International Tables for Crystallography (2006). Vol. B, Section 1.3.3.2.2, pp. 51–52.

(iv) calculate the N_2 transforms $\mathbf{Z}^*_{k_2^*}$ on N_1 points:

$$\mathbf{Z}^*_{k_2^*} = \bar{F}(N_1)[\mathbf{Z}_{k_2^*}], \quad k_2^* \in \mathbb{Z}/N_2\mathbb{Z};$$

(v) collect $X^*(k_2^* + k_1^* N_2)$ as $Z^*_{k_2^*}(k_1^*)$.

If the intermediate transforms in stages (ii) and (iv) are performed *in place*, *i.e.* with the results overwriting the data, then at stage (v) the result $X^*(k_2^* + k_1^* N_2)$ will be found at address $k_1^* + N_1 k_2^*$. This phenomenon is called *scrambling* by 'digit reversal', and stage (v) is accordingly known as *unscrambling*.

The initial *N-point* transform $\bar{F}(N)$ has thus been performed as N_1 transforms $\bar{F}(N_2)$ on N_2 points, followed by N_2 transforms $\bar{F}(N_1)$ on N_1 points, thereby reducing the arithmetic cost from $(N_1N_2)^2$ to $N_1N_2(N_1 + N_2)$. The phase shifts applied at stage (iii) are traditionally called 'twiddle factors', and the transposition between k_1 and k_2^* can be performed by the fast recursive technique of Eklundh (1972). Clearly, this procedure can be applied recursively if N_1 and N_2 are themselves composite, leading to an overall arithmetic cost of order $N \log N$ if N has no large prime factors.

The Cooley–Tukey factorization may also be derived from a geometric rather than arithmetic argument. The decomposition $k = k_1 + N_1 k_2$ is associated to a geometric partition of the residual lattice $\mathbb{Z}/N\mathbb{Z}$ into N_1 copies of $\mathbb{Z}/N_2\mathbb{Z}$, each translated by $k_1 \in \mathbb{Z}/N_1\mathbb{Z}$ and 'blown up' by a factor N_1. This partition in turn induces a (direct sum) decomposition of $\mathbf{X}$ as

$$\mathbf{X} = \sum_{k_1} \mathbf{X}_{k_1},$$

where

$$\begin{aligned} X_{k_1}(k) &= X(k) \quad \text{if } k \equiv k_1 \bmod N_1, \\ &= 0 \qquad \text{otherwise.} \end{aligned}$$

According to (i), $\mathbf{X}_{k_1}$ is related to $\mathbf{Y}_{k_1}$ by *decimation by* N_1 and *offset by* k_1. By Section 1.3.2.7.2, $\bar{F}(N)[\mathbf{X}_{k_1}]$ is related to $\bar{F}(N_2)[\mathbf{Y}_{k_1}]$ by *periodization by* N_2 and *phase shift by* $e(k^* k_1/N)$, so that

$$X^*(k^*) = \sum_{k_1} e\left(\frac{k^* k_1}{N}\right) Y^*_{k_1}(k_2^*),$$

the periodization by N_2 being reflected by the fact that $Y^*_{k_1}$ does not depend on k_1^*. Writing $k^* = k_2^* + k_1^* N_2$ and expanding $k^* k_1$ shows that the phase shift contains both the twiddle factor $e(k_2^* k_1/N)$ and the kernel $e(k_1^* k_1/N_1)$ of $\bar{F}(N_1)$. The Cooley–Tukey algorithm is thus naturally associated to the coset decomposition of a lattice modulo a sublattice (Section 1.3.2.7.2).

It is readily seen that essentially the same factorization can be obtained for $F(N)$, up to the complex conjugation of the twiddle factors. The normalizing constant $1/N$ arises from the normalizing constants $1/N_1$ and $1/N_2$ in $F(N_1)$ and $F(N_2)$, respectively.

Factors of 2 are particularly simple to deal with and give rise to a characteristic computational structure called a 'butterfly loop'. If $N = 2M$, then two options exist:

(*a*) using $N_1 = 2$ and $N_2 = M$ leads to collecting the even-numbered coordinates of $\mathbf{X}$ into $\mathbf{Y}_0$ and the odd-numbered coordinates into $\mathbf{Y}_1$

$$\begin{aligned} Y_0(k_2) &= X(2k_2), \qquad & k_2 &= 0, \ldots, M-1, \\ Y_1(k_2) &= X(2k_2 + 1), \qquad & k_2 &= 0, \ldots, M-1, \end{aligned}$$

and writing:

$$\begin{aligned} X^*(k_2^*) &= Y_0^*(k_2^*) + e(k_2^*/N) Y_1^*(k_2^*), \\ & \qquad k_2^* = 0, \ldots, M-1; \\ X^*(k_2^* + M) &= Y_0^*(k_2^*) - e(k_2^*/N) Y_1^*(k_2^*), \\ & \qquad k_2^* = 0, \ldots, M-1. \end{aligned}$$

This is the original version of Cooley & Tukey, and the process of formation of $\mathbf{Y}_0$ and $\mathbf{Y}_1$ is referred to as 'decimation in time' (*i.e.* decimation along the *data* index $\mathbf{k}$).

(*b*) using $N_1 = M$ and $N_2 = 2$ leads to forming

$$\begin{aligned} Z_0(k_1) &= X(k_1) + X(k_1 + M), \qquad & k_1 &= 0, \ldots, M-1, \\ Z_1(k_1) &= [X(k_1) - X(k_1 + M)] e\left(\frac{k_1}{N}\right), \qquad & k_1 &= 0, \ldots, M-1, \end{aligned}$$

then obtaining separately the even-numbered and odd-numbered components of $\mathbf{X}^*$ by transforming $\mathbf{Z}_0$ and $\mathbf{Z}_1$:

$$\begin{aligned} X^*(2k_1^*) &= Z_0^*(k_1^*), \quad k_1^* = 0, \ldots, M-1; \\ X^*(2k_1^* + 1) &= Z_1^*(k_1^*), \quad k_1^* = 0, \ldots, M-1. \end{aligned}$$

This version is due to Sande (Gentleman & Sande, 1966), and the process of separately obtaining even-numbered and odd-numbered results has led to its being referred to as 'decimation in frequency' (*i.e.* decimation along the *result* index k^*).

By repeated factoring of the number N of sample points, the calculation of $F(N)$ and $\bar{F}(N)$ can be reduced to a succession of stages, the smallest of which operate on single prime factors of N. The reader is referred to Gentleman & Sande (1966) for a particularly lucid analysis of the programming considerations which help implement this factorization efficiently; see also Singleton (1969). Powers of two are often grouped together into factors of 4 or 8, which are advantageous in that they require fewer complex multiplications than the repeated use of factors of 2. In this approach, large prime factors P are detrimental, since they require a full P^2-size computation according to the defining formula.

1.3.3.2.2. *The Good (or prime factor) algorithm*

1.3.3.2.2.1. *Ring structure on* $\mathbb{Z}/N\mathbb{Z}$

The set $\mathbb{Z}/N\mathbb{Z}$ of congruence classes of integers modulo an integer N [see *e.g.* Apostol (1976), Chapter 5] inherits from $\mathbb{Z}$ not only the additive structure used in deriving the Cooley–Tukey factorization, but also a *multiplicative* structure in which the product of two congruence classes mod N is uniquely defined as the class of the ordinary product (in $\mathbb{Z}$) of representatives of each class. The multiplication can be distributed over addition in the usual way, endowing $\mathbb{Z}/N\mathbb{Z}$ with the structure of a *commutative ring*.

If N is composite, the ring $\mathbb{Z}/N\mathbb{Z}$ has *zero divisors*. For example, let $N = N_1N_2$, let $n_1 \equiv N_1 \bmod N$, and let $n_2 \equiv N_2 \bmod N$: then $n_1 n_2 \equiv 0 \bmod N$. In the general case, a product of non-zero elements will be zero whenever these elements collect together all the factors of N. These circumstances give rise to a fundamental theorem in the theory of commutative rings, the *Chinese Remainder Theorem* (CRT), which will now be stated and proved [see Apostol (1976), Chapter 5; Schroeder (1986), Chapter 16].

1.3.3.2.2.2. *The Chinese remainder theorem*

Let $N = N_1 N_2 \ldots N_d$ be factored into a product of pairwise coprime integers, so that g.c.d. $(N_i, N_j) = 1$ for $i \neq j$. Then the system of congruence equations

$$\ell \equiv \ell_j \bmod N_j, \qquad j = 1, \ldots, d,$$

has a unique solution $\ell \bmod N$. In other words, each $\ell \in \mathbb{Z}/N\mathbb{Z}$ is associated in a one-to-one fashion to the d-tuple $(\ell_1, \ell_2, \ldots, \ell_d)$ of its residue classes in $\mathbb{Z}/N_1\mathbb{Z}, \mathbb{Z}/N_2\mathbb{Z}, \ldots, \mathbb{Z}/N_d\mathbb{Z}$.

The proof of the CRT goes as follows. Let

$$Q_j = \frac{N}{N_j} = \prod_{i \neq j} N_i.$$

Since g.c.d. $(N_j, Q_j) = 1$ there exist integers n_j and q_j such that

$$n_j N_j + q_j Q_j = 1, \qquad j = 1, \ldots, d,$$

then the integer

$$\ell = \sum_{i=1}^{d} \ell_i q_i Q_i \text{ mod } N$$

is the solution. Indeed,

$$\ell \equiv \ell_j q_j Q_j \text{ mod } N_j$$

because all terms with $i \neq j$ contain N_j as a factor; and

$$q_j Q_j \equiv 1 \text{ mod } N_j$$

by the defining relation for q_j.

It may be noted that

$$\begin{aligned} (q_i Q_i)(q_j Q_j) &\equiv 0 \qquad \text{mod } N \text{ for } i \neq j, \\ (q_j Q_j)^2 &\equiv q_j Q_j \quad \text{mod } N, \ \ j = 1, \ldots, d, \end{aligned}$$

so that the $q_j Q_j$ are mutually orthogonal *idempotents* in the ring $\mathbb{Z}/N\mathbb{Z}$, with properties formally similar to those of mutually orthogonal *projectors onto subspaces* in linear algebra. The analogy is exact, since by virtue of the CRT the ring $\mathbb{Z}/N\mathbb{Z}$ may be considered as the direct product

$$\mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_2\mathbb{Z} \times \ldots \times \mathbb{Z}/N_d\mathbb{Z}$$

via the two mutually inverse mappings:

(i) $\ell \longmapsto (\ell_1, \ell_2, \ldots, \ell_d)$ by $\ell \equiv \ell_j$ mod N_j for each j;

(ii) $(\ell_1, \ell_2, \ldots, \ell_d) \longmapsto \ell$ by $\ell = \sum_{i=1}^{d} \ell_i q_i Q_i$ mod N.

The mapping defined by (ii) is sometimes called the 'CRT reconstruction' of ℓ from the ℓ_j.

These two mappings have the property of sending sums to sums and products to products, *i.e*:

$$\begin{aligned} &\text{(i)} \qquad \ell + \ell' \longmapsto (\ell_1 + \ell'_1, \ell_2 + \ell'_2, \ldots, \ell_d + \ell'_d) \\ &\qquad\qquad \ell\ell' \longmapsto (\ell_1\ell'_1, \ell_2\ell'_2, \ldots, \ell_d\ell'_d) \\ &\text{(ii)} \qquad (\ell_1 + \ell'_1, \ell_2 + \ell'_2, \ldots, \ell_d + \ell'_d) \longmapsto \ell + \ell' \\ &\qquad\qquad (\ell_1\ell'_1, \ell_2\ell'_2, \ldots, \ell_d\ell'_d) \longmapsto \ell\ell' \end{aligned}$$

(the last proof requires using the properties of the idempotents $q_j Q_j$). This may be described formally by stating that the CRT establishes a *ring isomorphism*:

$$\mathbb{Z}/N\mathbb{Z} \cong (\mathbb{Z}/N_1\mathbb{Z}) \times \ldots \times (\mathbb{Z}/N_d\mathbb{Z}).$$

1.3.3.2.2.3. *The prime factor algorithm*

The CRT will now be used to factor the N-point DFT into a tensor product of d transforms, the jth of length N_j.

Let the indices k and k^* be subjected to the following mappings:

(i) $k \longmapsto (k_1, k_2, \ldots, k_d), k_j \in \mathbb{Z}/N_j\mathbb{Z}$, by $k_j \equiv k$ mod N_j for each j, with reconstruction formula

$$k = \sum_{i=1}^{d} k_i q_i Q_i \text{ mod } N;$$

(ii) $k^* \longmapsto (k_1^*, k_2^*, \ldots, k_d^*), k_j^* \in \mathbb{Z}/N_j\mathbb{Z}$, by $k_j^* \equiv q_j k^*$ mod N_j for each j, with reconstruction formula

$$k^* = \sum_{i=1}^{d} k_i^* Q_i \text{ mod } N.$$

Then

$$\begin{aligned} k^* k &= \left(\sum_{i=1}^{d} k_i^* Q_i\right)\left(\sum_{j=1}^{d} k_j q_j Q_j\right) \text{ mod } N \\ &= \sum_{i,\, j=1}^{d} k_i^* k_j Q_i q_j Q_j \text{ mod } N. \end{aligned}$$

Cross terms with $i \neq j$ vanish since they contain all the factors of N, hence

$$\begin{aligned} k^* k &= \sum_{j=1}^{d} q_j Q_j^2 k_j^* k_j \text{ mod } N \\ &= \sum_{j=1}^{d} (1 - n_j N_j) Q_j k_j^* k_j \text{ mod } N. \end{aligned}$$

Dividing by N, which may be written as $N_j Q_j$ for each j, yields

$$\begin{aligned} \frac{k^* k}{N} &= \sum_{j=1}^{d} (1 - n_j N_j) \frac{Q_j}{N_j Q_j} k_j^* k_j \text{ mod } 1 \\ &= \sum_{j=1}^{d} \left(\frac{1}{N_j} - n_j\right) k_j^* k_j \text{ mod } 1, \end{aligned}$$

and hence

$$\frac{k^* k}{N} \equiv \sum_{j=1}^{d} \frac{k_j^* k_j}{N_j} \text{ mod } 1.$$

Therefore, by the multiplicative property of $e(.)$,

$$e\left(\frac{k^* k}{N}\right) \equiv \bigotimes_{j=1}^{d} e\left(\frac{k_j^* k_j}{N_j}\right).$$

Let $\mathbf{X} \in L(\mathbb{Z}/N\mathbb{Z})$ be described by a one-dimensional array $X(k)$ indexed by k. The index mapping (i) turns $\mathbf{X}$ into an element of $L(\mathbb{Z}/N_1\mathbb{Z} \times \ldots \times \mathbb{Z}/N_d\mathbb{Z})$ described by a d-dimensional array $X(k_1, \ldots, k_d)$; the latter may be transformed by $\bar{F}(N_1) \bigotimes \ldots \bigotimes \bar{F}(N_d)$ into a new array $X^*(k_1^*, k_2^*, \ldots, k_d^*)$. Finally, the one-dimensional array of results $X^*(k^*)$ will be obtained by reconstructing k^* according to (ii).

The prime factor algorithm, like the Cooley–Tukey algorithm, reindexes a 1D transform to turn it into d separate transforms, but the use of coprime factors and CRT index mapping leads to the further gain that *no twiddle factors* need to be applied between the successive transforms (see Good, 1971). This makes up for the cost of the added complexity of the CRT index mapping.

The natural factorization of N for the prime factor algorithm is thus its factorization into prime powers: $\bar{F}(N)$ is then the tensor product of separate transforms (one for each prime power factor $N_j = p_j^{\nu_j}$) whose results can be reassembled without twiddle factors. The separate factors p_j within each N_j must then be dealt with by another algorithm (*e.g.* Cooley–Tukey, which does require twiddle factors). Thus, the DFT on a prime number of points remains undecomposable.

1.3.3.2.3. *The Rader algorithm*

The previous two algorithms essentially reduce the calculation of the DFT on N points for N composite to the calculation of smaller DFTs on prime numbers of points, the latter remaining irreducible. However, Rader (1968) showed that the p-point DFT for p an odd

references