Theoretical Computer Science 666 (2017) 48–64

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Promise problems solved by quantum and classical finite automata

Shenggen Zheng [a], Lvzhou Li [a], Daowen Qiu [a,*], Jozef Gruska [b]

[a] *Institute of Computer Science Theory, School of Data and Computer Science, Sun Yat-sen University, Guangzhou 510006, China*
[b] *Faculty of Informatics, Masaryk University, Brno 60200, Czechia*

ARTICLE INFO

Article history:
Received 17 November 2015
Received in revised form 18 December 2016
Accepted 20 December 2016
Available online 2 January 2017
Communicated by M. Hirvensalo

Keywords:
Promise problems
Quantum computing
Finite automata
Quantum finite automata
Recognizability
Solvability

ABSTRACT

The concept of *promise problems* was introduced and started to be systematically explored by Even, Selman, Yacobi, Goldreich, and other scholars. It has been argued that promise problems should be seen as partial *decision problems* and as such that they are more fundamental than decision problems and formal languages that used to be considered as the basic ones for complexity theory. The main purpose of this paper is to explore the promise problems accepted by classical, quantum and also semi-quantum finite automata. More specifically, we first introduce two acceptance modes of promise problems, *recognizability* and *solvability*, and explore their basic properties. Afterwards, we show several results concerning descriptional complexity on promise problems. In particular, we prove: (1) there is a promise problem that can be recognized exactly by *measure-once one-way quantum finite automata* (MO-1QFA), but no *deterministic finite automata* (DFA) can recognize it; (2) there is a promise problem that can be solved with error probability $\epsilon \leq 1/3$ by *one-way finite automaton with quantum and classical states* (1QCFA), but no *one-way probability finite automaton* (PFA) can solve it with error probability $\epsilon \leq 1/3$; and especially, (3) there are promise problems $A(p)$ with size p that can be solved *with any error probability* by MO-1QFA with only two quantum basis states, but they can not be solved *exactly* by any MO-1QFA with two quantum basis states; in contrast, the minimal PFA solving $A(p)$ *with any error probability* (usually smaller than 1/2) has p states. Finally, we mention a number of problems related to promise for further study.

1. Introduction

Informally, a promise problem is the problem to decide whether an object or process has a property P_1 or P_2, provided it is promised (known) to have a property P_3.

The concept of a promise problem was introduced explicitly in [11] and it has been argued there that promise problems are actually more fundamental for the study of computational theory issues than decision problems or, more formally, formal language versions/encodings of the decision problems.

Such a view on the fundamental importance of promise problems has been even more emphasized in the survey paper [15], where also the following basic version of the promise problems has been introduced.

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

http://dx.doi.org/10.1016/j.tcs.2016.12.025
0304-3975/

Definition 1. A promise problem over an alphabet Σ is a pair (A_{yes}, A_{no}) of disjoint subsets of Σ^*. The union $A_{yes} \cup A_{no}$ is then called the *promise* and A_{yes} as well A_{no} are called promise's components.

The goal is then to decide whether $x \in A_{yes}$ or $x \in A_{no}$ for a given string x from the promise set. In a special (trivial) case the promise is the whole set Σ^*. However, in general it may be very nontrivial to decided whether an input string is in a given promise set.

In spite of the fact that both papers [11,15] have brought interesting problems and outcomes, the study of promise problems did not get a proper momentum yet.

On the other side, the results concerning several promise problems in quantum information processing have had very large impact. They demonstrated that using quantum phenomena and processes one can solve several interesting promise problems with much less quantum queries (to quantum black boxes) than in the case only classical tools and queries (to classical black boxes) are available. The initial development in this area was culminated by the result of Simon [37] that the promise problem he introduced can be solved with the polynomial number of quantum and classical queries but not with polynomial number of classical queries only even if probabilistic tools are used. The second promise problem is the Hidden Subgroup Problem for non-commutative groups, which took very large attention, especially its special cases, for example integer factorization, due to Shor [36], and can be now seen as one of the most fundamental, and still open, problems.

Almost all papers so far, especially papers [11,15,38], dealt with promise problems in the context of such high level complexity classes as **P**, **NP**, **BPP**, **SZK** and so on.

In this paper we start to explore promise problems on another level, namely, using classical and quantum or even semi-quantum finite automata to attack some promise problems working in various (especially two special) modes. The remainder of the paper is organized as follows. In Section 2, we recall the definitions of classical and quantum finite automata that will be used in the paper, and define two acceptance modes of promise problems, *recognizability* and *solvability* of promise problems by automata. Then, in Section 3.3, we deal with the closure and ordering properties of promise problems. Afterwards, in Section 4, lower and upper bounds are derived concerning the state complexity in a promise problem between the promise and its two components.

In particular, we study some promise problems in terms of classical and quantum finite automata in Section 5, and obtain the following results: that there is a promise problem that can be recognized exactly by *measure-once one-way quantum finite automata* (MO-1QFA), but no *deterministic finite automata* (DFA) can recognize it (Theorem 13); there is a promise problem that can be solved with any error probability by *one-way finite automaton with quantum and classical states* (1QCFA), but no *one-way probability finite automaton* (PFA) can solve it with error probability $\epsilon \leq 1/3$ (Theorem 14).

Especially, in Section 5 we prove a hierarchic result concerning QFA. More exactly, we show that there are promise problems $A(p)$ with size p that can be solved *with any error probability* by MO-1QFA with only two quantum basis states, but they can not be solved *exactly* by any MO-1QFA with two quantum basis states (Theorem 15), and in contrast, the minimal PFA solving $A(p)$ with any error probability (usually smaller than 1/2) has p states (Theorem 16). However, we do not know whether there is an MO-1QFA with more than *two* quantum basis states being able to solve exactly this promise problems $A(p)$.

In addition, the above result may give rise to a hierarchic problem for the classes solved by MO-1QFA in terms of different quantum basis states. More precisely, let $\mathcal{C}(P)_n$ denote the class of promise problems solved exactly by an MO-1QFA with n quantum basis states. Then, whether does $\mathcal{C}(P)_m \subset \mathcal{C}(P)_n$ hold for $m \leq n$? Therefore, in Section 6 we mention a number of problems related for further study.

2. Preliminaries

We introduce in this section some basic concepts and notations concerning classical and quantum finite automata. For more on quantum information processing and (quantum and semi-quantum) finite automata we refer the reader to [29–33, 27,34,16,19,26].

2.1. Deterministic finite automata

In this subsection we recall the definition of *deterministic finite automata* (DFA) and give the definition of so-called *promise version deterministic finite automata* (pvDFA).

Definition 2. A deterministic finite automaton (DFA) $\mathcal{A}$ is specified by a 5-tuple

$$\mathcal{A} = (S, \Sigma, \delta, s_0, S_a), \tag{1}$$

where:

- S is a finite set of classical states;
- Σ is a finite set of input symbols;
- $s_0 \in S$ is the initial state of the automaton;