Contents lists available at ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

Optimal separation in exact query complexities for Simon's problem

Guangya Cai, Daowen Qiu [*]

Institute of Computer Science Theory, School of Data and Computer Science, Sun Yat-sen University, Guangzhou 510006, China

ARTICLE INFO

Article history:
Received 4 December 2016
Received in revised form 14 March 2018
Accepted 4 May 2018
Available online xxxx

Keywords:
Simon's problem
Exact query complexity
Quantum computing

ABSTRACT

Simon's problem is one of the most important problems demonstrating the power of quantum computers. In this paper, we propose another exact quantum algorithm for solving Simon's problem with $O(n)$ queries, which is simple, concrete and does not rely on special query oracles. Our algorithm combines Simon's algorithm with the quantum amplitude amplification technique to ensure its determinism. In particular, we show that Simon's problem can be solved by a classical *deterministic* algorithm with $O(\sqrt{2^n})$ queries (as we are aware, there were no classical deterministic algorithms for solving Simon's problem with $O(\sqrt{2^n})$ queries). Combining some previous results, we obtain the optimal separation in exact query complexities for Simon's problem: $\Theta(n)$ versus $\Theta(\sqrt{2^n})$.

1. Introduction

Query complexity has been very useful to study the relative power of quantum computation and classical computation [7,15]. According to their output, query algorithms can be studied either in the *bounded-error* setting (the algorithm gives the correct result with probability at least 2/3) or in the *exact* setting (the algorithm gives the correct result with certainty). For the bounded-error case, there are many algorithms achieving large separation in query complexities (for example, [1,9]), and some of them have exponential or even larger speedups for computing partial functions ([17] includes a more detailed list), though it is not known whether the separation is optimal for some of them.

As for exact query complexity, the result is more limited. For total functions, Ambainis [2] gave the first superlinear speedup example, and the best known separation is $\widetilde{O}(n)$ versus $\Omega(n^2)$ [3], which computes a variant of functions introduced in [10]. In fact, it has been proved that the quantum query algorithms can only achieve polynomial speedup with degree at most 3 [13]. However, for computing partial functions, there can be an exponential or larger separation, and the first example is the well-known Deutsch–Jozsa problem [8], whose separation is 1 versus $n/2+1$. In [17], the optimal separation for a generalized Deutsch–Jozsa problem was given, which is over exponential one as well.

Simon's problem [18] is a famous computational problem that achieves exponential separation in query complexities. In the bounded-error setting, Simon gave an elegant quantum algorithm which solves the problem with $O(n)$ queries and the physical realization has demonstrated its efficiency [19]. The $\Omega(n)$ lower bound was also proved in [11] using polynomial method [4]. On the other hand, the classical probabilistic query complexity for this problem is $\Theta(\sqrt{2^n})$ [20], which shows that the $\Theta(n)$ versus $\Theta(\sqrt{2^n})$ separation is an optimal one.

[*] Corresponding author.
E-mail address: issqdw@mail.sysu.edu.cn (D. Qiu).

https://doi.org/10.1016/j.jcss.2018.05.001

Please cite this article in press as: G. Cai, D. Qiu, Optimal separation in exact query complexities for Simon's problem, J. Comput. Syst. Sci. (2018), https://doi.org/10.1016/j.jcss.2018.05.001

As for the exact query complexities of Simon's problem, Brassard and Høyer [5] combined Simon's algorithm with two post-processing subroutines to ensure that their algorithm solves the problem exactly, which also requires $O(n)$ queries. However, their algorithm is quite complicated and involved. Mihara and Sung [14] proposed a simpler exact algorithm, but their algorithm relies on some non-standard query oracles and they did not show the construction of their oracles. Moreover, the $\Omega(n)$ quantum query lower bound is a direct corollary of previous bounded-error lower bound result. For the classical case, the $\Omega(\sqrt{2^n})$ lower bound can be easily obtained (Theorem 6). As we are aware, it was not known (until this point) whether this lower bound is a tight one, so it was not known (until this point) whether the $O(n)$ versus $\Omega(\sqrt{2^n})$ is optimal either.

In this paper, we propose a new exact quantum algorithm for solving Simon's problem also with $O(n)$ queries, which is much simpler and more concrete than Brassard and Høyer's algorithm [5] and does not rely on some non-standard query oracles as Mihara and Sung's construction [14]. Our algorithm directly combines Simon's algorithm with the quantum amplitude amplification technique [6] to ensure we get an exact result. Then, we design a classical deterministic algorithm for solving Simon's problem with $O(\sqrt{2^n})$ queries, which relies on some crucial insights about the bitwise exclusive-or operation results of the pairs of strings which are queried by the algorithm. Thus, we prove the $\Theta(\sqrt{2^n})$ classical deterministic query complexity for Simon's problem. With previously established results on the exact quantum query complexity, we can get the optimal separation in the exact query complexities for Simon's problem: $\Theta(n)$ versus $\Theta(\sqrt{2^n})$.

The remainder of the paper is organized as follows. In Section 2, we review Simon's problem, describe the Simon's algorithm [18] with a different way, and present some notions and notations that will be used hereinafter. Then in Section 3, we discuss the quantum query complexity of Simon's problem and give a new exact quantum algorithm to solve Simon's problem also with $O(n)$ queries. After that, in Section 4, we discuss the classical query complexity of Simon's problem and design a classical deterministic algorithm for solving Simon's problem with $O(\sqrt{2^n})$ queries. Finally, conclusions are summarized in Section 5.

2. Preliminaries

In the interest of readability, this section serves to introduce some basic notions concerning quantum computation and Simon's problem.

2.1. Basic introduction to quantum computation

First, let us introduce some basic terminology of quantum computation. For the details, we can refer to [16].

In quantum computers, the minimal unit of information is called a *quantum bit* or a *qubit*. As it is known, the classical bit can be one of the two states – either 0 or 1, but a qubit can be a *superposition* of the two states, written $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. The numbers α and β are complex numbers satisfying $|\alpha|^2 + |\beta|^2 = 1$. Put another way, the state of a qubit is a vector in two-dimensional complex vector space. $|0\rangle$ and $|1\rangle$ are known as *computational basis states*, and α and β are the *amplitudes* of the relevant computational basis states.

There are two things we can do with a qubit: measure it or let it evolve unitarily without measurements. We deal with measurements first. The most straightforward one is the measurement in the computational basis. In this way, the measured qubit is either $|0\rangle$ or $|1\rangle$. By physical restriction, we do not know the measurement result in advance, but we can ensure that we will see $|0\rangle$ with probability $|\alpha|^2$ and $|1\rangle$ with probability $|\beta|^2$. Of course, there exist other more general kinds of measurement, but throughout this paper, we only use the measurement in the computational basis.

Instead of measuring $|\psi\rangle$, we can also apply some operations to it. By a complex matrix U, a state $|\psi\rangle$ can be transformed to a state $|\varphi\rangle = U|\psi\rangle$. According to the principle of quantum mechanics [16], the transformation must be a *unitary* transformation, so U must be a *unitary* matrix.

The notions and notations above describe a system of one qubit, similarly we can think of systems of multiple qubits. A register of n qubits has 2^n basis states, each of form $|x\rangle = |x_1, x_2, \cdots, x_n\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle$, where $\otimes$ is the tensor product operation and $x \in \{0,1\}^n$. The state of the n qubit registers can be the superposition of these basis states. The measurements and state transformations of multiple qubits are similar to the one qubit case as well. Note that we are also using the tensor product operation to couple the transformation operators on different parts of the register, i.e. $(A \otimes B)(|x\rangle \otimes |y\rangle) = A|x\rangle \otimes B|y\rangle$.

2.2. Problem description

Now, let us recall Simon's problem. Let $n \geq 1$ be any positive integer and let $(\oplus): \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ denote the bitwise exclusive-or operation. Suppose we are given a function $f: \{0,1\}^n \to \{0,1\}^m$ with $m \geq n$, and we are promised that there exists an $s \in \{0,1\}^n \setminus \{0^n\}$ such that for all $x, y \in \{0,1\}^n$, $f(x) = f(y)$ if and only if $x = y$ or $x = y \oplus s$, the aim is to compute s.

There exists an associated decision problem for Simon's problem as well. Suppose that the given function f is either one-to-one, or satisfies the condition defined above. Then the purpose is to determine which of these conditions holds for f. Since any lower bound on this problem implies the same one on the original Simon's problem, it would be useful for the lower bound proof in what follows.