A Note on Computing Fourier Transforms by Quantum Programs

Richard Cleve
Department of Computer Science
University of Calgary
Calgary, Canada T2N 1N4
cleve@cpsc.ucalgary.ca

1994

For any positive integer q, let $Z_q = \{0, \ldots, q-1\}$ and define the unitary transformation A_q as

$$A_q(|x\rangle) = \frac{1}{\sqrt{q}} \sum_{y \in Z_q} \omega^{x \cdot y} |y\rangle,$$

for each $x \in Z_q$, where $\omega = e^{2\pi i/q}$.

A general goal is to simulate A_q, where q is an n-bit integer, by a quantum program of length polynomial in n. Shor (FOCS 94) shows how to do this when all of the prime factors of q are distinct and $O(\log n)$ bits. Presently, we show how to do this when the prime factors of q are *not necessarily distinct*, but each one is still $O(\log n)$ bits. A special case of this is when q is a power of 2.

We shall use the following as tools.

For any positive integers p and q, define the bijections E, $D : Z_{p \cdot q} \to Z_p \times Z_q$ as

$$E(|x\rangle) = |x \operatorname{div} q, x \bmod q\rangle$$

and

$$D(|x\rangle) = |x \bmod p, x \operatorname{div} p\rangle,$$

for each $x \in Z_{p \cdot q}$. By appealing to Bennett's work, both of the above transformations, as well as their inverses, can be computed by quantum programs of length polynomial in the number of bits in p and q.

For any positive integers p and q, and complex number ω with $|\omega| = 1$, define the unitary transformation $B^{\omega}_{(p,q)}$ as

$$B^{\omega}_{(p,q)}(|a, b\rangle) = \omega^{a \cdot b} |a, b\rangle,$$

for each $a \in Z_p$ and $b \in Z_q$. (Note that $B^{\omega}_{(p,q)}$ changes the phase but maintains the state.) We'll see how to efficiently simulate the $B^{\omega}_{(p,q)}$ later. Then our result will follow by recursively applying the following lemma.

Lemma 1: *For any positive integers p and q (they need not be relatively prime), and $\omega = e^{2\pi i/p \cdot q}$, the composition of transformations $D^{-1} \circ (I \otimes A_q) \circ B^{\omega}_{(p,q)} \circ (A_p \otimes I) \circ E$ has the same effect as $A_{p \cdot q}$. In the above, by $(A_p \otimes I)(|a, b\rangle)$, we mean apply A_p to the first argument, a, and, by $(I \otimes A_q)(|a, b\rangle)$, we mean apply A_q to the second argument, b.*

Proof: For any $x \in Z_{p \cdot q}$,

$$D^{-1} \circ (I \otimes A_q) \circ B^{\omega}_{(p,q)} \circ (A_p \otimes I) \circ E(|x\rangle) =$$

$$
\begin{aligned}
&= D^{-1} \circ (I \otimes A_q) \circ B^{\omega}_{(p,q)} \circ (A_p \otimes I)(|x \operatorname{div} q, x \bmod q\rangle) \\
&= D^{-1} \circ (I \otimes A_q) \circ B^{\omega}_{(p,q)} \left(\frac{1}{\sqrt{p}} \sum_{a \in Z_p} (\omega^q)^{a \cdot (x \operatorname{div} q)} |a, x \bmod q\rangle \right) \\
&= D^{-1} \circ (I \otimes A_q) \left(\frac{1}{\sqrt{p}} \sum_{a \in Z_p} \omega^{a \cdot q \cdot (x \operatorname{div} q)} \omega^{a \cdot (x \bmod q)} |a, x \bmod q\rangle \right) \\
&= D^{-1} \circ (I \otimes A_q) \left(\frac{1}{\sqrt{p}} \sum_{a \in Z_p} \omega^{a \cdot x} |a, x \bmod q\rangle \right) \\
&= D^{-1} \left(\frac{1}{\sqrt{p}} \frac{1}{\sqrt{q}} \sum_{a \in Z_p} \sum_{b \in Z_q} \omega^{a \cdot x} (\omega^p)^{b \cdot (x \bmod q)} |a, b\rangle \right) \\
&= D^{-1} \left(\frac{1}{\sqrt{p \cdot q}} \sum_{a \in Z_p} \sum_{b \in Z_q} \omega^{a \cdot x + p \cdot b \cdot x} |a, b\rangle \right) \\
&= D^{-1} \left(\frac{1}{\sqrt{p \cdot q}} \sum_{y \in Z_{p \cdot q}} \omega^{(y \bmod p) \cdot x + p \cdot (y \operatorname{div} p) \cdot x} |y \bmod p, y \operatorname{div} p\rangle \right) \\
&= D^{-1} \left(\frac{1}{\sqrt{p \cdot q}} \sum_{y \in Z_{p \cdot q}} \omega^{x \cdot y} |y \bmod p, y \operatorname{div} p\rangle \right) \\
&= \frac{1}{\sqrt{p \cdot q}} \sum_{y \in Z_{p \cdot q}} \omega^{x \cdot y} |y\rangle.
\end{aligned}
$$

□

Now, it remains to show that, for any positive integers p and q, and $\omega = e^{2\pi i / p \cdot q}$, $B^{\omega}_{(p,q)}$ can be simulated by a quantum program of length polynomial in the number of bits of p and q. A recursive construction follows immediately from the following lemma.

Lemma 2: *For any positive integers p, q, and r, and complex number ω with $|\omega| = 1$, the composition $(I \otimes E^{-1}) \circ (B^{\omega}_{(r,q)} \oslash I) \circ (B^{\omega^q}_{(r,p)} \otimes I) \circ (I \otimes E)$ has the same effect as $B^{\omega}_{(r,p \cdot q)}$. In the above, by $(B^{\omega}_{(r,q)} \oslash I)(|a, b, c\rangle)$, we mean apply $B^{\omega}_{(r,q)}$ to the first and third arguments, a and c.*

Proof: For any $x \in Z_r$ and $y \in Z_{p \cdot q}$,

$$
\begin{aligned}
&(I \otimes E^{-1}) \circ (B^{\omega}_{(r,q)} \oslash I) \circ (B^{\omega^q}_{(r,p)} \otimes I) \circ (I \otimes E)(|x, y\rangle) \\
&= (I \otimes E^{-1}) \circ (B^{\omega}_{(r,q)} \oslash I) \circ (B^{\omega^q}_{(r,p)} \otimes I)(|x, y \operatorname{div} q, y \bmod q\rangle) \\
&= (I \otimes E^{-1}) \circ (B^{\omega}_{(r,q)} \oslash I) \left((\omega^q)^{x \cdot (y \operatorname{div} q)} |x, y \operatorname{div} q, y \bmod q\rangle \right) \\
&= (I \otimes E^{-1}) \left(\omega^{x \cdot q \cdot (y \operatorname{div} q)} \omega^{x \cdot (y \bmod q)} |x, y \operatorname{div} q, y \bmod q\rangle \right) \\
&= (I \otimes E^{-1}) \left(\omega^{x \cdot y} |x, y \operatorname{div} q, y \bmod q\rangle \right) \\
&= \omega^{x \cdot y} |x, y\rangle.
\end{aligned}
$$

□