Mathematics of Quantum Computation IV v2

Wim van Dam
Department of Computer Science, University of California at Santa Barbara, Santa Barbara, CA 93106-5110, USA

Notes for the graduate course "Quantum Computation and Quantum Information" (290A), Spring 2005. v1

Quantum Fourier Transformation modulo N: Consider the N dimensional state space where the basis states are the integers modulo N. (In computer science this group is often denoted by $\mathbb{Z}_N$, although it is more correct to write $\mathbb{Z}/N\mathbb{Z}$ or $\mathbb{Z}/(N)$ or $\mathbb{Z}/N$.) The quantum Fourier transform (QFT) over $\mathbb{Z}_N$ is the unitary transformation defined by

$$\text{Four}_N : |x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y\in\mathbb{Z}_N} \mathrm{e}^{2\pi\mathrm{i}xy/N} |y\rangle,$$

for all $x \in \mathbb{Z}_N$. From now on we use the definition $\zeta := \mathrm{e}^{2\pi\mathrm{i}/N}$, such that

$$\sum_{x\in\mathbb{Z}_N} \zeta^{dx} = \begin{cases} N & \text{if } d=0 \\ 0 & \text{otherwise.} \end{cases}$$

By its definition, the matrix representation of the Fourier transformation is

$$\text{Four}_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta & \zeta^2 & \cdots & \zeta^{N-1} \\ 1 & \zeta^2 & \zeta^4 & \cdots & \zeta^{2N-2} \\ \vdots & \vdots & & \ddots & \vdots \\ 1 & \zeta^{N-1} & \zeta^{2N-2} & \cdots & \zeta^{(N-1)(N-1)} \end{pmatrix},$$

or, much more succinct,

$$\text{Four}_N = \tfrac{1}{\sqrt{N}} \sum_{x,y\in\mathbb{Z}_N} \zeta^{xy} |y\rangle\langle x|.$$

The Hermitian conjugate of Four_N is

$$\text{Four}_N^\dagger = \tfrac{1}{\sqrt{N}} \sum_{x',y'\in\mathbb{Z}_N} \zeta^{-x'y'} |x'\rangle\langle y'|,$$

which allows to prove the unitarity of $\text{Four}_N \in \mathbb{C}^{N\times N}$ by (using $|y'\rangle\langle y| = 1$ if $y'=y$ and $|y'\rangle\langle y| = 0$ otherwise)

$$\begin{aligned} \text{Four}_N^\dagger \cdot \text{Four}_N &= \frac{1}{N}\left(\sum_{x',y'\in\mathbb{Z}_N} \zeta^{-x'y'}|x'\rangle\langle y'|\right)\left(\sum_{x,y\in\mathbb{Z}_N}\zeta^{xy}|y\rangle\langle x|\right) \\ &= \frac{1}{N}\left(\sum_{x',y',x,y\in\mathbb{Z}_N} \zeta^{-x'y'+xy}|x'\rangle\langle y'||y\rangle\langle x|\right) \\ &= \frac{1}{N}\left(\sum_{x',x,y\in\mathbb{Z}_N} \zeta^{(x-x')y}|x'\rangle\langle x|\right) \\ &= \frac{1}{N}\left(\sum_{x',x\in\mathbb{Z}_N}\left(\sum_{y\in\mathbb{Z}_N}\zeta^{(x-x')y}\right)|x'\rangle\langle x|\right) \\ &= \frac{1}{N}\left(\sum_{x\in\mathbb{Z}_N} N|x\rangle\langle x|\right) \\ &= I. \end{aligned}$$

Efficient Implementation of Four_N To be able to use the Fourier transform as part of an efficient quantum computation we have to show that it can be implemented (approximately) with a quantum circuit of size $O(\text{poly}(\log N))$. For $N = 2^n$, the transformation can be implemented as follows.

Each number $x \in \mathbb{Z}_N$ is represented by n bits $x_0, x_1, \ldots, x_{n-1}$ such that for example $y = \sum_{j=0}^{n-1} y_j 2^j$. The Fourier transform of $x \in \mathbb{Z}_N$ can then be written as the tensor product of n qubits:

$$\begin{aligned} \text{Four}_N : |x\rangle &\mapsto \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} \mathrm{e}^{2\pi\mathrm{i}x(\sum_{j=0}^{n-1} y_j 2^j)/2^n} |y_0,\ldots,y_{n-1}\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} \bigotimes_{j=0}^{n-1} \mathrm{e}^{2\pi\mathrm{i}xy_j2^j/2^n} \left|y_j\right\rangle \\ &= \frac{1}{\sqrt{2^n}} \bigotimes_{j=0}^{n-1} \sum_{y_j\in\{0,1\}} \mathrm{e}^{2\pi\mathrm{i}xy_j2^j/2^n} \left|y_j\right\rangle \\ &= \bigotimes_{j=0}^{n-1} \tfrac{1}{\sqrt{2}}(|0\rangle_j + \mathrm{e}^{2\pi\mathrm{i}x2^j/2^n}|1\rangle_j) \\ &= \bigotimes_{j=0}^{n-1} \tfrac{1}{\sqrt{2}}(|0\rangle_j + \mathrm{e}^{2\pi\mathrm{i}\sum_{k=0}^{n-1}x_k2^{k+j-n}}|1\rangle_j) \\ &=: \bigotimes_{j=0}^{n-1} \left|z_j\right\rangle, \end{aligned}$$

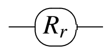
where the subscript in $|b\rangle_j$ indicates position of the j-th qubit. Now, because $\exp(2\pi\mathrm{i}\cdot x_k 2^s) = 1$ for all integer $s \geq 0$, we see that the j-th output qubit z_j is in fact

$$\left|z_j\right\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle_j + \mathrm{e}^{2\pi\mathrm{i}(x_0 2^{j-n} + x_1 2^{j+1-n} + \cdots + x_{n-1-j}2^{-1})}|1\rangle_j),$$

and hence only depends on the $n-j$ input bits $x_0,\ldots,x_{n-1-j}$.

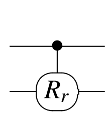
To describe a quantum circuit that implements the Fourier transform, we define the single phase rotations

$$R_r = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{2\pi\mathrm{i}/2^r} \end{pmatrix} \quad \simeq$$



and the two qubit, Controlled-R_r rotation with $C\text{-}R_r\,|a,b\rangle \mapsto \mathrm{e}^{2\pi\mathrm{i}ab/2^r}\,|a,b\rangle$ for $a,b \in \{0,1\}$ such that

$$C\text{-}R_r = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \mathrm{e}^{2\pi\mathrm{i}/2^r} \end{pmatrix} \quad \simeq$$



The circuit (of size $O(n^2)$) on the next page uses these gates in combination with n Hadamard gates to implement the quantum Fourier transform over $\mathbb{Z}_{2^n}$.

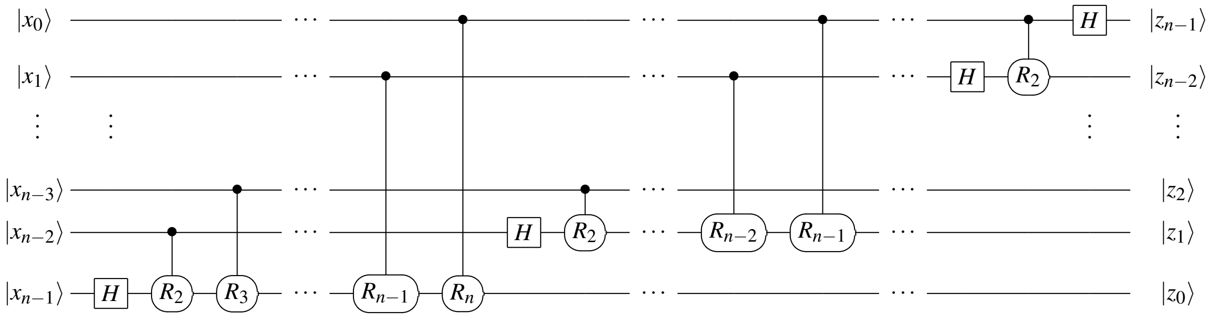


FIG. 1: Circuit for Quantum Fourier Transform
Schematic overview of an efficient (size $O(n^2)$) implementation of a quantum Fourier transformation over the group $\mathbb{Z}_{2^n}$. Note how the order of the n output bits $z_0, \ldots, z_{n-1}$ is reversed in comparison with the order of the input bits $x_0, \ldots, x_{n-1}$.

For more information, see Sections 5–5.1 in Nielsen and Chuang's *Quantum Computation and Quantum Information.*