THE FFT OF THE SYMMETRIC GROUP OVER FINITE FIELDS

JACKSON WALTERS

$$K = \mathbb{F}_q, \qquad \operatorname{char}(K) = p > n.$$

In this range $K[S_n]$ is semisimple and split, so the ordinary representation-theoretic Fourier transform is available over K.

For each partition $\lambda \vdash n$, let

$$\rho_\lambda : S_n \to \mathrm{GL}_{d_\lambda}(K)$$

be Young's seminormal irreducible representation, where d_λ is the number of standard Young tableaux of shape λ. For

$$f = \sum_{g \in S_n} f(g) g \in K[S_n],$$

the Fourier transform is the block family

$$\widehat{f}(\lambda) = \sum_{g \in S_n} f(g) \rho_\lambda(g) \in M_{d_\lambda}(K), \qquad \lambda \vdash n.$$

Equivalently,

$$K[S_n] \cong \bigoplus_{\lambda \vdash n} M_{d_\lambda}(K).$$

The FFT uses the subgroup chain

$$S_1 \leq S_2 \leq \cdots \leq S_n$$

and the multiplicity-free branching rule

$$\rho_\lambda \downarrow_{S_{n-1}} \cong \bigoplus_{\mu \nearrow \lambda} \rho_\mu.$$

Writing

$$f = \sum_{j=1}^{n} g_{j,n} f_j, \qquad f_j \in K[S_{n-1}],$$

with $g_{j,n} = (j \ j+1 \ \cdots \ n)$, the transform satisfies

$$\widehat{f}(\lambda) = \sum_{j=1}^{n} \rho_\lambda(g_{j,n}) \left(\bigoplus_{\mu \nearrow \lambda} \widehat{f_j}(\mu) \right).$$

Young's seminormal form makes the adjacent transposition matrices sparse, so the products by $\rho_\lambda(g_{j,n})$ can be applied as products of sparse matrices.

The inverse transform is Fourier inversion:

$$f(g) = \frac{1}{|S_n|} \sum_{\lambda \vdash n} d_\lambda \operatorname{tr}\Big(\rho_\lambda(g^{-1}) \widehat{f}(\lambda)\Big).$$

Since $p > n$, the scalar $|S_n| = n!$ is invertible in K. The inverse FFT uses the same branching structure in reverse: shift each block by $\rho_\lambda(g_{j,n}^{-1})$, project to the μ-blocks appearing in $\rho_\lambda \downarrow_{S_{n-1}}$, rescale by the appropriate dimension factor, and recurse down the subgroup chain.

For group algebra multiplication, if

$$v, w \in K[S_n],$$

their product is the convolution

$$(vw)(x) = \sum_{gh=x} v(g)w(h).$$

The Fourier transform converts convolution into blockwise matrix multiplication:

$$\widehat{vw}(\lambda) = \widehat{v}(\lambda)\widehat{w}(\lambda), \qquad \lambda \vdash n.$$

Thus fast multiplication is computed by

$$vw = \mathrm{FFT}^{-1}\left(\left(\widehat{v}(\lambda)\widehat{w}(\lambda)\right)_{\lambda \vdash n}\right).$$

This is the nonabelian analogue of polynomial multiplication by FFT: transform, multiply pointwise/blockwise, then apply the inverse transform.