Journal of Symbolic Computation 75 (2016) 219–243

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Quantum Fourier transform over symmetric groups — improved result ☆

Yasuhito Kawano [a], Hiroshi Sekigawa [b]

[a] NTT Communication Science Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi-shi, Kanagawa, 243-0198, Japan
[b] Department of Mathematical Information Science, Tokyo University of Science, 1-3 Kagurazaka, Shinjuku-ku, Tokyo, 162-8601, Japan

ARTICLE INFO

Article history:
Received 8 December 2014
Accepted 10 July 2015
Available online 5 November 2015

Keywords:
Quantum Fourier transform
Fast Fourier transform
Symmetric group
Representation theory
Non-abelian group

ABSTRACT

This paper describes the fastest quantum algorithm at this moment for the quantum Fourier transform (QFT) over symmetric groups. We provide a new FFT (classical) algorithm over symmetric groups and then transform it to a quantum algorithm. The complexity of our QFT algorithm is $O(n^3 \log n)$, faster than the existing $O(n^4 \log n)$ QFT algorithm. In addition, we show that the algorithm can be performed in $O(n^3)$ if the use of threshold gates is allowed.

1. Introduction

The quantum Fourier transform (QFT) plays an important role in many quantum algorithms exponentially faster than their classical counterparts. The quantum algorithms proposed by Shor (1997) that efficiently solve the factoring problem and the discrete logarithm problem apply the QFT over cyclic groups. The QFT over cyclic groups has been studied in detail, and efficient algorithms have been proposed (Hales and Hallgren, 2000; Cleve and Watrous, 2000; Mosca and Zalka, 2004; Gyongyosi and Imre, 2010).

☆ Preliminary versions of this paper were published as "Quantum Fourier Transform over Symmetric Groups" in *Proceedings of the International Symposium on Symbolic and Algebraic Computation (ISSAC 2013), pp. 227–234, Northeastern University, Boston, USA (June 26–29, 2013)* and as "Quantum Fourier Transform over Symmetric Groups — Improved Result" in a poster presentation at *International Symposium on Symbolic and Algebraic Computation (ISSAC 2014), Kobe University, Kobe, Japan (July 22–25, 2014)*. Abstract in ACM Communications in Computer Algebra, Vol. 48, No. 3, Issue 189, pp. 127–129, 2014.

E-mail addresses: kawano.yasuhito@lab.ntt.co.jp (Y. Kawano), sekigawa@rs.tus.ac.jp (H. Sekigawa).

http://dx.doi.org/10.1016/j.jsc.2015.11.016
0747-7171/

To find new quantum algorithms that achieve exponential speed-ups, QFT algorithms over non-abelian groups have been studied. Among non-abelian groups, symmetric groups were the first to come to attention since they were thought to be applicable to the graph isomorphism problem (Nielsen and Chuang, 2000, Subsection 5.4.4). Unfortunately, evidence that the graph isomorphism problem cannot be solved efficiently using the QFT over symmetric groups was found (Hallgren et al., 2010). On the other hand, as a positive result of an exponential speed-up, it has been proved that the QFT over symmetric groups can achieve an exponential speed-up for a certain oracle problem (Brandão and Horodecki, 2013); more precisely, there is an oracle problem such that it can be solved by a quantum computer using the QFT over symmetric groups with a constant number of queries, but it cannot be solved by a classical computer with an exponential number of queries even if the classical computer has postselection ability.

An efficient QFT algorithm over symmetric groups was first proposed by Beals (1997). The algorithm was obtained by transforming the fast Fourier transform (FFT) algorithm over symmetric groups proposed by Clausen (1989) and Diaconis and Rockmore (1990). Later, Moore et al. (2006) applied recent progress in the FFT algorithm and proposed efficient QFT algorithms over non-abelian groups, including symmetric groups. The complexity of their QFT algorithm over symmetric group S_n is $O(n^4 \log n)$ (Moore et al., 2006, Lemma 4.1), where some simple operations capable of being performed in polynomial time are counted as single gates (the types of operations counted as single gates will be explained later in this section). Their QFT algorithm sums amplitudes over cosets serially, where the sum-of-amplitudes is the most complex calculation in the QFT algorithm. Performing the sum-of-amplitudes serially was an overhead of the algorithm.

Kawano and Sekigawa (2013) proposed an $O(n^4)$ QFT algorithm over symmetric groups that calculates the sum-of-amplitudes in parallel. (Further details of the technical key point for the speed-up will be given in Subsection 5.1.) Here, to compare the complexity of our algorithm to the algorithm in Moore et al. (2006), the same types of operations as in that paper were counted as single gates. To construct our algorithm, we decomposed the FFT matrix into multiplications of $O(n^3)$ sparse unitary matrices, and then transformed it into a quantum algorithm. Note that the FFT algorithm defined by the above matrix decomposition has the same complexity $O(n^3 n!)$ (Clausen, 1989, Theorem 1.4) as the Clausen–Diaconis–Rockmore (CDR) FFT algorithm.

Furthermore, Kawano and Sekigawa (2014) provided a more efficient QFT algorithm by improving the subroutines for the bottlenecks in the previous one. As a result, the complexity of the new QFT algorithm became $O(n^3 \log n)$, which is faster than our previous algorithm.

In this paper, we provide complete proofs of the lemmas and theorems in those two papers. In addition, this paper shows that our previous $O(n^3 \log n)$ algorithm can be performed in $O(n^3)$ if the use of threshold gates is allowed. Here, the threshold gate is one of the fundamental quantum operations and can be performed by a constant-depth circuit in $\mathrm{QNC}_{\mathrm{f}}^0$ (Høyer and Špalek, 2005), though it is $O(\log n)$ using the standard elementary gates — single-qubit rotations and CNOT. Completely different techniques will be necessary for further optimization. A hint for this research direction will be mentioned in the conclusion section.

As a byproduct, we obtain a new FFT (classical) algorithm over symmetric groups. The complexity of the algorithm is $O(n^3 n!)$, which is the same as the CDR algorithm (Clausen, 1989, Theorem 1.4). To check the classical algorithm described in this paper, we made an FFT software program on Mathematica system ver 8.0.4.0. The software can, for example, calculate $\mathfrak{F}_{10}\vec{v}$ from a 10!-length random column vector $\vec{v}$ ($\mathfrak{F}_{10}$ is the $10! \times 10!$ Fourier transform matrix over S_{10}) in about two hours on an Intel(R) Xeon(R) CPU E7-4870 2.40-GHz processor.

1.1. Notification regarding single gates

Theorem 1 in the paper by Moore et al. (2006) states that QFT over a polynomially uniform group with a subgroup tower $G = G_n > \cdots > \{1\}$ is performed using $poly(I \times D \times M \times \log|G|)$ elementary quantum operations, where I is the maximum index $\max_i[G_i : G_{i-1}]$, D is the adapted diameter, and M is the maximum multiplicity. When G is symmetric group S_n with the tower $G = S_n > \cdots > \{1\}$, we have $I = \max_i[S_i : S_{i-1}] = n$, $D = n^2$, $M = 2$, and $\log|G| = O(n \log n)$. The complexity of the QFT circuit over symmetric groups in Moore et al. (2006) is then $poly(n^4 \log n)$. Here, the expression $poly(n^4 \log n)$