

Discrete Cosine Transforms on Quantum Computers

Andreas Klappenecker
Texas A&M University
Department of Computer Science
College Station, TX 77843-3112, USA

Martin Rötteler
Universität Karlsruhe
Institut für Algorithmen und Kognitive Systeme
Quantum Computing Group, Prof. Thomas Beth
Am Fasanengarten 5, 76 128 Karlsruhe, Germany

Abstract

A classical computer does not allow to calculate a discrete cosine transform on N points in less than linear time. This trivial lower bound is no longer valid for a computer that takes advantage of quantum mechanical superposition, entanglement, and interference principles. In fact, we show that it is possible to realize the discrete cosine transforms and the discrete sine transforms of size $N \times N$ and types I, II, III, and IV with as little as $O(\log^2 N)$ operations on a quantum computer, whereas the known fast algorithms on a classical computer need $O(N \log N)$ operations.

1 Introduction

Feynman proposed in 1982 a computational model that was based on the principles of quantum physics instead of classical physics. The model has been considered a mere curiosity until Peter Shor showed in 1994 that it is possible to factor integers in polynomial time on a quantum computer [1]. Thus, a moderate sized quantum computer is for instance able to break the RSA public key cryptosystem. Quantum computing is an exciting area of emerging signal processing applications. In fact, signal processing methods play a key role in Shor's integer factoring algorithm and in many other quantum algorithms.

A quantum computer is based on the concept of a quantum bit, just as a classical computer is based on the notion of a bit. A single quantum bit represents the state of a two-level quantum system such as a polarized photon or a spin-1/2 system. Unlike a classical computer, adding another quantum bit to the memory of a quantum computer will not increase the dimensionality of the state space by one but will *double* it, allowing for linear combinations of 2^n different base states in the case of n quantum bits.

A program on a quantum computer is composed of a sequence of elementary 'gates', which perform simple unitary transforms (as explained in Section 3). In fact, many

algorithms in quantum computing rely on the fast Fourier transforms, the Walsh-Hadamard transforms, or other unitary transforms well-known in signal processing.

The purpose of this paper is to derive (extremely) fast quantum algorithms for the discrete cosine and sine transforms. These algorithms can be implemented on a number of quantum computing technologies based on Raman-coupled low-energy states of trapped ions [2, 3], nuclear spins in silicon [4], electron spins in quantum dots [5], atomic cavity quantum electrodynamics [6], or linear optics [7]. Coherent control of up to four quantum bits has been demonstrated [8], and much progress is expected in the near future.

2 Definitions

Recall the definitions [9] of the *discrete cosine transforms*:

$$\begin{aligned} C_N^I &:= \left(\frac{2}{N}\right)^{1/2} \left[k_i \cos \frac{ij\pi}{N} \right]_{i,j=0..N} \\ C_N^{II} &:= \left(\frac{2}{N}\right)^{1/2} \left[k_i \cos \frac{i(j+1/2)\pi}{N} \right]_{i,j=0..N-1} \\ C_N^{III} &:= \left(\frac{2}{N}\right)^{1/2} \left[k_i \cos \frac{(i+1/2)j\pi}{N} \right]_{i,j=0..N-1} \\ C_N^{IV} &:= \left(\frac{2}{N}\right)^{1/2} \left[k_i \cos \frac{(i+1/2)(j+1/2)\pi}{N} \right]_{i,j=0..N-1} \end{aligned}$$

where $k_i := 1$ for $i = 1, \dots, N-1$ and $k_0 := 1/\sqrt{2}$. The numbers k_i ensure that the transforms are orthogonal. The discrete sine transforms S_N^I , S_N^{II} , S_N^{III} , and S_N^{IV} are defined accordingly, see [9] for details. Notice that C_N^{III} (resp. S_N^{III}) is the transpose of C_N^{II} (resp. S_N^{II}), hence it suffices to derive circuits for the type II transforms. In the following, we content ourselves to $N = 2^n$, which is justified by the machine model introduced below.

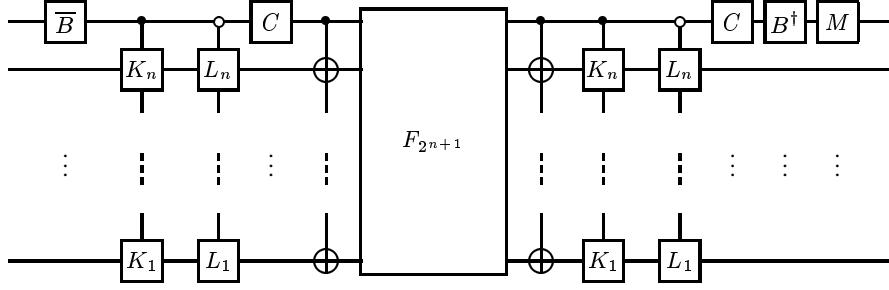


Figure 3. Complete quantum circuit for DCT_{IV}

and $\omega = \exp(2\pi i/4N)$ with $i^2 = -1$.

Theorem 3 *The discrete cosine transform C_N^{II} and the discrete sine transform S_N^{II} can be realized with $O(\log^2 N)$ elementary quantum gates; the quantum circuit for these transforms is shown in Figure 4.*

Proof. We need to derive efficient quantum circuits for the matrices V_N and U_N in equation (3). The matrix V_N has a fairly simple decomposition in terms of quantum circuits.

Lemma 4 $V_N = \pi_1(H \otimes \mathbf{1}_N)$.

Proof. It is clear that the Hadamard transform on the most significant bit $H \otimes \mathbf{1}_N$ is – up to a permutation of rows – equivalent to V_N . The appropriate permutation of rows has been introduced in the previous section, namely $\pi_1|0x\rangle = |1x\rangle$ and $\pi_1|1x\rangle = |\overline{1x}\rangle$ for all $0 \leq x < 2^n$. We can conclude that $V_N = \pi_1(H \otimes \mathbf{1}_N)$ as desired. \square

The decomposition of U_N is more elaborate. Notice that

$$\begin{aligned} U_N|00\rangle &= |00\rangle & U_N|11\rangle &= (-1)|10\rangle \\ U_N|0x\rangle &= \frac{\overline{\omega}^x}{\sqrt{2}}|0x\rangle + \frac{\omega^x}{\sqrt{2}}|1x'\rangle \\ U_N|1y\rangle &= -\frac{i\overline{\omega}^{y+1}}{\sqrt{2}}|0(y+1 \bmod 2^n)\rangle + \frac{i\omega^{y+1}}{\sqrt{2}}|1\overline{y}\rangle \end{aligned}$$

for all integers x in the range $1 \leq x < 2^n$ and all integers y in $0 \leq y < 2^n - 1$. Here $\mathbf{0}$ and $\mathbf{1}$ denote the n -bit integers 0 and $2^n - 1$ respectively.

Define D_0 by $D_0|10\rangle = i|10\rangle$ and $D_0|x\rangle = |x\rangle$ otherwise. We define a permutation π_2 by $\pi_2|0x\rangle = |0x\rangle$ and $\pi_2|1x\rangle = |1(x+1 \bmod 2^n)\rangle$ for all integers x in $0 \leq x < 2^n$.

Lemma 5 $U_N = D_1^\dagger \overline{T}_N D_0 \pi_2$.

Proof. Since $D_1^\dagger|0x\rangle = \overline{\omega}^x|0x\rangle$ and $D_1^\dagger|1x\rangle = \omega^{x'}|1x\rangle$, we obtain

$$\begin{aligned} D_1^\dagger \overline{T}_N |0x\rangle &= \frac{\overline{\omega}^x}{\sqrt{2}}|0x\rangle + \frac{\omega^x}{\sqrt{2}}|1x'\rangle \\ D_1^\dagger \overline{T}_N |1x\rangle &= -\frac{i\overline{\omega}^x}{\sqrt{2}}|0x\rangle + \frac{i\omega^x}{\sqrt{2}}|1x'\rangle \end{aligned}$$

We have $D_0\pi_2|0x\rangle = |0x\rangle$ and moreover $D_0\pi_2|1x\rangle = |1(x+1 \bmod 2^n)\rangle$ for all integers x in $0 \leq x < 2^n - 1$, and $D_0\pi_2|11\rangle = i|10\rangle$. We note that $(x+1 \bmod 2^n)' = \overline{x}$, whence combining $D_1\overline{T}_N$ with $D_0\pi_2$ shows the result. \square

Recall that $T_N = \pi D$. It follows that

$$U_N^\dagger = \pi_2^{-1}(\overline{D}_0 D^t) \pi^{-1} D_1.$$

The implementation of D_1 has been described in the section on the DCT_{IV} , and the implementation of π (and hence π^{-1}) is contained in the section on the DCT_I . The implementation of π_2^{-1} is also straightforward. It remains to find an implementation of $\overline{D}_0 D^t$. We observe that

$$\begin{aligned} \overline{D}_0 D^t |00\rangle &= |00\rangle, & \overline{D}_0 D^t |0x\rangle &= \frac{1}{\sqrt{2}}|0x\rangle + \frac{i}{\sqrt{2}}|1x\rangle, \\ \overline{D}_0 D^t |10\rangle &= -i|10\rangle, & \overline{D}_0 D^t |1x\rangle &= \frac{1}{\sqrt{2}}|0x\rangle - \frac{i}{\sqrt{2}}|1x\rangle. \end{aligned}$$

This can be accomplished by a single qubit operation followed by a multiply conditioned gate, where the single qubit operation is given by $B^t \otimes \mathbf{1}_N$ and the conditional gate acts via

$$J = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}.$$

The full circuit is shown in Figure 4. The statement about the complexity is clear. \square

7 Conclusions

Signal processing methods have proved to be useful in virtually all known quantum algorithms. A basic problem in the design of quantum algorithms is to choose a well-adapted basis to recoup relevant information about the state of the system. The well-known decorrelation properties of DCTs may prove to be useful within this framework. We have shown that the DCT and DST of types I, II, III, and IV can be realized with a polylogarithmic number of elementary operations on a quantum computer. Compared to the classical realization of the DCT, this is a tremendous speed-up, making the DCT attractive in the design of other quantum algorithms.

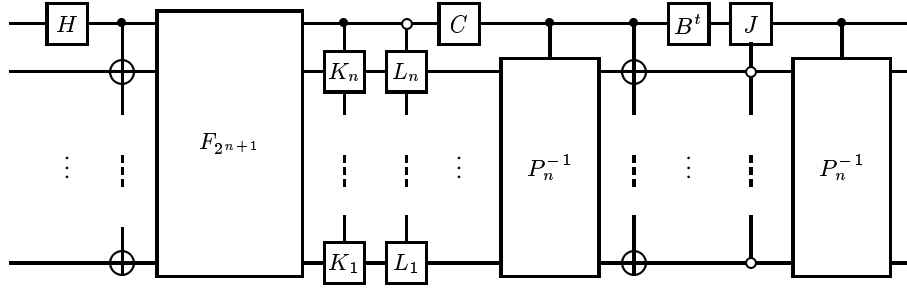


Figure 4. Complete quantum circuit for DCT_{II}

Acknowledgments. We thank Hyunyoung Lee for comments that improved the presentation of this paper. We thank the European Community for supporting this research under IST-1999-10596 (Q-ACTA).

References

- [1] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithm and Factoring," in *Proc. FOCS 94*. 1994, pp. 124–134, IEEE Computer Society Press.
- [2] J.I. Cirac and P. Zoller, "Quantum computations with cold trapped ions," *Phys. Rev. Lett.*, vol. 74, no. 20, pp. 4091–4094, 1995.
- [3] H. Nägerl, D. Leibfried, H. Rohde, J. Thalhammer, G. Eschner, F. Schmidt-Kaler, and R. Blatt, "Laser addressing of individual ions in a linear ion trap," *Physical Review A*, vol. 60, no. 1, pp. 145–148, 1999.
- [4] B.E. Kane, "A silicon-based nuclear spin quantum computer," *Nature*, vol. 393, no. 6681, pp. 133–137, 1998.
- [5] A. Imamoglu, D.D. Awschalom, G. Burkard, D.P. DiVincenzo, D. Loss, M. Sherwin, and A. Small, "Quantum information processing using quantum dot spins and cavity-qed," *Phys. Rev. Lett.*, vol. 83, pp. 4204–4207, 1999.
- [6] A. Rauschenbeutel, G. Nogues, S. Osnaghi, P. Bertet, M. Brune, J.M. Raimond, and Haroche S., "Coherent operation of a tunable quantum phase gate in cavity QED," *Phys. Rev. Lett.*, vol. 83, no. 24, pp. 5166–5169, 1999.
- [7] E. Knill, R. Laflamme, and G.J. Milburn, "A scheme for efficient quantum computation with linear optics," *Nature*, vol. 409, pp. 46–52, 2001.
- [8] D. Kielpinski et al., "Recent results in trapped-ion quantum computing at NIST," *To appear in Proc. of IQC 2001*, 2001.
- [9] K. R. Rao and P. Yip, *Discrete Cosine Transform: Algorithms, Advantages, and Applications*, Academic Press, 1990.
- [10] A. Barenco *et al.*, "Elementary gates for quantum computation," *Physical Review A*, vol. 52, no. 5, pp. 3457–3467, Nov. 1995.
- [11] V. Wickerhauser, *Adapted Wavelet Analysis from Theory to Software*, A.K. Peters, Wellesley, 1993.
- [12] M. Püschel, M. Rötteler, and Th. Beth, "Fast Quantum Fourier Transforms for a Class of non-abelian Groups," in *Proc. AAECC-13*. 1999, vol. 1719 of LNCS, pp. 148–159, Springer.