1.3.4.2.2.4, 1.3.4.2.2.5) extend naturally to actions of $\mathbb{Z}G$ on $\mathbb{Z}^2$ in which an element $z = a + bg$ of $\mathbb{Z}G$ acts *via*

$$\mathbf{m} = \begin{pmatrix} m_1 \\ m_2 \end{pmatrix} \longmapsto z\mathbf{m} = (a\mathbf{I} + b\mathbf{R}_g)\begin{pmatrix} \mathbf{m}_1 \\ \mathbf{m}_2 \end{pmatrix}$$

in real space, and *via*

$$\mathbf{h} = \begin{pmatrix} h_1 \\ h_2 \end{pmatrix} \longmapsto z\mathbf{h} = (a\mathbf{I} + b\mathbf{R}_g^T)\begin{pmatrix} h_1 \\ h_2 \end{pmatrix}$$

in reciprocal space. These two actions are related by conjugation, since

$$(a\mathbf{I} + b\mathbf{R}_g^T) = \mathbf{J}^{-1}(a\mathbf{I} + b\mathbf{R}_g)\mathbf{J}$$

and the following identity (which is fundamental in the sequel) holds:

$$(z\mathbf{h}) \cdot \mathbf{m} = \mathbf{h} \cdot (z\mathbf{m}) \quad \text{for all } \mathbf{m}, \mathbf{h} \in \mathbb{Z}^2.$$

Let us now consider the calculation of a $p \times p$ two-dimensional DFT with n-fold cyclic symmetry ($n = 3$, 4, 6) for an odd prime $p \geq 5$. Denote $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{Z}_p$. Both the data and the results of the DFT are indexed by $\mathbb{Z}_p \times \mathbb{Z}_p$: hence the action of $\mathbb{Z}G$ on these indices is in fact an action of $\mathbb{Z}_pG$, the latter being obtained from $\mathbb{Z}G$ by carrying out all integer arithmetic in $\mathbb{Z}G$ modulo p. The algebraic structure of $\mathbb{Z}_pG$ combines the symmetry-carrying ring structure of $\mathbb{Z}G$ with the finite field structure of $\mathbb{Z}_p$ used in Section 1.3.3.2.3.1, and holds the key to a symmetry-adapted factorization of the DFT at hand.

The structure of $\mathbb{Z}_pG$ depends on whether $P(X)$ remains irreducible when considered as a polynomial over $\mathbb{Z}_p$. Thus two cases arise:

(1) $P(X)$ remains irreducible mod p, *i.e.* there is no nth root of unity in $\mathbb{Z}_p$;

(2) $P(X)$ factors as $(X - u)(X - v)$, *i.e.* there are nth roots of unity in $\mathbb{Z}_p$.

These two cases require different developments.

Case 1. $\mathbb{Z}_pG$ is a finite field with p^2 elements. There is essentially (*i.e.* up to isomorphism) only one such field, denoted $GF(p^2)$, and its group of units is a cyclic group with $p^2 - 1$ elements. If γ is a generator of this group of units, the input data $\rho_{\mathbf{m}}$ with $\mathbf{m} \neq \mathbf{0}$ may be reordered as

$$\mathbf{m}_0, \gamma\mathbf{m}_0, \gamma^2\mathbf{m}_0, \gamma^3\mathbf{m}_0, \ldots, \gamma^{p^2-2}\mathbf{m}_0$$

by the *real-space action* of γ; while the results $F_{\mathbf{h}}$ with $\mathbf{h} \neq \mathbf{0}$ may be reordered as

$$\mathbf{h}_0, \gamma\mathbf{h}_0, \gamma^2\mathbf{h}_0, \gamma^3\mathbf{h}_0, \ldots, \gamma^{p^2-2}\mathbf{h}_0$$

by the *reciprocal-space action* of γ, where $\mathbf{m}_0$ and $\mathbf{h}_0$ are arbitrary non-zero indices.

The core $\mathbf{C}_{p\times p}$ of the DFT matrix, defined by

$$\mathbf{F}_{p\times p} = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ 1 & & & \\ \vdots & & \mathbf{C}_{p\times p} & \\ 1 & & & \end{pmatrix},$$

will then have a skew-circulant structure (Section 1.3.3.2.3.1) since

$$(\mathbf{C}_{p\times p})_{jk} = e\left[\frac{(\gamma^j\mathbf{h}_0) \cdot (\gamma^k\mathbf{m}_0)}{p}\right] = e\left[\frac{\mathbf{h}_0 \cdot (\gamma^{j+k}\mathbf{m}_0)}{p}\right]$$

depends only on $j + k$. Multiplication by $\mathbf{C}_{p\times p}$ may then be turned into a cyclic convolution of length $p^2 - 1$, which may be factored by two DFTs (Section 1.3.3.2.3.1) or by Winograd's techniques (Section 1.3.3.2.4). The latter factorization is always favourable, as it is easily shown that $p^2 - 1$ is divisible by 24 for any odd prime $p \geq 5$. This procedure is applicable even if no symmetry is present in the data.

Assume now that cyclic symmetry of order $n = 3$, 4 or 6 *is* present. Since n divides 24 hence divides $p^2 - 1$, the generator g of this symmetry is representable as $\gamma^{(p^2-1)/n}$ for a suitable generator γ of the group of units. The reordered data will then be $(p^2 - 1)/n$-periodic rather than simply $(p^2 - 1)$-periodic; hence the reindexed results will be *n-decimated* (Section 1.3.2.7.2), and the $(p^2 - 1)/n$ non-zero results can be calculated by applying the DFT to the $(p^2 - 1)/n$ unique input data. In this way, the n-fold symmetry can be used in full to calculate the core contributions from the unique data to the unique results by a DFT of length $(p^2 - 1)/n$.

It is a simple matter to incorporate non-primitive translations into this scheme. For example, when going from structure factors to electron densities, reordered data items separated by $(p^2 - 1)/n$ are not equal but differ by a phase shift proportional to their index mod p, whose effect is simply to shift the origin of the n-decimated transformed sequence. The same economy of computation can therefore be achieved as in the purely cyclic case.

Dihedral symmetry elements, which map g to g^{-1} (Section 1.3.4.2.2.3), induce extra one-dimensional symmetries of order 2 in the reordered data which can also be fully exploited to reduce computation.

Case 2. If $p \geq 5$, it can be shown that the two roots u and v are always distinct. Then, by the Chinese remainder theorem (CRT) for polynomials (Section 1.3.3.2.4) we have a ring isomorphism

$$\mathbb{Z}_p[X]/P(X) \cong \{\mathbb{Z}_p[X]/(X - u)\} \times \{\mathbb{Z}_p[X]/(X - v)\}$$

defined by sending a polynomial $Q(X)$ from the left-hand-side ring to its two residue classes modulo $X - u$ and $X - v$, respectively. Since the latter are simply the constants $Q(u)$ and $Q(v)$, the CRT reindexing has the particularly simple form

$$a + bX \longmapsto (a + bu, a + bv) = (\alpha, \beta)$$

or equivalently

$$\begin{pmatrix} a \\ b \end{pmatrix} \longmapsto \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \mathbf{M}\begin{pmatrix} a \\ b \end{pmatrix} \bmod p, \quad \text{with } \mathbf{M} = \begin{pmatrix} 1 & u \\ 1 & v \end{pmatrix}.$$

The CRT reconstruction formula similarly simplifies to

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \longmapsto \begin{pmatrix} a \\ b \end{pmatrix} = \mathbf{M}^{-1}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \bmod p,$$
$$\text{with } \mathbf{M}^{-1} = \frac{1}{v - u}\begin{pmatrix} v & -u \\ -1 & 1 \end{pmatrix}.$$

The use of the CRT therefore amounts to the *simultaneous diagonalization* (by $\mathbf{M}$) of all the matrices representing the elements of $\mathbb{Z}_pG$ in the basis $(1, X)$.

A first consequence of this diagonalization is that the internal structure of $\mathbb{Z}_pG$ becomes clearly visible. Indeed, $\mathbb{Z}_pG$ is mapped isomorphically to a direct product of two copies of $\mathbb{Z}_p$, in which arithmetic is carried out *component-wise* between eigenvalues α and β. Thus if

$$z = a + bX \overset{\text{CRT}}{\longleftrightarrow} (\alpha, \beta),$$
$$z' = a' + b'X \overset{\text{CRT}}{\longleftrightarrow} (\alpha', \beta'),$$

then

$$z + z' \overset{\text{CRT}}{\longleftrightarrow} (\alpha + \alpha', \beta + \beta'),$$
$$zz' \overset{\text{CRT}}{\longleftrightarrow} (\alpha\alpha', \beta\beta').$$

Taking in particular

$$z \overset{\text{CRT}}{\longleftrightarrow} (\alpha, 0) \neq (0, 0),$$
$$z' \overset{\text{CRT}}{\longleftrightarrow} (0, \beta) \neq (0, 0),$$

we have $zz' = 0$, so that $\mathbb{Z}_pG$ contains zero divisors; therefore $\mathbb{Z}_pG$ *is not a field.* On the other hand, if $z \overset{\text{CRT}}{\longleftrightarrow} (\alpha, \beta)$ with $\alpha \neq 0$ and $\beta \neq 0$, then α and β belong to the group of units $U(p)$ (Section 1.3.3.2.3.1) and hence have inverses α^{-1} and β^{-1}; it follows that z is a unit in $\mathbb{Z}_pG$, with inverse $z^{-1} \overset{\text{CRT}}{\longleftrightarrow} (\alpha^{-1}, \beta^{-1})$. Therefore, $\mathbb{Z}_pG$ consists of four distinct pieces:

$$0 \overset{\text{CRT}}{\longleftrightarrow} \{(0, 0)\},$$
$$D_1 \overset{\text{CRT}}{\longleftrightarrow} \{(\alpha, 0) | \alpha \in U(p)\} \cong U(p),$$
$$D_2 \overset{\text{CRT}}{\longleftrightarrow} \{(0, \beta) | \beta \in U(p)\} \cong U(p),$$
$$U \overset{\text{CRT}}{\longleftrightarrow} \{(\alpha, \beta) | \alpha \in U(p), \beta \in U(p)\} \cong U(p) \times U(p).$$

A second consequence of this diagonalization is that the actions of $\mathbb{Z}_pG$ on indices $\mathbf{m}$ and $\mathbf{h}$ can themselves be brought to diagonal form by basis changes:

$$\mathbf{m} \longmapsto (a\mathbf{I} + b\mathbf{R}_g)\mathbf{m}$$
$$\text{becomes } \boldsymbol{\mu} \longmapsto \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}\boldsymbol{\mu} \quad \text{with } \boldsymbol{\mu} = \mathbf{Mm},$$
$$\mathbf{h} \longmapsto (a\mathbf{I} + b\mathbf{R}_g^T)\mathbf{h}$$
$$\text{becomes } \boldsymbol{\eta} \longmapsto \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}\boldsymbol{\eta} \quad \text{with } \boldsymbol{\eta} = \mathbf{MJh}.$$

Thus the sets of indices $\boldsymbol{\mu}$ and $\boldsymbol{\eta}$ can be split into four pieces as $\mathbb{Z}_pG$ itself, according as these indices have none, one or two of their coordinates in $U(p)$. These pieces will be labelled by the same symbols – 0, D_1, D_2 and U – as those of $\mathbb{Z}_pG$.

The scalar product $\mathbf{h} \cdot \mathbf{m}$ may be written in terms of $\boldsymbol{\eta}$ and $\boldsymbol{\mu}$ as

$$\mathbf{h} \cdot \mathbf{m} = [\boldsymbol{\eta} \cdot ((\mathbf{M}^{-1})^T \mathbf{JM}^{-1})\boldsymbol{\mu}],$$

and an elementary calculation shows that the matrix $= (\mathbf{M}^{-1})^T \mathbf{JM}^{-1}$ is *diagonal* by virtue of the relation

$$uv = \text{constant term in } P(X) = 1.$$

Therefore, $\mathbf{h} \cdot \mathbf{m} = 0$ if $\mathbf{h} \in D_1$ and $\boldsymbol{\mu} \in D_2$ or *vice versa.*

We are now in a position to rearrange the DFT matrix $\mathbf{F}_{p \times p}$. Clearly, the structure of $\mathbf{F}_{p \times p}$ is more complex than in case 1, as there are three types of 'core' matrices:

type 1: $D \times D$ (with $D = D_1$ or D_2);

type 2: $D \times U$ or $U \times D$;

type 3: $U \times U$.

(Submatrices of type $D_1 \times D_2$ and $D_2 \times D_1$ have all their elements equal to 1 by the previous remark.)

Let γ be a generator of $U(p)$. We may reorder the elements in D_1, D_2 and U – and hence the data and results indexed by these elements – according to powers of γ. This requires one exponent in each of D_1 and D_2, and two exponents in U. For instance, in the $\mathbf{h}$-index space:

$$D_1 = \left\{ \begin{pmatrix} \gamma & 0 \\ 0 & 0 \end{pmatrix}^j \begin{pmatrix} \eta_1 \\ 0 \end{pmatrix}_0 \middle| j = 1, \ldots, p - 1 \right\}$$

$$D_2 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & \gamma \end{pmatrix}^j \begin{pmatrix} 0 \\ \eta_2 \end{pmatrix}_0 \middle| j = 1, \ldots, p - 1 \right\}$$

$$U = \left\{ \begin{pmatrix} \gamma & 0 \\ 0 & 1 \end{pmatrix}^{j_1} \begin{pmatrix} 1 & 0 \\ 0 & \gamma \end{pmatrix}^{j_2} \begin{pmatrix} \eta_1 \\ \eta_2 \end{pmatrix}_0 \middle| j_1 = 1, \ldots, p - 1; \; j_2 = 1, \ldots, p - 1 \right\}$$

and similarly for the $\boldsymbol{\mu}$ index.

Since the diagonal matrix $\boldsymbol{\Delta}$ commutes with all the matrices representing the action of γ, this rearrangement will induce skew-circulant structures in all the core matrices. The corresponding cyclic convolutions may be carried out by Rader's method, *i.e.* by diagonalizing them by means of two $(p - 1)$-point one-dimensional DFTs in the $D \times D$ pieces and of two $(p - 1) \times (p - 1)$-point two-dimensional DFTs in the $U \times U$ piece (the $U \times D$ and $D \times U$ pieces involve extra section and projection operations).

In the absence of symmetry, no computational saving is achieved, since the same reordering could have been applied to the initial $\mathbb{Z}_p \times \mathbb{Z}_p$ indexing, without the CRT reindexing.

In the presence of n-fold cyclic symmetry, however, the rearranged $\mathbf{F}_{p \times p}$ lends itself to an n-fold reduction in size. The basic fact is that whenever case 2 occurs, $p - 1$ is divisible by n (*i.e.* $p - 1$ is divisible by 6 when $n = 3$ or 6, and by 4 when $n = 4$), say

$p-1=nq$. If g is a generator of the cyclic symmetry, the generator γ of $U(p)$ may be chosen in such a way that $g=\gamma^q$. The action of g is then to increment the j index in D_1 and D_2 by q, and the (j_1, j_2) index in U by (q, q). Since the data items whose indices are related in this way have identical values, the DFTs used to diagonalize the Rader cyclic convolutions will operate on *periodized data*, hence yield *decimated results*; and the non-zero results will be obtained from the unique data by DFTs n times smaller than their counterparts in the absence of symmetry.

A more thorough analysis is needed to obtain a Winograd factorization into the normal from **CBA** in the presence of symmetry (see Bricogne & Tolimieri, 1990).

Non-primitive translations and dihedral symmetry may also be accommodated within this framework, as in case 1.

This reindexing by means of algebraic integers yields larger orbits, hence more efficient algorithms, than that of Auslander *et al.* (1988) which only uses ordinary integers acting by scalar dilation.

1.3.4.3.5. *Treatment of conjugate and parity-related symmetry properties*

Most crystallographic Fourier syntheses are real-valued and originate from Hermitian-symmetric collections of Fourier coefficients. Hermitian symmetry is closely related to the action of a centre of inversion in reciprocal space, and thus interacts strongly with all other genuinely crystallographic symmetry elements of order 2. All these symmetry properties are best treated by factoring by 2 and reducing the computation of the initial transform to that of a collection of smaller transforms with less symmetry or none at all.

1.3.4.3.5.1. *Hermitian-symmetric or real-valued transforms*

The computation of a DFT with Hermitian-symmetric or real-valued data can be carried out at a cost of half that of an ordinary transform, essentially by 'multiplexing' pairs of special partial transforms into general complex transforms, and then 'demultiplexing' the results on the basis of their symmetry properties. The treatment given below is for general dimension n; a subset of cases for $n=1$ was treated by Ten Eyck (1973).

(*a*) *Underlying group action*

Hermitian symmetry is not a geometric symmetry, but it is defined in terms of the action in reciprocal space of point group $G=\bar{1}$, *i.e.* $G=\{e,-e\}$, where e acts as $\mathbf{I}$ (the $n\times n$ identity matrix) and $-e$ acts as $-\mathbf{I}$.

This group action on $\mathbb{Z}^n/\mathbf{N}\mathbb{Z}^n$ with $\mathbf{N}=\mathbf{N}_1\mathbf{N}_2$ will now be characterized by the calculation of the cocycle $\boldsymbol{\eta}_1$ (Section 1.3.4.3.4.1) under the assumption that $\mathbf{N}_1$ and $\mathbf{N}_2$ are both *diagonal.* For this purpose it is convenient to associate to any integer vector

$\mathbf{v}=\begin{pmatrix} v_1\\ \vdots\\ v_n\end{pmatrix}$ in $\mathbb{Z}^n$ the vector $\boldsymbol{\zeta}(\mathbf{v})$ whose jth component is

$$\begin{cases} 0 \text{ if } & v_j=0\\ 1 \text{ if } & v_j\neq 0.\end{cases}$$

Let $\mathbf{m}=\mathbf{m}_1+\mathbf{N}_1\mathbf{m}_2$, and hence $\mathbf{h}=\mathbf{h}_2+\mathbf{N}_2\mathbf{h}_1$. Then

$$\begin{aligned} -\mathbf{h}_2 \bmod \mathbf{N}\mathbb{Z}^n &= \mathbf{N}\boldsymbol{\zeta}(\mathbf{h}_2)-\mathbf{h}_2,\\ -\mathbf{h}_2 \bmod \mathbf{N}_2\mathbb{Z}^n &= \mathbf{N}_2\boldsymbol{\zeta}(\mathbf{h}_2)-\mathbf{h}_2,\end{aligned}$$

hence

$$\begin{aligned}\boldsymbol{\eta}_1(-e,\mathbf{h}_2) &= \mathbf{N}_2^{-1}\{[\mathbf{N}\boldsymbol{\zeta}(\mathbf{h}_2)-\mathbf{h}_2]-[\mathbf{N}_2\boldsymbol{\zeta}(\mathbf{h}_2)-\mathbf{h}_2]\} \bmod \mathbf{N}_1\mathbb{Z}^n\\ &= -\boldsymbol{\zeta}(\mathbf{h}_2) \bmod \mathbf{N}_1\mathbb{Z}^n.\end{aligned}$$

Therefore $-e$ acts by

$$(\mathbf{h}_2,\mathbf{h}_1)\longmapsto[\mathbf{N}_2\boldsymbol{\zeta}(\mathbf{h}_2)-\mathbf{h}_2, \mathbf{N}_1\boldsymbol{\zeta}(\mathbf{h}_1)-\mathbf{h}_1-\boldsymbol{\zeta}(\mathbf{h}_2)].$$

Hermitian symmetry is traditionally dealt with by factoring by 2, *i.e.* by assuming $\mathbf{N}=2\mathbf{M}$. If $\mathbf{N}_2=2\mathbf{I}$, then each $\mathbf{h}_2$ is invariant under G, so that each partial vector $\mathbf{Z}^*_{\mathbf{h}_2}$ (Section 1.3.4.3.4.1) inherits the symmetry internally, with a 'modulation' by $\boldsymbol{\eta}_1(g,\mathbf{h}_2)$. The 'multiplexing–demultiplexing' technique provides an efficient treatment of this singular case.

(*b*) *Calculation of structure factors*

The computation may be summarized as follows:

$$\not{\rho}\overset{\mathbf{dec}(\mathbf{N}_1)}{\longmapsto}\mathbf{Y}\overset{\bar{F}(\mathbf{N}_2)}{\longmapsto}\mathbf{Y}^*\overset{\mathrm{TW}}{\longmapsto}\mathbf{Z}\overset{\bar{F}(\mathbf{N}_1)}{\longmapsto}\mathbf{Z}^*\overset{\mathbf{rev}(\mathbf{N}_2)}{\longmapsto}\mathbf{F}$$

where $\mathbf{dec}(\mathbf{N}_1)$ is the initial decimation given by $Y_{\mathbf{m}_1}(\mathbf{m}_2)=\not{\rho}(\mathbf{m}_1+\mathbf{N}_1\mathbf{m}_2)$, TW is the transposition and twiddle-factor stage, and $\mathbf{rev}(\mathbf{N}_2)$ is the final unscrambling by coset reversal given by $F(\mathbf{h}_2+\mathbf{N}_2\mathbf{h}_1)=\mathbf{Z}^*_{\mathbf{h}_2}(\mathbf{h}_1)$.

(i) *Decimation in time* $(\mathbf{N}_1=2\mathbf{I}, \mathbf{N}_2=\mathbf{M})$

The decimated vectors $\mathbf{Y}_{\mathbf{m}_1}$ are real and hence have Hermitian transforms $\mathbf{Y}^*_{\mathbf{m}_1}$. The 2^n values of $\mathbf{m}_1$ may be grouped into 2^{n-1} pairs $(\mathbf{m}'_1,\mathbf{m}''_1)$ and the vectors corresponding to each pair may be multiplexed into a general complex vector

$$\mathbf{Y}=\mathbf{Y}_{\mathbf{m}'_1}+i\mathbf{Y}_{\mathbf{m}''_1}.$$

The transform $\mathbf{Y}^*=\bar{F}(\mathbf{M})[\mathbf{Y}]$ can then be resolved into the separate transforms $\mathbf{Y}^*_{\mathbf{m}'_1}$ and $\mathbf{Y}^*_{\mathbf{m}''_1}$ by using the Hermitian symmetry of the latter, which yields the demultiplexing formulae

$$\begin{aligned} Y^*_{\mathbf{m}'_1}(\mathbf{h}_2)+iY^*_{\mathbf{m}''_1}(\mathbf{h}_2) &= Y^*(\mathbf{h}_2)\\ \overline{Y^*_{\mathbf{m}'_1}(\mathbf{h}_2)}+\overline{iY^*_{\mathbf{m}''_1}(\mathbf{h}_2)} &= Y^*[\mathbf{M}\boldsymbol{\zeta}(\mathbf{h}_2)-\mathbf{h}_2].\end{aligned}$$

The number of partial transforms $\bar{F}(\mathbf{M})$ is thus reduced from 2^n to 2^{n-1}. Once this separation has been achieved, the remaining steps need only be carried out for a unique half of the values of $\mathbf{h}_2$.

(ii) *Decimation in frequency* $(\mathbf{N}_1=\mathbf{M}, \mathbf{N}_2=2\mathbf{I})$

Since $\mathbf{h}_2\in\mathbb{Z}^n/2\mathbb{Z}^n$ we have $-\mathbf{h}_2=\mathbf{h}_2$ and $\boldsymbol{\zeta}(\mathbf{h}_2)=\mathbf{h}_2 \bmod 2\mathbb{Z}^n$. The vectors of decimated and scrambled results $\mathbf{Z}^*_{\mathbf{h}_2}$ then obey the symmetry relations

$$Z^*_{\mathbf{h}_2}(\mathbf{h}_1-\mathbf{h}_2)=\overline{Z^*_{\mathbf{h}_2}[\mathbf{M}\boldsymbol{\zeta}(\mathbf{h}_1)-\mathbf{h}_1]}$$

which can be used to halve the number of $\bar{F}(\mathbf{M})$ necessary to compute them, as follows.

Having formed the vectors $\mathbf{Z}_{\mathbf{h}_2}$ given by

$$Z_{\mathbf{h}_2}(\mathbf{m}_1)=\left[\sum_{\mathbf{m}_2\in\mathbb{Z}^n/2\mathbb{Z}^n}\frac{(-1)^{\mathbf{h}_2\cdot\mathbf{m}_2}}{2^n}\not{\rho}(\mathbf{m}_1+\mathbf{M}\mathbf{m}_2)\right]e[\mathbf{h}_2\cdot(\mathbf{N}^{-1}\mathbf{m}_1)],$$

we may group the 2^n values of $\mathbf{h}_2$ into 2^{n-1} pairs $(\mathbf{h}'_2,\mathbf{h}''_2)$ and for each pair form the multiplexed vector:

$$\mathbf{Z}=\mathbf{Z}_{\mathbf{h}'_2}+i\mathbf{Z}_{\mathbf{h}''_2}.$$

After calculating the 2^{n-1} transforms $\mathbf{Z}^*=\bar{F}(\mathbf{M})[\mathbf{Z}]$, the 2^n individual transforms $\mathbf{Z}^*_{\mathbf{h}'_2}$ and $\mathbf{Z}^*_{\mathbf{h}''_2}$ can be separated by using for each pair the demultiplexing formulae

$$\begin{aligned} Z^*_{\mathbf{h}'_2}(\mathbf{h}_1)+iZ^*_{\mathbf{h}''_2}(\mathbf{h}_1) &= Z^*(\mathbf{h}_1)\\ Z^*_{\mathbf{h}'_2}(\mathbf{h}_1-\mathbf{h}'_2)+iZ^*_{\mathbf{h}''_2}(\mathbf{h}_1-\mathbf{h}''_2) &= \overline{Z^*[\mathbf{M}\boldsymbol{\zeta}(\mathbf{h}_1)-\mathbf{h}_1]}\end{aligned}$$

which can be solved recursively. If all pairs are chosen so that they differ only in the jth coordinate $(\mathbf{h}_2)_j$, the recursion is along $(\mathbf{h}_1)_j$ and can be initiated by introducing the (real) values of $Z^*_{\mathbf{h}'_2}$ and $Z^*_{\mathbf{h}''_2}$ at $(\mathbf{h}_1)_j=0$ and $(\mathbf{h}_1)_j=M_j$, accumulated *e.g.* while forming $\mathbf{Z}$ for that pair. Only points with $(\mathbf{h}_1)_j$ going from 0 to $\frac{1}{2}M_j$ need be resolved,