Theoretical Computer Science ••• (••••) •••–•••

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Quantum finite automata: Advances on Bertoni's ideas ☆

Maria Paola Bianchi [a], Carlo Mereghetti [b,*], Beatrice Palano [b]

[a] *Department of Computer Science, ETH-Zurich, Universitätstrasse 6, CH-8092 Zürich, Switzerland*
[b] *Dipartimento di Informatica, Università degli Studi di Milano, via Comelico 39, 20135 Milano, Italy*

A R T I C L E   I N F O

Article history:
Received 15 April 2015
Received in revised form 19 December 2015
Accepted 31 January 2016
Available online xxxx

To our friend and mentor
Alberto Bertoni (1946⋆–2014†)

Keywords:
Quantum finite automata
Descriptional complexity

A B S T R A C T

We first outline main steps and achievements along Bertoni's research path in quantum finite automata theory – from the very basic definitions of the models of quantum finite automata throughout the investigation of their computational and descriptional power. Next, we choose to focus on Bertoni's studies on quantum finite automata descriptional complexity. In particular, we expand on a statistical framework for the synthesis of succinct quantum finite automata, discussing its adaptation to the case of multiperiodic events and languages. We then improve such a framework to obtain even more succinct quantum finite automata for some multiperiodic languages. Finally, we introduce some promise problems for multiperiodic inputs, showing that even on this class of problems the descriptional power of quantum finite automata greatly outperforms that of equivalent classical finite automata.

1. Some aspects of Alberto Bertoni's explorations in quantum finite automata theory

Quantum computing is a prolific research area, halfway between physics and computer science [39,43,65]. Most likely, its origins may be dated back to 70's, when some works on quantum information began to appear (see, e.g., [47,50]). In early 80's, R.P. Feynman suggested that the computational power of quantum mechanical processes might be beyond that of traditional computation models [35]. Almost at the same time, P. Benioff already proved that such processes are at least as powerful as Turing machines [7]. In 1985, D. Deutsch [33] proposed the notion of a quantum Turing machine as a physically realizable model for a quantum computer. From the point of view of structural complexity, E. Bernstein and U. Vazirani introduced in [9] the class **BQP** of problems solvable in polynomial time on quantum Turing machines, focusing attention on relations with the corresponding deterministic and probabilistic classes **P** and **BPP**, respectively. Further works in the literature explored classical issues in complexity theory from the quantum paradigm perspective (see, e.g., [8,72,73]).

The first impressive result witnessing quantum power was P. Shor's algorithm for integer factorization, which could run in polynomial time on a quantum computer [70]. (It should be stressed that no classical polynomial time factoring algorithm is currently known. On this fact, the security of many nowadays cryptographic protocols actually relies.) Another relevant progress was made by L. Grover [38], who proposed a quantum algorithm for searching an item in an unsorted database containing n items, which runs in time $O(\sqrt{n})$.

Being both a physicist and a computer scientist, *Alberto Bertoni* naturally approached the study of quantum computing at the beginning of 90's. His first deep investigations in the field are most likely to be singled out in his collaboration with

☆ Partially supported by the Italian MIUR under the project PRIN-2010LYA9RH_005 "PRIN: Automi e Linguaggi Formali: Aspetti Matematici e Applicativi."
* Corresponding author.
E-mail addresses: maria.bianchi@inf.ethz.ch (M.P. Bianchi), mereghetti@di.unimi.it (C. Mereghetti), palano@di.unimi.it (B. Palano).

http://dx.doi.org/10.1016/j.tcs.2016.01.045
0304-3975/

Please cite this article in press as: M.P. Bianchi et al., Quantum finite automata: Advances on Bertoni's ideas, Theoret. Comput. Sci. (2016), http://dx.doi.org/10.1016/j.tcs.2016.01.045

M. Carpentieri, a PhD student at the Department of Computer Science – University of Milano during 1995–99. Carpentieri's PhD activity, supervised by Bertoni, almost entirely dealt with quantum computing, and his doctoral dissertation [30] covered several aspects of the discipline. Of particular interest here is Bertoni and Carpentieri's contribution to the novel (at that time) theory of quantum finite automata.

In this regard, we feel it noteworthy to emphasize that the main body of their research on quantum finite automata was already presented in a version of Carpentieri's doctoral dissertation dating 1996 (the second author of the present paper was an internal reviewer of the dissertation). If we add to the fact that the foundational works on quantum finite automata theory are unanimously considered to be the papers by A. Kondacs and J. Watrous [51] and by C. Moore and J. Crutchfield [63] both issued in 1997, then one may truly grasp the importance of Bertoni and Carpentieri's work within quantum finite automata theory.

Informally, a quantum finite automaton can be obtained by imposing the quantum paradigm – complex state superposition, unitary evolution, quantum measurement – on classical finite automata, e.g., deterministic or probabilistic. Thus, quantum finite automata may represent a theoretical model for a quantum computational device with finite memory. Several observations motivate the introduction and study of quantum finite automata, both theoretical and applied. From a theoretical viewpoint, quantum finite automata computations exhibit all the relevant ingredients of general quantum computing in a slightly more simplified form. So, tackling problems on such "simple" devices may be more manageable and shed some light on questions pertaining to general quantum computers. Yet, it is natural to seek for the simplest model of computation where the quantum paradigm may possibly outperform the classical one. From application perspective, while we can hardly expect to see a full-featured quantum computer in the near future, it is reasonable to envision classical computing devices incorporating small quantum components, i.e., with memory consisting of few quantum bits only. Thus, it is well worth modeling such small components by quantum finite automata, as a tool to explore their computational capabilities.

Bertoni and Carpentieri formally settled the most basic and widely studied model of a quantum finite automaton, named *measure-once quantum finite automaton* later on in the literature [29,40]. Such a model served as a basis for several variants of quantum finite automata introduced and studied in a plenty of contributions (see, e.g., [2,5,17,76]). Being the only model to be considered in the present paper, from now on for the sake of brevity we will simply write "quantum finite automaton" instead of "measure-once quantum finite automaton".

The "hardware" of a quantum finite automaton is that of a classical finite automaton. Thus, we have an input tape scanned by a one-way input head moving one position forward at each move,[1] plus a finite state control. At any given time during the computation, the state of the quantum finite automaton is represented by a complex linear combination of classical states, called a superposition. At each step, a unitary transformation associated with the currently scanned input symbol makes the automaton evolve to the next superposition. Superposition dynamics can transfer the complexity of the problem from a large number of sequential steps to a large number of coherently superposed quantum states. At the end of the input processing, the automaton is observed in its final superposition. This operation makes the superposition collapse to a particular classical state with a certain probability. The probability that the automaton accepts the input word is given by the probability of observing (collapsing into) an accepting state.

Quantum finite automata exhibit both advantages and disadvantages with respect to their classical counterparts. Basically, quantum superposition offers some computational advantages on probabilistic superposition. On the other hand, quantum dynamics must be reversible, and this requirement may impose severe computational limitations to finite memory devices. As a matter of fact, as we will see later on, it is sometimes impossible to simulate classical finite automata by quantum finite automata.

Bertoni's work contributed to explicitly single out both strength and weakness of quantum finite automata. Weakness are pointed out by Bertoni and Carpentieri since the very beginning. In fact, they established the exact *computational power* of the model, proving that quantum finite automata are strictly less powerful than classical finite automata. Precisely, by using a Rabin-like technique and the compactness of the metric space (unit sphere) containing quantum superpositions, they showed that the class of languages accepted with isolated cut point by quantum finite automata coincides with the class of group languages [66], a proper subclass of regular languages. This fundamental result was published only in 2001 [11], and independently proved in [29] though in a slightly less general form. Further relevant results concerning the power of quantum finite automata (among others: some closure properties, regularity conditions, and a "pumping lemma" for languages accepted by quantum finite automata) may be found in [12], again published only in 2001.

From the scenario depicted so far, it was clear that the strength of quantum finite automata has not to be found in "what" they do, but possibly in "how" they work. Following this guideline, Bertoni, together with the authors of the present paper, switched the research focus from the computational to the *descriptional power* of quantum finite automata, thus settling investigations on the area of descriptional complexity. In this discipline, roughly speaking, the models of computation are studied on the basis of their size. Typical questions under examination are, e.g., size upper and lower limits for accomplishing certain tasks, or comparing the size of different models to single out their descriptional power, i.e., the ability to operate succinctly. For finite automata, a natural and widely used size measure is the number of control states. In this regard, probably the first well known result in the descriptional complexity is the optimal exponential gain on the descrip-

[1] This type of automaton is sometimes referred to as *real time* automaton [40,63], stressing the fact that it can never perform stationary moves.

Please cite this article in press as: M.P. Bianchi et al., Quantum finite automata: Advances on Bertoni's ideas, Theoret. Comput. Sci. (2016), http://dx.doi.org/10.1016/j.tcs.2016.01.045