Information and Computation 239 (2014) 122–148

Contents lists available at ScienceDirect

Information and Computation

www.elsevier.com/locate/yinco

One-way reversible and quantum finite automata with advice ☆,☆☆

Tomoyuki Yamakami

Department of Information Science, University of Fukui, 3-9-1 Bunkyo, Fukui 910-8507, Japan

ARTICLE INFO

Article history:
Received 23 August 2013
Available online 16 October 2014

Keywords:
Reversible finite automaton
Quantum finite automaton
Regular language
Context-free language
Randomized advice
Quantum advice
Rewritable tape

ABSTRACT

We examine the characteristic features of reversible and quantum computations in the presence of supplementary external information, known as advice. In particular, we present a simple, algebraic characterization of languages recognized by one-way reversible finite automata augmented with deterministic advice. With a further elaborate argument, we prove a similar but slightly weaker result for bounded-error one-way quantum finite automata with advice. Immediate applications of those properties lead to containments and separations among various language families when they are assisted by appropriately chosen advice. We further demonstrate the power and limitation of randomized advice and quantum advice when they are given to one-way quantum finite automata.

1. Background, motivation, and challenge

In a wide range of the past literature, various notions of supplemental external information have been sought to empower automated computing devices and the power and limitation of such extra information have been studied extensively. In the early 1980s, Karp and Lipton [11] investigated a role of simple external information, known as *(deterministic) advice*, which encodes useful data, given in parallel with a standard input, into a single string (called an *advice string*) depending only on the size of the input. Such advice has been since then widely used for polynomial-time Turing machines, particularly, in connection to non-uniform circuit families. When *one-way deterministic finite automata* (or 1dfa's, in short) are concerned, Damm and Holzer [7] first studied such advice whose advice string is given "next to" an ordinary input string written on a single input tape. By contrast, Tadaki, Yamakami, and Li [23] provided 1dfa's with advice "in dextroposition with" an input string, simply by splitting an input tape into two tracks, in which the upper track carries a given input string and the lower track holds an advice string. Using the latter model of advice, a series of recent studies [23,25–28] concentrating on the strengths and weaknesses of the advice have unearthed advice's delicate roles for various types of underlying one-way finite automata. Notice that these "advised" automaton models have immediate connections to other important fields, including one-way communication, random access coding, two-player zero-sum games, and pseudorandom generator. Two central questions concerning the advice are: how can we encode necessary information into a piece of advice before a computation starts and, as a computation proceeds step by step, how can we decode and utilize such information stored inside the advice? Whereas there is rich literature on the power and limitation of advice for a model of polynomial-time quantum

☆ An extended abstract appeared in the Proceedings of the 6th International Conference on Language and Automata Theory and Applications (LATA 2012), March 5–9, 2012, A Coruña, Spain, Lecture Notes in Computer Science, Vol. 7183, pp. 526–537, Springer-Verlag, 2012.

☆☆ This work was partly supported by the Mazda Foundation and the Japanese Ministry of Education, Science, Sports, and Culture.

E-mail address: TomoyukiYamakami@gmail.com.

http://dx.doi.org/10.1016/j.ic.2014.10.003
0890-5401/

Turing machine (see, for instance, [1,16,22]), disappointingly, except for the aforementioned studies, little has been known to date for the roles of advice when it is given to finite automata. To promote our understandings of the advice, we intend to expand a scope of our study from 1dfa's to one-way reversible and quantum finite automata.

From theoretical as well as practical interests, we wish to examine two machine models realizing reversible and quantum computations, known as (deterministic) reversible finite automata and quantum finite automata. Since our objective is to analyze the roles of various forms of advice, we want to choose simpler models for reversible and quantum computations in order to make our analysis easier. Of various types of such automata, we intend to initiate our study by limiting our focal point within one of the simplest automaton models: *one-way (deterministic) reversible finite automata* (or 1rfa's, in short) and *one-way measure-many quantum finite automata* (or 1qfa's, thereafter). Although these particular models are known to be strictly weaker in computational power than even regular languages, they still embody an essence of reversible and quantum mechanical computations for which the advice can play a significantly important role. Our 1qfa scans each cell of a read-only input tape by moving a single tape head only in one direction (without stopping) and performs a *(projective) measurement* immediately after every head move, until the tape head eventually scans the right endmarker. From a theoretical perspective, the 1qfa's having more than 7/9 success probability are essentially as powerful as 1rfa's [2], and therefore 1rfa's are important part of 1qfa's. As this fact indicates, for bounded-error 1qfa's, it is not always possible to make a sufficient amplification of success probability. This is merely one of many intriguing features that make an analysis of the 1qfa's distinct from that of polynomial-time quantum Turing machines, and it is such remarkable features that have kept stimulating our research since their introduction in late 1990s. Let us recall some of the numerous unconventional features that have been revealed in an early period of intensive study of the 1qfa's. As Ambainis and Freivalds [2] demonstrated, certain quantum finite automata can be built more state-efficiently than deterministic finite automata. However, as Kondacs and Watrous [12] proved, not all regular languages are recognized with bounded-error probability by 1qfa's. Moreover, by Brodsky and Pippenger [6], no bounded-error 1qfa recognizes languages accepted by minimal finite automata that lack a so-called *partial order condition*. The latter two facts suggest that the language-recognition power of 1qfa's is hampered by their own inability to generate useful quantum states from input information alone.

We wish to understand how advice can change the nature of 1rfa's and 1qfa's. For a bounded-error 1qfa, for instance, an immediate advantage of taking advice is the elimination of the *both* endmarkers placed on the 1qfa's read-only input tape. Beyond such a clear advantage, however, there are numerous challenges lying in the study of the roles of the advice. To analyze the behaviors of "advised" 1qfa's as well as "advised" 1rfa's, we must face those challenges and eventually overcome them. Generally speaking, the presence of advice tends to make an analysis of underlying computations quite difficult and it often demands quite different kinds of proof techniques. As a quick example, a standard *pumping lemma*—a typical proof technique that showcases the non-regularity of a given language—is not quite serviceable to advised computations; therefore, we have already developed other useful tools (e.g., a swapping lemma [25]) for them. In similar light, certain advised 1qfa's fail to meet the aforementioned partial order condition (Lemma 3.4) and, unfortunately, this fact makes a proof technique of Kondacs and Watrous [12] inapplicable to, for example, a class separation between advised regular languages and languages accepted by bounded-error advised 1qfa's.

To overcome foreseen difficulties in out study, our first task must be to lay out a necessary ground work in order to (1) capture fundamental features of those automata when advice is given to boost their language-recognition power and (2) develop methodology necessary to lead to collapses and separations of advised language families. It is the difficulties surrounding the advice for 1qfa's that motivate us to seek different kinds of proof techniques.

In Sections 3.3 and 4.1, we will prove two main theorems. In the first main theorem (Theorem 3.5), with an elaborate argument using a new metric vector space called $\mathcal{Y}_{\mathcal{H}}$, we will show a machine-independent, algebraic necessary condition for languages to be recognized by bounded-error 1qfa's that take appropriate deterministic advice. In the second theorem (Theorem 4.1) for 1rfa's augmented with deterministic advice, we will give a completely machine-independent, algebraic necessary and sufficient condition. These two conditions exhibit certain behavioral characteristics of 1rfa's and 1qfa's when appropriate advice is prepared. Our proof techniques for 1qfa's, for instance, are quite different from the previous work [2,4,6,12,14]. Applying those theorems further, we can prove several class separations among advised language families. These separations indicate, to some extent, inherent strengths and weaknesses of reversible and quantum computations even in the presence of advice.

Another important revelation throughout our study in the field of reversible and quantum computation is the excessive power of *randomized advice* over deterministic advice. In randomized advice [27], advice strings of a fixed length are generated at random according to a pre-determined probability distribution so that a finite automaton looks like "probabilistically" processing each of those generated advice strings together with a standard input. *Quantum advice* further extends randomized advice; however, our current model of 1qfa with "read-only" advice strings inherently has a structural limitation, which prevents quantum advice from being more resourceful than randomized advice. Hence, we will engage in another challenging task of seeking a "simple" modulation of the existing 1qfa's in order to utilize more effectively quantum information stored in quantum advice. We will discuss in Section 5.2 how to remedy the deficiency of the current 1qfa model and which direct implications such a remedy leads to. Similar treatments were already made for various types of one-way quantum finite automata in, e.g., [20,24]. The model of 1qfa itself has been also extended in various directions, including *interactive proof systems* [17–19,29].