Characters and the Discrete Fourier Transform

The most important quantum algorithm is the *Discrete Fourier transform* (DFT). There are two reasons for this:

- DFT is exponentially faster for quantum computers than for classical computers;
- DFT allows (among other things) to factorize of natural numbers.

The discrete Fourier deals with the mappings from a finite commutative group G to $\mathbb{C}$. Any such mapping f can be understood as a vector $(f(g_1), f(g_2), \dots, f(g_n))$, where $n = |G|$ and g_i are elements of G. The set of all mappings thus forms the vector space $\mathbb{C}^n$, and the base to which the notation relates is the basis of the characteristic functions of individual elements, i.e. the functions $b_1, b_2, \dots, b_n$ defined by the relation $b_i(g_j) = \delta_{ij}$ (where "the Kronecker delta" δ_{ij} is equal to 1 or 0 according to whether $i = j$ or not).

DFT is a transition from a " chronological " notation of a function in this base, to a notation in the base of the so-called group of *characters* G, which expresses the "frequency" decomposition of a function. To understand DFT, it is therefore necessary to first discuss characters of finite groups.

Let $(G, \cdot)$ be a commutative group. Each group homomorphism

$$\chi : (G, \cdot) \to (\mathbb{C}, \cdot)$$

is called a *character* of the group G. We shall further consider only finite groups G.

Characters also form a group, with multiplication defined by

$$(\chi_1 \cdot \chi_2)(g) = \chi_1(g) \cdot \chi_2(g).$$

The unit element of this group of characters is the identical one, which we denote by ε and we call it the *trivial* character.

Theorem. Let X be the group of characters of a finite commutative group G. Then

$$X \cong G.$$

Proof. Because G is finite, all its elements must be mapped to a unit circle. More precisely, the g element must be mapped to the r-th root of 1, where r is the order of g. So we have

$$\chi(g) = \exp\left[2\pi i \frac{k}{r}\right],$$

for some $k \in \mathbb{Z}_r$.

Let $\{h_1, \dots, h_m\}$ be some minimal set of generators of the group G, where h_j has order r_j. Then

$$G \cong \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \cdots \times \mathbb{Z}_{r_m}$$

and the character χ is determined by the choice of

$$(k_1, \dots, k_m) \in \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \cdots \times \mathbb{Z}_{r_m}$$

such that

$$\chi(h_j) = \exp\left[2\pi i \frac{k_j}{r_j}\right].$$

It is easy t see that the mapping $\chi \mapsto (k_1, \dots, k_m)$ yields the required isomorphism. □

Since we move on a unit circle, we have

$$\chi^{-1}(g) = \chi(g)^{-1} = \chi(g)^*.$$

It is also useful to note that for $g, h \in \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \cdots \times \mathbb{Z}_{r_m}$ we have

$$\chi_h(g) = \chi_g(h).$$

Indeed, bth sides are equal to

$$\exp\left[2\pi i \sum_{j=1}^{m} \left(\frac{k_j \ell_j}{r_j}\right)\right], \tag{$\diamond$}$$

where $g = (k_1, k_2, \dots, k_m)$ a $h = (\ell_1, \ell_2, \dots, \ell_m)$.

The following statement is crucial for computation with characters.

Lemma. For any non-trivial character χ of the group G we have

$$\sum_{g \in G} \chi(g) = 0.$$

Proof. Let χ be nontrivial, and choose $h \in G$ such that $\chi(h) \neq 1$. Since $g \mapsto hg$ is a permutation of the group G, we have

$$\sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg) = \chi(h) \sum_{g \in G} \chi(g),$$

hence

$$\sum_{g \in G} \chi(g) = 0.$$

□

The following statement shows that characters form an orthogonal set with respect to the standard scalar product (so we work in the Hilbert space $\mathbb{H}_n$, not only in $\mathbb{C}_n$).

Lemma. Let χ_1 a χ_2 be two distinct characters of the group G. Then

$$\sum_{g \in G} \chi_1(g)^* \chi_2(g) = 0.$$

Proof. Since $\chi_1 \neq \chi_2$, the character $\chi_1^* \chi_2 = \chi_1^{-1} \chi_2$ is nontrivial, and the claim follows from the previous lemma. □

The norm of each character χ is

$$\sqrt{\sum_{g \in G} \chi(g)^* \chi(g)} = \sqrt{n}.$$

We then see that the set

$$\left(\frac{1}{\sqrt{n}}\chi_1, \frac{1}{\sqrt{n}}\chi_2, \dots, \frac{1}{\sqrt{n}}\chi_n\right)$$

is an orthonormal basis of $\mathbb{H}_n$, which we call the *basis of characters*.

As mentioned at the beginning, the Discrete Fourier Transform is the conversion of the representation $f : G \to \mathbb{C}$ from the notation in the basis of characteristic functions to the notation in the basis of characters. Because both bases are orthonormal, the operator is unitary. The DFT matrix is thus the inverse of the transition matrix from the canonical basis to the basis of characters. Since the inverse matrix of a unitary matrix is its adjoint matrix, we have

$$[\mathrm{DFT}]_{k,\ell} = \frac{1}{\sqrt{n}} \chi_{g_k}(g_\ell)^*,$$

where $g_1, g_2, \ldots, g_n$ is some numbering of elements of the group G. Due to the interchangeability of indices shown above, the DFT and DFT^{-1} are complex conjugate, and we usually considered the inverse transformation IFT to simplify the notation (this allows to omit minus signs in the exponent).