A presentation of the quantum Fourier transform from a recursive viewpoint

Gloria Paradisi

Notes from a talk by Prof. Hugues Randriam
October 21, 2004

In most introductory texts to quantum computation, such as [ChNi] or [Pres], the presentation of the quantum Fourier transform relies on the derivation of an explicit formula, which is then translated into a quantum circuit. The connection with the classical fast Fourier transform is also cited, but not explicited, or left as an exercise.

In this note we construct a quantum Fourier transform circuit in a recursive way, by directly copying the construction of the fast Fourier transform algorithm that is given, for example, in [CLRS], chapter 30. We do not pretend this presentation to be original, nor claim for any anteriority. The aim of this paper is purely pedagogical.

The author would like to thank Prof. Hugues Randriam for his supervision of the writing of this text.

1 The fast Fourier transform

Let n be an integer and $N = 2^n$. The discrete Fourier transform associates to each complex N-tuple $a = (a_0, \ldots, a_{N-1})$ the complex N-tuple $b = (b_0, \ldots, b_{N-1})$ with

$$b_k = 2^{-n/2} \sum_{j=0}^{N-1} \zeta_n^{jk} a_j \tag{1}$$

where

$$\zeta_n = e^{\frac{2i\pi}{2^n}} \tag{2}$$

is a primitive N-th root of 1.

Thus, apart from some power of $\sqrt{2}$, the discrete Fourier transform amounts to evaluating the polynomial

$$P(X) = \sum_{j=0}^{N-1} a_j X^j, \tag{3}$$

of degree $2^n - 1$, at the powers of ζ_n. The fast Fourier transform algorithm performs this using a *divide and conquer* strategy. Obviously P can be written in a unique way

$$P(X) = P_{even}(X^2) + X P_{odd}(X^2). \tag{4}$$

In this decomposition the degree of P_{even} (resp. P_{odd}) is $2^{n-1} - 1$, and its coefficients are the a_j for even (resp. odd) j's. Using the fact that $\zeta_n^2 = \zeta_{n-1}$, one gets

$$P(\zeta_n^k) = P_{even}(\zeta_{n-1}^k) + \zeta_n^k P_{odd}(\zeta_{n-1}^k). \tag{5}$$

Thus, to perform a Fourier transform of order n, one has to perform *two* Fourier transforms of order $n-1$, and then $O(n)$ additions and multiplications. We will summarize this as

$$FFT_n = 2.FFT_{n-1} + O(n) \tag{6}$$

which finally gives us that the total number of elementary operations required grows as

$$FFT_n = O(n2^n). \tag{7}$$

2 The quantum Fourier transform

As we just saw, the exponential factor 2^n in the complexity of the fast Fourier transform algorithm comes from the factor 2 in equation (6), that is, from the fact that the computation of a Fourier transform of order n requires *two* Fourier transforms of order $n-1$. Hopefully this factor 2 could be shrunk down to 1 using quantum parallelism. Indeed, recall that when one has a quantum circuit F acting on $n-1$ qubits, then the circuit $F \otimes \mathbf{1}$ (see figure 1 below) on n qubits, applied to a vector $|x\rangle = |x_0\rangle|0\rangle + |x_1\rangle|1\rangle$, gives as output $(F|x_0\rangle)|0\rangle + (F|x_1\rangle)|1\rangle$, thus, in some way, computing simultaneously $F|x_0\rangle$ and $F|x_1\rangle$ at the cost of only *one* application of F. Carrying this out succesfully will lead to a dramatic decrease of complexity in the adaptation

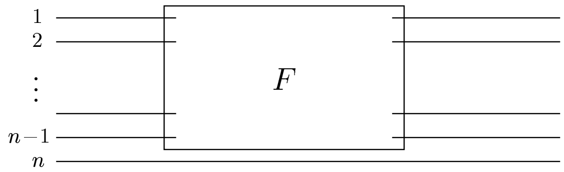


Figure 1: constructing $F \otimes \mathbf{1}$ out of F

of the Fourier transform from the classical world to the quantum world: from an exponential complexity we will get to a quadratic one.

To make it formally, consider an n qubits system, and denote the vectors of the computational basis by

$$|j\rangle = |j_1\rangle \dots |j_{n-1}\rangle|j_n\rangle, \tag{8}$$

for $j \in \{0, \dots, N-1\}$ (recall that $N = 2^n$) with base 2 expansion

$$j = j_1 2^{n-1} + \dots + j_{n-1}2 + j_n. \tag{9}$$

We will construct a quantum circuit which sends the unitary vector $\sum_j a_j|j\rangle$ to $\sum_k b_k|k\rangle$ where the b_k's are deduced from the a_j's by relation (1). Remark that, since quantum circuits can only perform unitary transformations, this implies that formula (1) is norm preserving. Although this fact is well known (Parseval's theorem), we will not need to assume it. Indeed our construction can be considered as a way of re-proving it.

Now let

$$|P\rangle = \sum_{j=0}^{N-1} a_j|j\rangle. \tag{10}$$

Grouping together terms according to $j_n = 0$ (that is, j even) or $j_n = 1$ (that is, j odd) we get a decomposition

$$|P\rangle = |P_{even}\rangle|0\rangle + |P_{odd}\rangle|1\rangle, \tag{11}$$

which is the exact analogue of decomposition (4).

According to formula (5), we have then to perform a Fourier transform on the first $n-1$ qubits, which can be done as in figure 1. In doing that one has however to be careful on the ordering of the output qubits. Indeed, write

$$k = k_1 2^{n-1} + k_2 2^{n-2} + \dots + k_{n-1}2 + k_n. \tag{12}$$

Then, as $\zeta_{n-1}^{2^{n-1}} = 1$ and $\zeta_n^{2^{n-1}} = -1$, formula (5) can be re-writen as

$$P(\zeta_n^k) = P_{even}(\zeta_{n-1}^{k'}) + (-1)^{k_1}\zeta_n^{k'} P_{odd}(\zeta_{n-1}^{k'}) \tag{13}$$

where

$$k' = k_2 2^{n-2} + \cdots + k_{n-1}2 + k_n. \tag{14}$$

Thus, while $|P_{even}\rangle$ and $|P_{odd}\rangle$ are vector states of the *first* $n-1$ qubits $j_1, \ldots, j_{n-1}$, their Fourier transforms should be output on the *last* $n-1$ qubits $k_2, \ldots, k_n$. To circumvent this difficulty we will consider a *modified* quantum Fourier transform, $mQFT$, which reverses the order of the output qubits. Obviously this is not a serious problem, since the correct order can then be restablished using only $n/2$ swap gates.

Our modified quantum Fourier transform circuit of order n should then look like:

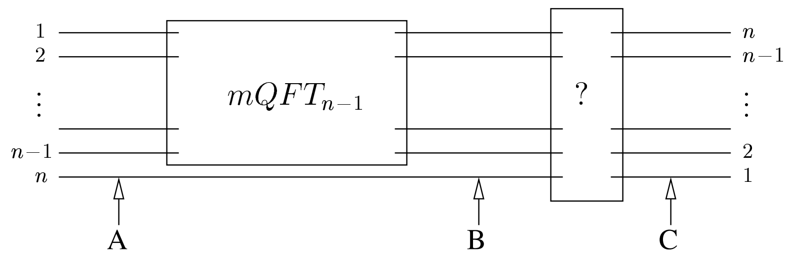


Figure 2: recursive scheme for $mQFT_n$.

At point A we input the vector

$$|P\rangle = |P_{even}\rangle|0\rangle + |P_{odd}\rangle|1\rangle, \tag{15}$$

so that at point B we get

$$|\widetilde{P_{even}}\rangle|0\rangle + |\widetilde{P_{odd}}\rangle|1\rangle, \tag{16}$$

where we denoted by $\tilde{\cdot}$ the effect of our (modified) quantum Fourier transform. According to formula (13) we have

$$P(\zeta_n^k) = \begin{cases} P_{even}(\zeta_{n-1}^{k'}) + \zeta_n^{k'} P_{odd}(\zeta_{n-1}^{k'}) & \text{for } k_1 = 0 \\ P_{even}(\zeta_{n-1}^{k'}) - \zeta_n^{k'} P_{odd}(\zeta_{n-1}^{k'}) & \text{for } k_1 = 1 \end{cases} \tag{17}$$

so that, putting the $2^{-n/2}$ back, at point C we should get

$$(18)\qquad |\widetilde{P}\rangle = \frac{1}{\sqrt{2}}(|\widetilde{P_{even}}\rangle + \zeta_n^{k'}|\widetilde{P_{odd}}\rangle)|0\rangle + \frac{1}{\sqrt{2}}(|\widetilde{P_{even}}\rangle - \zeta_n^{k'}|\widetilde{P_{odd}}\rangle)|1\rangle,$$

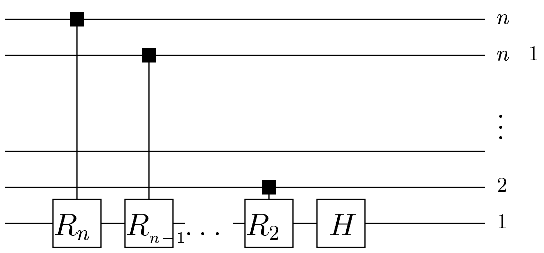
where $\zeta_n^{k'}$ can be understood as the diagonal matrix acting on the first $n-1$ qubits by multiplying $|k'\rangle$ by $\zeta_n^{k'}$, or equivalently as the controlled operation that multiplies the last qubit by $\zeta_n^{k'}$ when the first $n-1$ qubits are set to $|k'\rangle$.

Clearly one can go from (16) to (18) by sending $|0\rangle$ to $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|1\rangle$ to $\frac{1}{\sqrt{2}}(\zeta_n^{k'}|0\rangle - \zeta_n^{k'}|1\rangle)$, that is by acting on the last qubit through

$$(19)\qquad \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & \zeta_n^{k'} \\ 1 & -\zeta_n^{k'} \end{bmatrix} = HR_2^{k_2}\dots R_{n-1}^{k_{n-1}}R_n^{k_n},$$

where $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ is the usual Hadamard matrix and $R_d = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2i\pi}{2^d}} \end{bmatrix}$.

This means that we can complete our quantum Fourier circuit by replacing the '?' circuit in figure 2 with



Thus we see that the (modified) quantum Fourier circuit of order n can be constructed from the order $n-1$ one by adding $n-1$ controlled operations and one Hadamard gate. Putting all together, since the quantum Fourier circuit of order 0 is trivial (the identity), we get a total complexity of $\frac{n(n+1)}{2}$ gates.

The reader will remark that the circuit we get is the inverse of the one that is given in [ChNi], figure 5.1. This is not a mistake: it only indicates that the Fourier transform is essentially its own inverse.

References

[ChNi] Chuang M., Nielsen I. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

[CLRS] Cormen T., Leiserson C., Rivest R., Stein C. *Introduction to Algorithms, Second Edition.* MIT Press, 2001.

[Pres] Preskill J. *Lecture Notes for Physics 229: Quantum Information and Computation.* Preprint, 1998.

Gloria Paradisi, c/o Hugues Randriam
Ecole nationale supérieure des télécommunications
46, rue Barrault
75634 Paris Cedex 13
France

Gloria.Paradisi@salle-s.org