$$Y^*(0) = \sum_k Y(k)$$

$$\begin{aligned} Y^*(m^*+1) &= Y(0) + \sum_{m=0}^{p-2} C(m^*+m)Y(m+1) \\ &= Y(0) + \sum_{m=0}^{p-2} C(m^*-m)Z(m) \\ &= Y(0) + (\mathbf{C} * \mathbf{Z})(m^*), \quad m^* = 0, \ldots, p-2, \end{aligned}$$

where $\mathbf{Z}$ is defined by $Z(m) = Y(p-m-2)$, $m = 0, \ldots, p-2$.

Thus $\mathbf{Y}^*$ may be obtained by cyclic convolution of $\mathbf{C}$ and $\mathbf{Z}$, which may for instance be calculated by

$$\mathbf{C} * \mathbf{Z} = F(p-1)[\bar{F}(p-1)[\mathbf{C}] \times \bar{F}(p-1)[\mathbf{Z}]],$$

where $\times$ denotes the component-wise multiplication of vectors. Since p is odd, $p-1$ is always divisible by 2 and may even be highly composite. In that case, factoring $\bar{F}(p-1)$ by means of the Cooley–Tukey or Good methods leads to an algorithm of complexity $p \log p$ rather than p^2 for $\bar{F}(p)$. An added bonus is that, because $g^{(p-1)/2} = -1$, the elements of $\bar{F}(p-1)[\mathbf{C}]$ can be shown to be either purely real or purely imaginary, which halves the number of real multiplications involved.

1.3.3.2.3.2. N a power of an odd prime

This idea was extended by Winograd (1976, 1978) to the treatment of prime powers $N = p^\nu$, using the cyclic structure of the multiplicative group of units $U(p^\nu)$. The latter consists of all those elements of $\mathbb{Z}/p^\nu\mathbb{Z}$ which are not divisible by p, and thus has $q_\nu = p^{\nu-1}(p-1)$ elements. It is cyclic, and there exist primitive roots g modulo p^ν such that

$$U(p^\nu) = \{1, g, g^2, g^3, \ldots, g^{q_\nu - 1}\}.$$

The $p^{\nu-1}$ elements divisible by p, which are divisors of zero, have to be treated separately just as 0 had to be treated separately for $N = p$.

When $k^* \notin U(p^\nu)$, then $k^* = pk_1^*$ with $k_1^* \in \mathbb{Z}/p^{\nu-1}\mathbb{Z}$. The results $X^*(pk_1^*)$ are p-decimated, hence can be obtained *via* the $p^{\nu-1}$-point DFT of the $p^{\nu-1}$-periodized data $\mathbf{Y}$:

$$X^*(pk_1^*) = \bar{F}(p^{\nu-1})[\mathbf{Y}](k_1^*)$$

with

$$Y(k_1) = \sum_{k_2 \in \mathbb{Z}/p\mathbb{Z}} X(k_1 + p^{\nu-1}k_2).$$

When $k^* \in U(p^\nu)$, then we may write

$$X^*(k^*) = X_0^*(k^*) + X_1^*(k^*),$$

where $\mathbf{X}_0^*$ contains the contributions from $k \notin U(p^\nu)$ and $\mathbf{X}_1^*$ those from $k \in U(p^\nu)$. By a converse of the previous calculation, $\mathbf{X}_0^*$ arises from p-decimated data $\mathbf{Z}$, hence is the $p^{\nu-1}$-periodization of the $p^{\nu-1}$-point DFT of these data:

$$X_0^*(p^{\nu-1}k_1^* + k_2^*) = \bar{F}(p^{\nu-1})[\mathbf{Z}](k_2^*)$$

with

$$Z(k_2) = X(pk_2), \qquad k_2 \in \mathbb{Z}/p^{\nu-1}\mathbb{Z}$$

(the $p^{\nu-1}$-periodicity follows implicity from the fact that the transform on the right-hand side is independent of $k_1^* \in \mathbb{Z}/p\mathbb{Z}$).

Finally, the contribution X_1^* from all $k \in U(p^\nu)$ may be calculated by reindexing by the powers of a primitive root g modulo p^ν, *i.e.* by writing

$$X_1^*(g^{m^*}) = \sum_{m=0}^{q_\nu - 1} X(g^m)e(g^{(m^*+m)/p^\nu})$$

then carrying out the multiplication by the skew-circulant matrix core as a convolution.

Thus the DFT of size p^ν may be reduced to two DFTs of size $p^{\nu-1}$ (dealing, respectively, with p-decimated results and p-decimated data) and a convolution of size $q_\nu = p^{\nu-1}(p-1)$. The latter may be 'diagonalized' into a multiplication by purely real or purely imaginary numbers (because $g^{(q_\nu/2)} = -1$) by two DFTs, whose factoring in turn leads to DFTs of size $p^{\nu-1}$ and $p-1$. This method, applied recursively, allows the complete decomposition of the DFT on p^ν points into arbitrarily small DFTs.

1.3.3.2.3.3. N a power of 2

When $N = 2^\nu$, the same method can be applied, except for a slight modification in the calculation of $\mathbf{X}_1^*$. There is no primitive root modulo 2^ν for $\nu > 2$: the group $U(2^\nu)$ is the direct product of *two* cyclic groups, the first (of order 2) generated by -1, the second (of order $N/4$) generated by 3 or 5. One then uses a representation

$$\begin{aligned} k &= (-1)^{m_1} 5^{m_2} \\ k^* &= (-1)^{m_1^*} 5^{m_2^*} \end{aligned}$$

and the reindexed core matrix gives rise to a two-dimensional convolution. The latter may be carried out by means of two 2D DFTs on $2 \times (N/4)$ points.

1.3.3.2.4. The Winograd algorithms

The cyclic convolutions generated by Rader's multiplicative reindexing may be evaluated more economically than through DFTs if they are re-examined within a new algebraic setting, namely the theory of congruence classes of polynomials [see, for instance, Blahut (1985), Chapter 2; Schroeder (1986), Chapter 24].

The set, denoted $\mathbb{K}[X]$, of polynomials in one variable with coefficients in a given field $\mathbb{K}$ has many of the formal properties of the set $\mathbb{Z}$ of rational integers: it is a *ring* with no zero divisors and has a *Euclidean algorithm* on which a theory of divisibility can be built.

Given a polynomial $P(z)$, then for every $W(z)$ there exist unique polynomials $Q(z)$ and $R(z)$ such that

$$W(z) = P(z)Q(z) + R(z)$$

and

$$\text{degree } (R) < \text{degree } (P).$$

$R(z)$ is called the *residue* of $H(z)$ modulo $P(z)$. Two polynomials $H_1(z)$ and $H_2(z)$ having the same residue modulo $P(z)$ are said to be *congruent* modulo $P(z)$, which is denoted by