Information and Computation 241 (2015) 197–214

Contents lists available at ScienceDirect

Information and Computation

www.elsevier.com/locate/yinco

# Power of the interactive proof systems with verifiers modeled by semi-quantum two-way finite automata

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

[a] Department of Computer Science, Sun Yat-sen University, Guangzhou 510006, China
[b] Faculty of Informatics, Masaryk University, Brno 60200, Czech Republic
[c] SQIG–Instituto de Telecomunicações, Departamento de Matemática, Instituto Superior Técnico, Universidade de Lisboa, Av. Rovisco Pais 1049-001, Lisbon, Portugal

ARTICLE INFO

*Article history:*
Received 13 March 2013
Available online 7 February 2015

*Keywords:*
Quantum computing
Quantum finite automata
Quantum Arthur–Merlin proof systems
Two-way finite automata with quantum and classical states

ABSTRACT

*Interactive proof systems* (IP) are very powerful – languages they can accept form exactly PSPACE. They represent also one of the very fundamental concepts of theoretical computing and a model of computation by interactions. One of the key players in IP is verifier. In the original model of IP whose power is that of PSPACE, the only restriction on verifiers is that they work in randomized polynomial time. Because of such key importance of IP, it is of large interest to find out how powerful will IP be when verifiers are more restricted. So far this was explored for the case that verifiers are *two-way probabilistic finite automata* (Dwork and Stockmeyer, 1990) and *one-way quantum finite automata* as well as *two-way quantum finite automata* (Nishimura and Yamakami, 2009). IP in which verifiers use *public randomization* is called *Arthur–Merlin proof systems* (AM). AM with verifiers modeled by Turing Machines augmented with a fixed-size quantum register (qAM) were studied also by Yakaryilmaz (2012). He proved, for example, that an NP-complete language $L_{knapsack}$, representing the 0–1 knapsack problem, can be recognized by a qAM whose verifier is a *two-way finite automaton* working on quantum mixed states using superoperators.

In this paper we explore the power of AM for the case that verifiers are *two-way finite automata with quantum and classical states* (2QCFA) – introduced by Ambainis and Watrous in 2002 – and the communications are classical. It is of interest to consider AM with such "semi-quantum" verifiers because they use only limited quantum resources. Our main result is that such Quantum Arthur–Merlin proof systems (QAM(2QCFA)) with polynomial expected running time are more powerful than the models in which the verifiers are two-way probabilistic finite automata (AM(2PFA)) with polynomial expected running time. Moreover, we prove that there is a language which can be recognized by an exponential expected running time QAM(2QCFA), but cannot be recognized by any AM(2PFA), and that the NP-complete language $L_{knapsack}$ can also be recognized by a QAM(2QCFA) working only on quantum pure states using unitary operators.



* Corresponding author at: Department of Computer Science, Sun Yat-sen University, Guangzhou 510006, China.
*E-mail address:* issqdw@mail.sysu.edu.cn (D. Qiu).

http://dx.doi.org/10.1016/j.ic.2015.02.003
0890-5401/

## 1. Introduction

An important way to get deeper insights into the power of various quantum resources and operations is to explore the power of various quantum variations of the basic models of classical automata. Of a special interest is to do that for various quantum variations of the classical finite automata, especially for those that use limited amounts of always expensive quantumness – quantum resources: states, correlations, operations and measurements. This paper aims to contribute to such a line of research.

There are two basic approaches toward how to introduce quantum features to classical models of finite automata. The first one is to consider quantum variants of the classical *one-way (deterministic) finite automata* (1FA or 1DFA) and the second one is to consider quantum variants of the classical *two-way finite automata* (2FA or 2DFA). Already the very first attempts to introduce such models, by Moore and Crutchfields [21] as well as Kondacs and Watrous [17] demonstrated that in spite of the fact that in the classical case, 1FA and 2FA have the same recognition power, this is not so for their quantum variations (in case only unitary operations and projective measurements are considered as quantum operations). Moreover, already the first model of *two-way quantum finite automata* (2QFA), namely that introduced by Kondacs and Watrous, demonstrated that quantum variants of 2FA are much too powerful – they can recognize even some *non-context free languages* and are actually not really finite in a strong sense [17]. It started to be therefore of interest to introduce and explore some "less quantum" variations of 2FA and their power [1–3,5,6,18–20,32,33].

A "hybrid" quantum variation of 2FA, namely, *two-way finite automata with quantum and classical states* (2QCFA) was introduced by Ambainis and Watrous [3]. Using this model they were able to show, in an elegant way, that already an addition of a single qubit to a classical model can much increase its power. A 2QCFA is essentially a classical 2FA augmented with a quantum memory of constant size (for states of a fixed Hilbert space) that does not depend on the size of the (classical) input. In spite of such a restriction, 2QCFA have been shown to be more powerful than *two-way probabilistic finite automata* (2PFA) [3,36,37].

In mid 1980s, Babai [4] and Goldwasser et al. [12], independently, introduced so-called *interactive proof systems* with unlimited power provers and polynomial power randomized verifiers. A famous result of [29], stated as IP = PSPACE, that languages recognized by IP are exactly those from PSPACE, demonstrated enormous power hidden in simple interactions of IP.

It is therefore natural to explore power also of some weaker variations of IP. Since unlimited power of provers seems to be very essential for the whole concept of IP, the research started to focus on the cases with limited power verifiers. This has been done at first by Dwork and Stockmeyer [9] – they explored the case that verifiers are *two-way probabilistic finite automata* (IP(2PFA)). They showed that every language in the class EXP can be accepted by some IP(2PFA). However, the set of languages recognized by such IP in which verifiers use *public randomization* (also called Arthur–Merlin proof systems) is a proper subset of $P$. Later, Nishimura and Yamakami [24] explored the case that verifiers are modeled by *one-way quantum finite automata* as well as *two-way quantum finite automata* and demonstrated strengths and weaknesses of both IP.

Of importance is also a variant of IP, called *Arthur–Merlin proof systems* (AM). The difference between IP and AM is that the prover of IP has at each step only *partial information* of the configuration of the verifier while the prover of AM always has *complete information* of the current configuration of the verifier. Also for such *interactive proof systems* it is of importance to explore their power for the case that verifiers have a more limited power and to find out relations between IP and AM with verifiers of different power. AM with verifiers modeled by Turing Machines augmented with a fixed-size quantum register (qAM) were studied also in [34,35] and it was shown that the an NP-complete language $L_{knapsack}$, representing the 0–1 knapsack problem, can be recognized by a qAM whose verifier is a *two-way finite automaton* working on quantum mixed states using superoperators. In Yakaryilmaz's notation, *two-way finite automata* working on quantum mixed states using superoperators are called 2QCFA. However, 2QCFA as defined originally in [3], are working only on quantum pure states using unitary operators. They can be simulated efficiently by *two-way finite automata* working on quantum mixed states, but whether *two-way finite automata* working on quantum mixed states can be simulated by 2QCFA, or not, is unknown. The model of 2QCFA we use is that of [3] and it is weaker, actually a special case of the model used in [34,35]. Our results concerning the acceptance of the language $L_{knapsack}$ are therefore stronger. It is also worth mentioning that a notion of QMA for quantum-automata verifiers was introduced in [23–25] (under the name "public QIP").

Our model will be denoted as QAM(2QCFA). One can see this model also as a classical AM augmented with a quantum memory of constant size – to store quantum states of a fixed Hilbert space – that does not depend on the size of the (classical) input. Our main results show that such models are more powerful than AM(2PFA) – that is AM with 2PFA as verifiers, and the NP-complete language can be recognized by QAM(2QCFA).

The paper is structured as follows. In Section 2 all models involved are described in detail. After that we show for the language $L_{middle} = \{xay \mid x, y \in \{a, b\}^*, |x| = |y|\}$ that for any $0 \leq \varepsilon < 1/2$ there is a QAM(2QCFA) $A(P, V_\varepsilon)$ – with the prover $P$ and the verifier $V_\varepsilon$ that accepts $L_{middle}$ with one-sided error $\varepsilon$ in a polynomial expected running time – notation QAM(ptime-2QCFA). This language cannot be recognized by any AM(2PFA) in polynomial expected running time, as shown in [9]. As we will show in the paper, for the language $L_{mpal} = \{xax^R \mid x \in \{a, b\}^*\}$, that for any $0 \leq \varepsilon < 1/2$ there is a QAM(2QCFA) $A(P, V_\varepsilon)$ that can recognize $L_{mpal}$ with one-sided error $\varepsilon$ in an exponential expected running time. We will prove that this language cannot be recognized at all by an AM(2PFA). These results show that QAM(2QCFA) are more powerful than AM(2PFA). Afterwards we show that there is an NP-complete language, namely $L_{knapsack}$, representing the 0–1 knapsack problem, that can be recognized by QAM(2QCFA) in an exponential expected running time. Finally, we discuss