SIMULATING THE PROBABILISTIC BY A QUANTUM FINITE AUTOMATA

GATIS MIDRIJĀNIS*

University of Latvia, Raiņa bulvāris 29, Riga, Latvia. e-mail: mgatis@inbox.lv

Abstract

We present a language L_n which is recognizable by a probabilistic finite automaton (PFA) with probability $1-\epsilon$ for all $\epsilon > 0$ with $O(log^2 n)$ states, with a deterministic finite automaton (DFA) with $O(n)$ states, but a quantum finite automaton (QFA) needs at least $2^{\Omega(n/\log n)}$ states.

A PFA is generalization of DFA. Many authors have tried to find out ([AF98], [Fre82], [Amb96], [Ras00] a. o.) the size advantages of PFA over DFA. On the other side it is known ([ANTSV98], [AF98]) that the size of reversible finite automata (RFA) and the size of QFA exceed the size of the corresponding DFA almost exponentially for some regular languages (i.e. for languages recognizable by DFA). And so A. Ambainis, A. Nayak, A. Ta-Shma, U. Vazirani [ANTSV98] wrote:

> *Another open problem involves the blow up in size while simulating a 1-way PFA by a 1-way QFA. The only known way for doing this is by simulating the PFA by a 1-way DFA and then simulating the DFA by a QFA. Both simulating a PFA by a DFA (*[Amb96], [Fre82], [Rab63]*) and simulating DFA by a QFA (this paper) can involve exponential or nearly exponential increase in size. This means that the straightforward simulation of a probabilistic automaton by a QFA (described above) could result in a doubly-exponential increase in size. However, we do not known of any examples where both transforming a PFA into a DFA and transforming a DFA into a QFA cause big increases of size. Better simulations of PFA by QFAs may well be possible.*

We solve this problem.

We use the definition of 1-way QFA (further in text simply QFA) as in [AF98] and [ANTSV98]. This model was first introduced in [KW97]. A RFA is a QFA with elements only 0 and 1 in the matrices. A PFA is the same as a QFA but only instead of unitary matrices it has stochastic ones. A DFA is a PFA with only 0 and 1 in the matrices. More exact definitions one can find, for example, in [AF98].

Our main result:

Theorem 1. *For all $k \geq 1$, $n = 2^*k$, we define language*

$$L_n = \{\omega \in \{0,1\}^n : \exists x, y \in \{0,1\}^* : \omega = x00y\}.$$

(0) *There is a RFA (so also a QFA, a PFA and a DFA) that recognize L_n.*

*Research supported by Grant No.01.0354 from the Latvian Council of Science, and Contract IST-1999-11234 (QAIP) from the European Commission.

(1) *Any RFA that recognizes L_n, has at least $2^{O(n)}$ states.*
(2) *Any QFA that recognizes L_n with probability $p > 1/2$, has at least $2^{\Omega(\frac{n}{\log n})}$ states.*
(3) *Any DFA that recognizes L_n, has at least $O(n)$ states.*
(4) *For any $\epsilon > 0$, there is a PFA with $O(\log^2 n)$ states recognizing L_n with probability $1 - \epsilon$.*

Sketch of proof. 0th part. Easy.

1st part. We look words in form $a_1 1 a_2 1 a_3 1 a_4 1 a_5 1 a_6 1 ... a_k 1$, where $a_i \in \{0, 1\}$. We prove that automaton always has to branch at every a_i. Suppose contrary, there is a_i where automaton goes to the same state whether it read $a_i = 0$ or $a_i = 1$. Then forward we give the next symbols 01^{n-2i} and automaton cannot decide what to answer. So it must branch for every a_i, we can say it "*remembers*" this bit. But maybe it can merge ("*forget*") afterwards? No, because it cannot merging with the same symbol are forbidden by reversibility, but with different symbols by the same reason as branching must occur.

2nd part. We use technique introduced in [ANTSV98] and ideas from 0th part to show that there must be a serial quantum encoding of the a_is over bases states and obtain such account of states.

3rd part. Evident.

4rd part. It easy to see that there is a simple deterministic automata that recognize language where two 0s are adjacent. The only problem is to compute when there are exactly n symbols in the word. But this problem is solved by Freivalds. Freivalds [Fre82] showed that there is a PFA that recognizes language L_n consisting of one word a^n with arbitrary hight probability. We construct our probabilistic automata to compute the both these things parallel. □

We have shown that sometimes quantum automata must be almost doubly exponential larger than classical automaton. As follows from result of Ambainis and Freivalds [AF98], doubly exponential increase is the maximum for a QFA with high enough (this was precisely computed by Ambainis and Ķikusts [AK01] - greater than $\frac{52+4\sqrt{7}}{81} = 0.7726...$) probability of success. But it is not clear how it is when we allow smaller probability of correctness. Author do not now any lower or upper bound in this case.

References

[AF98] Andris Ambainis and Rusins Freivalds. 1-way quantum finite automata: strengths, weaknesses and generalizations. *Proc. 39th FOCS*, pages 332–341, 1998.

[AK01] Andris Ambainis and Arnolds Kikusts. Exact results for accepting probabilities of quantum automata. 2001. quant-ph/0109136.

[Amb96] Andris Ambainis. The complexity of probabilistic versus deterministic finite automata. *Lecture Notes in Computer Science*, (1178):233–237, 1996.

[ANTSV98] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani. Dense quantum coding and a lower bound for 1-way quantum automata. 1998. quant-ph/9804043.

[Fre82] Rusins Freivalds. On the growth of the number of states of determinization of probabilistic automata. *Avtomatika i Vychislitelnaja Tehnika*, 3:39–42, 1982. (in Russian).

[KW97] Attila Kondacs and John Watrous. On the power of quantum finite state automata. *Proc. 38th FOCS*, pages 66–75, 1997.

[Rab63] M. O. Rabin. Probabilistic automata. *Information and Control*, 6:230–245, 1963.

[Ras00] Zigmars Rascevskis. The complexity of probabilistic versus deterministic finite automata. 2000.