Quantum decomposition of the Discrete Fourier Transform

Quantum realization of the Discrete Fourier Transform consists in the construction of the circuit calculating the DFT operator, i.e. in the decomposition of DFT into small operators.

We have defined the DFT for a general group G. The most important and most common is the DFT for the cyclic group $(\mathbb{Z}_N, +)$, and unless explicitly stated otherwise, the term DFT means this case.

To illustrate the concept and to become familiar with it, however, we first perform the DFT on the group $(\mathbb{Z}_2^m, +)$. We have $M = 2^m$. The k-th - basis element of $\mathbb{H}_M$ is as usual denoted by $|k\rangle = |k_1 k_2 \dots k_m\rangle$, where $k_1 k_2 \dots k_m$ is a binary expansion of k. We will also assume that the numbering of the group $\mathbb{Z}_2^m$ corresponds to this notation, so that the k-th element is just $(k_1, k_2, \dots, k_m)$.

According to $(\diamond)$ we then have

$$[\mathrm{DFT}]_{k,\ell} = \frac{1}{\sqrt{2^m}} \exp\left[-2\pi i \sum_{j=1}^{m} \frac{k_j \ell_j}{2}\right] = \frac{1}{\sqrt{2^m}} (-1)^{\sum_{j=1}^{m} k_j \ell_j} = \frac{1}{\sqrt{2^m}} (-1)^{k\cdot\ell}.$$

However, this is a matrix we already know from the Deutsch-Jozsa algorithm above; over $\mathbb{Z}_2^m$ we therefore get an easy decomposition

$$\mathrm{DFT} = H^{\otimes m}.$$

Let us now turn to the case $(\mathbb{Z}_M, +)$. We will use the remark at the end of the previous section and decompose IFT, where

$$[\mathrm{IFT}]_{k,\ell} = \frac{1}{\sqrt{M}} \exp\left[2\pi i \frac{k\ell}{M}\right].$$

he circuit is always defined on the basis elements. So we want to construct a circuit that maps the input $|k\rangle = |k_1\rangle|k_2\rangle \cdots |k_m\rangle$ to:

$$|k\rangle \mapsto \frac{1}{\sqrt{M}} \sum_{\ell=0}^{M-1} \exp\left[2\pi i \frac{k\ell}{M}\right] |\ell\rangle,$$

which after the decomposition

$$|\ell\rangle = \bigotimes_{j=1}^{m} |\ell_j\rangle, \qquad \frac{\ell}{M} = \sum_{j=1}^{m} \frac{\ell_j}{2^j}$$

yields

$$|k\rangle \mapsto \frac{1}{\sqrt{M}} \sum_{\ell_1=0}^{1} \sum_{\ell_2=0}^{1} \cdots \sum_{\ell_m=0}^{1} \bigotimes_{j=1}^{m} \exp\left[2\pi i \frac{k}{2^j} \ell_j\right] |\ell_j\rangle.$$

This can be decomposed as the product of m sums of two terms

$$|k\rangle \mapsto \frac{1}{\sqrt{M}} \bigotimes_{j=1}^{m} \sum_{\ell_j=0}^{1} \exp\left[2\pi i \frac{k}{2^j} \ell_j\right] |\ell_j\rangle = \bigotimes_{j=1}^{m} \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left[2\pi i \frac{k}{2^j}\right] |1\rangle\right).$$

The factor at $|1\rangle$ can be expanded as:

$$\exp\left[2\pi i \frac{k}{2^j}\right] = \exp\left[2\pi i \frac{\sum_{t=1}^{m} 2^{m-t} k_t}{2^j}\right] = \exp\left[2\pi i \sum_{t=1}^{m} 2^{(m-t-j)} k_t\right]$$

and from the periodicity of the exponential function we get

$$\exp\left[2\pi i\frac{k}{2^j}\right] = \exp\left[2\pi i\sum_{t=m-j+1}^{m} 2^{(m-t-j)}k_t\right]$$

To make the notation more readable, it is convenient to extend the binary expansion even beyond the decimal (or rather “binary”) dot, and write

$$0, a_1a_2\cdots = \sum_j \frac{a_j}{2^j}.$$

The IFT can then be expressed as:

$$|k\rangle \mapsto \quad \frac{|0\rangle + \exp\left[2\pi i(0,k_m)\right]|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + \exp\left[2\pi i(0,k_{m-1}k_m)\right]|1\rangle}{\sqrt{2}} \otimes \cdots$$
$$\otimes \frac{|0\rangle + \exp\left[2\pi i(0,k_2\cdots k_{m-1}k_m)\right]|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + \exp\left[2\pi i(0,k_1\cdots k_{m-1}k_m)\right]|1\rangle}{\sqrt{2}}.$$

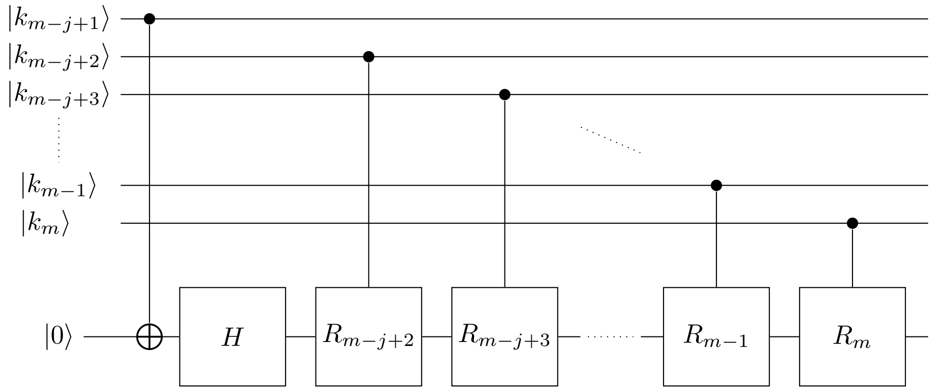
It is no more difficult to construct a circuit computing the IFT. First note that

$$\frac{|0\rangle + \exp\left[2\pi i(0,a)\right]|1\rangle}{\sqrt{2}} = H|a\rangle,$$

where H is the Hadamard operator. Moreover, we need the relative phase shift matrices

$$R_t = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^t} \end{pmatrix},$$

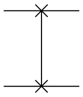
which we apply controlled by the bit on the t-th position beyond the “binary” dot. The construction of the j-th output qubit now looks like this:



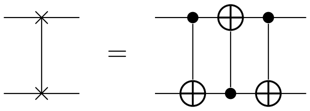
It is enough to use m auxiliary qubits, initially in the state $|0\rangle$, as the output register of the transformation.

However, it is also possible to save auxiliary qubits if we notice that the first qubit of the input is needed only to calculate the n-th output qubit, the second qubit of the input only to calculate the last two output qubits, etc. Using this observation we can start with the first qubit of the output, and thus gradually construct in the j-th input qubit the j-th output counted from the back.

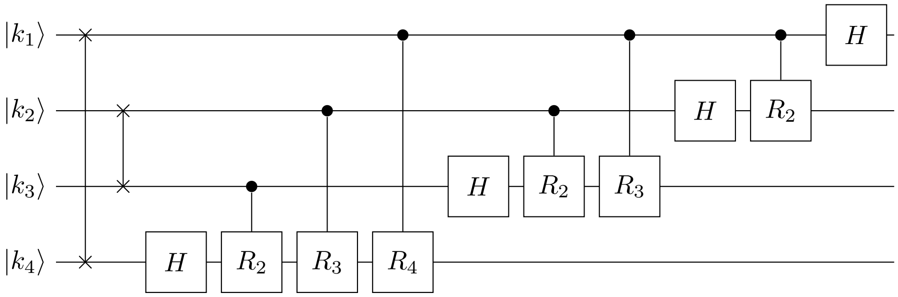
We then get the Fourier transform "upside down", which is certainly not a serious problem. If we also want to remove this inaccuracy, just reverse the order of the input qubits at the beginning using $\left\lfloor \frac{m}{2} \right\rfloor$ transpositions. The transposition of base qubits is, of course, unitary (like any permutation), it is denoted as



and it is easy to see that



The whole IFT circuit for $\mathbb{Z}_{2^4}$ is shown in the following picture.



It is obvious that the complexity of the algorithm (number of gates) is $\mathcal{O}(m^2) = \mathcal{O}(\ log^2 M)$. The fastest classical algorithm, the so-called *fast Fourier transform*, has complexity of $\mathcal{O}(M \log M)$. In this case, therefore, quantum computers bring exponential speed up.