Quantum Fourier Transforms

Burton Rosenberg

November 10, 2003

Fundamental notions

First, review and maybe introduce some notation. It's all about functions from G to $\mathbb{C}$. A vector is consider a function by the transform,

$$(c_j) \mapsto \sum_j c_j e_j$$

where the e_j, rather than standard unit vectors, are considered as functions,

$$e_j(k) = \begin{cases} 1 & j = k \\ 0 & \text{else} \end{cases}$$

The Fourier coefficients $\hat{c_j}$ are then the complex numbers for which,

$$\sum_j c_j e_j = \sum_j \hat{c_j} \chi_j / \sqrt{n}$$

where χ_j are the characters of G and n is the number of elements in G (this is also the number of distinct characters). The scale factor $1/\sqrt{n}$ is needed make the characters unit length and thereby insure that the Fourier transform is unitary.

A small amount of thought and it is clear that for $G = \mathbb{Z}_n$ the image of a character must be an n-th root of unity, and the map is determined by which n-th root of unity is the image of 1. We also have the short proof,

$$\sum_g \chi_i(g) = \sum_g \chi_i(g + a) = \chi_i(a) \sum_g \chi_i(g).$$

So if χ_i is not identically 1, the sum is 0. This can be used to show the orthogonality of characters, since $\langle \chi_i \,|\, \chi_j \rangle = \chi_i^* \cdot \chi_j = \sum_g \chi_k(g)$, and χ_k is trivial if and only if $i = j$.

Taking inner products against $\chi_k/\sqrt{n}$ in the two representations of the vector,

$$\begin{aligned} (\chi_k/\sqrt{n}) \cdot \sum_j \hat{c_j} \chi_j / \sqrt{n} &= \sum_j \hat{c_j} (\chi_k \cdot \chi_j)/n \\ &= \hat{c_k} \end{aligned}$$

which equals

$$\begin{aligned}(\chi_k/\sqrt{n}) \cdot \sum_j c_j e_j &= \sum_j c_j (\chi_k \cdot e_j)/\sqrt{n} \\ &= (1/\sqrt{n}) \sum_j c_j \chi_k(j)^*\end{aligned}$$

Using matrix notation,

$$(\hat{c_k}) = (1/\sqrt{n})[\chi_k(j)^*](c_j)$$

that is, row k gives value of $\chi_k(j)^*$ in column j. We derive the inverse transform by taking inner products against e_k,

$$\begin{aligned}e_k \cdot \sum_j c_j e_j &= \sum_j c_j (e_k \cdot e_j) \\ &= c_k\end{aligned}$$

and

$$\begin{aligned}e_k \cdot \sum_j \hat{c_j} \chi_j/\sqrt{n} &= \sum_j \hat{c_j} (e_k \cdot \chi_j)/\sqrt{n} \\ &= (1/\sqrt{n}) \sum_j \hat{c_j} \chi_j(k)\end{aligned}$$

written as a matrix,

$$(c_k) = (1/\sqrt{n})[\chi_j(k)](\hat{c_j})$$

Noting the reversal of the indices j and k, we have also shown that the inverse transform is the Hermetian transpose of the forward transform. So the transformation matrix is unitary.

This fast and loose claim of invertibility might need a bit more justification. Consider (c_j) transformed to $(\hat{c_j})$ and then back to (c'_j), for which we claim $c_j = c'_j$. Recall, that (c_j) and $(\hat{c_j})$ describe exactly the same vector, so that we can immediately claim (c_j) and (c'_j) at least describe the same vector. That $c_j = c'_j$ really depends upon the linear independence of the e_j. The reader is encouraged to review the linear algebra confirming this.

An example

As an example of the Fourier transform, the characters of $\mathbb{Z}_4$ are $\chi_k(j) = e^{2\pi ijk/4}$. Allowing that our matrix be written out starting the indexing at zero, the transformation matrix is,

$$[\chi_k(j)^*] = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix}$$

and the reverse transformation $(\hat{c_j}) \mapsto (c_j)$ is the Hermetian transpose of this matrix. For instance, the function $(1, 1, -1, -1)$ has Fourier transform $(0, 1-i, 0, 1+i)$. The reader should check that the function $(1/2)((1-i)\chi_1 + (1+i)\chi_3)$ has the proper values.

Periodicity and the Fourier transform

A function $f : \mathbb{Z}_n \to \mathbb{C}$ is *periodic* if there exists a period r such that $f(k+r) = f(k)$. Note that r must divide n. Periodic functions have limited amounts of information and the Fourier transform reflects this by having many zero coefficients. Precisely, $\hat{c_j}$ is non-zero only if j is a multiple of n/r. Here's the proof.

$$\begin{aligned}
\sqrt{n}\hat{f}(j) &= \sum_{k=0}^{n-1} e^{-2\pi ijk/n} f(k) \\
&= \sum_{k'=0}^{r-1} \sum_{k''=0}^{n/r-1} e^{-2\pi ij(k'+rk'')/n} f(k'+rk'') \\
&= \sum_{k'=0}^{r-1} f(k') e^{-2\pi ijk'/n} \sum_{k''=0}^{n/r-1} e^{-2\pi ijrk''/n}
\end{aligned}$$

Consider the second sum. By the assumption of divisibility, let $d = n/r$. The sum is therefore over all powers of the j-th power of the d-th roots of unity. If j/d is not an integer, this sum is zero. Else each term is 1 and the sum is n/r. Therefore,

$$\hat{f}(j) = \begin{cases} (\sqrt{n}/r) \sum_{k=0}^{r-1} f(k) e^{-2\pi ijk/n} & j = 0, n/r, 2n/r, \ldots \\ 0 & \text{else} \end{cases}$$

An example

For an easy example of periodicity, take a function f periodic with period 2, $f(k+2) = f(k)$. There are essentially only two values for this function $f(k)$ when k is even, and when k is odd. The non-zero fourier coefficients are at $j = 0$ and $j = n/2$. The only two characters involved are the trivial character and the character which alternates between 1 and -1. It is easy to see how to adjust their weights so as to combine these characters to equal the function f.

In general, when the periodicity of f implies that there are only d independent values for f then only d Fourier coefficients will be possibly non-zero. Another way to look at this, the periodicity of the characters with non-zero coefficients must be compatible to the periodicity of the function. It seems that this might give a better proof: take the fourier transform in $\mathbb{Z}_r$ of the r-periodic function and then transfer the coefficients using the embedding of the r-th roots of unity into the n-th roots of unity, when r divides n.

Quantum Fourier transform

Given the Fourier transform, we derive a quantum circuit. This essentially mean we give a bunch of two qubit unitary transformations laid out so as to perform the Fourier transformation. It turns

out that superposition lets us evaluate the Fourier transform using exponentially less circuitry than if done classically.

Since the Fourier transform is linear, we need only discuss the circuit for inputs of the form $|x\rangle$. General inputs of the form $\sum c_i|x\rangle$ are obtained by the superposition of basis states.

$$\mathcal{F}\,|x\rangle = \frac{1}{\sqrt{n}} \sum_{y=0}^{n-1} e^{-2\pi i x y/n} |y\rangle$$

We write this in a product form. Assume $n = 2^m$ and that we represent x and y as the tensor of qubits. Any $|y\rangle$ is of the form $|y'0\rangle$ or $|y'1\rangle$. We write the sums separately and factor over the tensor,

$$\begin{aligned}
\mathcal{F}\,|x\rangle &= \frac{1}{\sqrt{n}} \sum_{y'=0}^{2^{m-1}-1} e^{-\pi i x(2y')/2^{m-1}} |y'0\rangle + \frac{1}{\sqrt{n}} \sum_{y'=0}^{2^{m-1}-1} e^{-\pi i x(2y'+1)/2^{m-1}} |y'1\rangle \\
&= \frac{1}{\sqrt{n}} \sum_{y'=0}^{2^{m-1}-1} e^{-\pi i x y'/2^{m-2}} \otimes (|0\rangle + e^{-\pi i x/2^{m-1}}|1\rangle)
\end{aligned}$$

Continuing in this manner,

$$\begin{aligned}
\mathcal{F}\,|x\rangle &= \frac{1}{\sqrt{n}} \sum_{y'=0}^{2^{m-2}-1} e^{-\pi i x y'/2^{m-3}} \otimes (|0\rangle + e^{-\pi i x/2^{m-2}}|1\rangle) \otimes (|0\rangle + e^{-\pi i x/2^{m-1}}|1\rangle) \\
&\;\;\vdots \\
&= \frac{1}{\sqrt{n}} (|0\rangle + e^{-\pi i x}|1\rangle) \otimes (|0\rangle + e^{-\pi i x/2}|1\rangle) \otimes \ldots \otimes (|0\rangle + e^{-\pi i x/2^{m-1}}|1\rangle)
\end{aligned}$$

To express this as the tensor of qubits $y_{m-1} \otimes y_{m-2} \otimes \ldots \otimes y_0$ we set,

$$y_l = \frac{1}{\sqrt{2}} (|0\rangle + e^{-\pi i x/2^{m-l-1}}|1\rangle)$$

The coefficient of the $|1\rangle$ in y_l factors by expanding $x = \sum x_k 2^k$,

$$e^{-\pi i \sum x_k 2^k/2^{m-l-1}} = \prod_{k=0}^{m-1} e^{-\pi i x_k/2^{m-l-k-1}} = (-1)^{x_{m-l-1}} \prod_{\kappa=1}^{m-l-1} e^{-\pi i x_{m-l-1-\kappa}/2^\kappa}$$

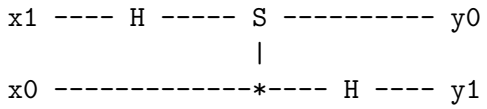
The quantum fourier recipe

1. Let $l' = m - l - 1$. Apply the Hadamard transform to $x_{l'}$, giving $(1/\sqrt{2})(|0\rangle + (-1)^{x_{l'}}|1\rangle)$.
2. For $\kappa = 1, 2, \ldots, l'$, if $x_{l'-\kappa}$ is 1, apply the phase shift $e^{-\pi i/2^\kappa}$ to the $|1\rangle$ component of the qubit.
3. Assign the result to qubit y_l.

Note that after collecting all m factors of $1/\sqrt{2}$ we will have the required scale factor $1/\sqrt{2^m}$.

An example

For the 2 qubit transform the circuit is,



Where H is the Hadamard transform, and S is a controlled phase shift by $-i$. That is, if its two inputs are 1, it outputs $-i$, else it outputs the first input. Also, by careful experiment, the controlled gate S should be,

$$S = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -i \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & S' \end{bmatrix}$$

Note the reversal of the order of the bits of y. We can put the bits in the usual order by applying the matrix,

$$R = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

So we need multiply,

$$\begin{aligned} R(I \otimes H)S(H \otimes I) &= (1/\sqrt{2})R \begin{bmatrix} H & 0 \\ 0 & H \end{bmatrix} \begin{bmatrix} I & 0 \\ 0 & S' \end{bmatrix} \begin{bmatrix} I & I \\ I & -I \end{bmatrix} \\ &= (1/\sqrt{2})R \begin{bmatrix} H & H \\ HS' & -HS' \end{bmatrix} \\ &= \frac{1}{2} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \\ 1 & i & -1 & -i \end{bmatrix} \\ &= \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix} \end{aligned}$$

Which is indeed the Fourier transform on $\mathbb{Z}_4$.

References

1. Mika Hirvensalo, *Quantum Computing*, Springer. 2001. 3–540–66783–0.

2. Michale Nielsen, Issac Chuang, *Quantum Computing and Quantum Information,* Cambridge. 2000. 0–521–63503–9.

3. Arthur Pittenger, *An Introduction to Quamtum Computing Algorithms,* Birkhauser. 2001. 3–7643–4127–0.

4. A. Kitaev, A. Shen, M. Vyalyi, *Classical and Quantum Computing,* AMS GSM Vol. 47. 2002. 0–8218–2161–X.