The Complexity of Quantum Fourier Transforms and Integer Multiplication*.

Graeme Ahokas[1 †] Richard Cleve[1 ‡] Lisa Hales[2 §]

[1] *Department of Computer Science*
University of Calgary
Calgary, Alberta, Canada T2N 1N4
[2] *Department of Computer Science, U.C. Berkeley*
California, U.S.A

Abstract. We consider the minimum number of gates necessary to compute an approximation of the quantum Fourier transform (QFT) modulo 2^n with precision $1/n^{O(1)}$. We give an upper bound of $O(n(\log\log n)^2 \log\log\log n)$, which is an improvement over previous bounds that are $O(n\log n)$. We also show that if there exist circuits of size $o(n\log n\log\log n)$ performing the QFT for arbitrary n-bit moduli then there exist quantum circuits of size $o(n\log n\log\log n)$ for integer multiplication—smaller than the Schönhage-Strassen bound.

Keywords: quantum algorithms, quantum Fourier transforms, integer multiplication

1 Introduction and summary of results

Since quantum Fourier transforms (QFTs) play a pivotal role in many fast quantum algorithms, it is natural to investigate their properties—including the cost of computing them with various resource measures, such as size and depth in the basic quantum circuit model [5, 2, 4, 7, 6, 10]. For the QFT mod 2^n, it is shown in [5] that size $O(n\log(n/\epsilon))$ is sufficient for an approximation within accuracy ϵ. For exact computations, there is an upper bound of $O(n(\log n)^2\log\log n)$ [4]. For the QFT with respect to an arbitrary n-bit modulus, the best size bound that we are aware of is $O(n\log(n/\epsilon)\log\log(n/\epsilon))$ for approximations within ϵ [7, 6, 8]. Until recently, there was no known polynomial-size construction for exactly computing the QFT in the arbitrary modulus case; however, in [10], it is shown that this can be done.

For the purposes of quantum algorithms, approximations of QFTs are arguably appropriate, since exact implementations of quantum circuits are unlikely to be feasible in physical terms. Also, in some contexts where noise is present and fault-tolerant implementations are necessary, the product of the circuit depth and width might be the most realistic measure of "cost" (as discussed in [4]). Our present focus is on circuit size (the number of one- and two-qubit gates). There are noisy contexts where this is reasonable, such as circumstances where noise may be low and there exist fault-tolerant mechanisms for preserving quantum states whose cost is small relative to the cost of computational steps. We also note that our particular constructions reveal information about the structure of QFTs—particularly their relationship to approximate integer multiplication algorithms.

We consider the question: Can QFTs be computed (exactly or approximately) by linear-size circuits? Although we are unable to answer this question, we provide a construction for the QFT modulo 2^n that is size $O(n(\log\log(n/\epsilon))^2\log\log\log(n/\epsilon))$. This is significantly closer to linear than previous constructions, since its ratio with n is polynomial in $\log\log(n/\epsilon)$ instead of $\log(n/\epsilon)$. We also consider the case of arbitrary moduli and show the following. If there exist circuits of size $o(n\log n\log\log n)$ computing QFTs with respect to arbitrary n-bit moduli then there exists a quantum circuit of size $o(n\log n\log\log n)$ for multiplying n-bit integers—smaller than the Schönhage-Strassen bound [11]. This can be interpreted as evidence that the size improvements possible for the mod 2^n case do not carry over the the arbitrary modulus case. Alternatively, this reduction might contribute to a quantum algorithm for integer multiplication that is superior to existing classical algorithms.

2 Improved approximate QFT mod 2^n

Our approach is a combination of the ideas behind constructions in [4] and [5]. Specifically, we start with a construction in [4], in which phase shifts of the form $|x\rangle|y\rangle \mapsto (e^{2\pi i/2^m})^{xy}|x\rangle|y\rangle$ occur, for $m/2$-bit integers x and y (and various values of m). These phase shifts are computed by efficiently multiplying the two numbers x and y. Our approach is to approximate each of these multiplications by only using the high-order bits of each. This reduces the cost of the multiplications but also introduces an error. We show that the trade-off can be adjusted to yield a circuit of size $O(n(\log\log(n/\epsilon))^2\log\log\log(n/\epsilon))$.

3 QFT mod q and integer multiplication

We show that if there is a quantum circuit of size $o(n\log n\log\log n)$ that approximately computes the QFT mod q then there is also a quantum circuit of size $o(n\log n\log\log n)$ that multiples an n-bit integer by q with success probability $1 - 1/n^{O(1)}$. Such a quantum circuit would be smaller than the most efficient classical multiplication circuit that is known [11].

This reduction uses the results about the modulo 2^m case from the previous section, combined with the *phase*

*Research supported in part by Canada's NSERC, MITACS and CIAR, and Alberta's *i*CORE

†ahokas@cpsc.ucalgary.ca
‡cleve@cpsc.ucalgary.ca
§hales@cs.berkeley.edu

estimation algorithm [9, 3], which can be expressed as follows. Let U be any n-qubit unitary operation and $|\psi\rangle$ be an eigenvector of U with eigenvalue $e^{2\pi i\lambda}$ for some $\lambda \in [0,1)$. Then there is a quantum algorithm that, given state $|\psi\rangle$ as input, computes λ to m bits of precision with success probability $1-\delta$, and whose cost is the sum of the following costs, where $m' = m + O(\log(1/\delta))$:

- The circuit size of computing a QFT modulo $2^{m'}$.
- The circuit size of performing an m'-bit generalized controlled-U operation that maps $|x\rangle\,|y\rangle$ to $|x\rangle\,U^x\,|y\rangle$, for all $x \in \{0,1,\ldots,2^{m'}-1\}$ and $y \in \{0,1\}^n$.

We show that phase estimation can be used to divide; it can be shown that division can be used to multiply. Suppose we have two n-bit integers a, b, and we wish to compute a/b (assume that $a < b$). We begin by computing the QFT mod $b2^{m'-n}$ on $\left|a \cdot 2^{m'-n}\right\rangle$.

$$\begin{aligned} |\psi_a\rangle &= F_{b2^{m'-n}}\left|a \cdot 2^{m'-n}\right\rangle \\ &= \frac{1}{\sqrt{b2^{m'-n}}}\sum_{k=0}^{b2^{m'-n}-1} e^{2\pi i k a 2^{m'-n}/b2^{m'-n}}\,|k\rangle \end{aligned}$$

We now input $|\psi_a\rangle$ into the phase estimation algorithm. The unitary operator $U\,|k\rangle = \left|k-1 \mod b2^{m'-n}\right\rangle$ for $0 \le k < b2^{m'-n}$ has eigenvectors $|\psi_a\rangle$ with corresponding eigenvalues $e^{2\pi i a 2^{m'-n}/b2^{m'-n}} = e^{2\pi i a/b}$. This operator will be used as the controlled-U operator in the phase estimation algorithm. If we use m' bits as the control for phase estimation, the controlled-U can be performed by subtracting the first register from the second modulo $b2^{m'-n}$, since $|x\rangle\,U^x\,|y\rangle = |x\rangle\left|y-x \mod b2^{m'-n}\right\rangle$. This subtraction can be performed in time linear in m'. As output, we will receive an m-bit approximation to a/b with probability $1-\delta$.

References

[1] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997.

[2] R. Cleve. A note on computing quantum Fourier transforms by quantum programs. Manuscript. Available at http://www.cpsc.ucalgary.ca/~cleve/papers.html, 1994.

[3] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca. Quantum algorithms revisited. *Proc. R. Soc. Lond. A*, pages 339–354, 1998.

[4] R. Cleve and J. Watrous. Fast parallel circuits for the quantum Fourier transform. *Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science (FOCS 00)*, pages 526–536, 2000.

[5] D. Coppersmith. An approximate Fourier transform useful in quantum factoring. Technical Report RC19642, IBM, 1994.

[6] L. Hales. *The quantum Fourier transform and extensions of the abelian hidden subgroup problem.* PhD thesis, University of California at Berkeley, 2002. Los Alamos Preprint Archive quant-ph/0212002.

[7] L. Hales and S. Hallgren. Improved quantum fourier transform algorithm and applications. *Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science (FOCS 00)*, 2000.

[8] S. Hallgren. *Quantum Fourier Sampling, the Hidden Subgroup Problem, and Beyond.* PhD thesis, University of California at Berkeley, 2000.

[9] A. Kitaev. Quantum measurments and the abelian stabilizer problem. *Los Alamos Preprint Archive quant-ph/9511026*, 1995.

[10] M. Mosca and C. Zalka. Exact quantum Fourier transforms and discrete logarithm algorithms. *Los Alamos Preprint Archive quant-ph/0301093*, 2003.

[11] A. Schönhage and V. Strassen. Schnelle multiplikation großer zahlen. *Computing*, 7:281–292, 1971.