

一方向量子有限オートマトンの初期状態の不完全性

ルディレイモンド H.P.[†], 天野 正己[‡], 岩間 一雄[†]

[†] 京都大学大学院情報学研究科

[‡] IBM 東京基礎研究所

要旨本稿では、1QFA(一方向量子有限オートマトン)の初期状態が不完全な場合、最終的な受理確率にどのような影響を与えるかについて述べる。具体的には、初期状態が $|\Psi\rangle$ と $|\Psi'\rangle = \sqrt{1-\delta}|\Psi\rangle + \sqrt{\delta}|\epsilon\rangle$ で、それ以外は同じ2つのQFAの受理確率の差が同じ入力に対して高々 $\sqrt{\delta}$ であることを示す。

Imperfections in Initial States of 1-QFAs

Rudy Raymond H.P.[†], Masami Amano[‡] and Kazuo Iwama[†]

[†] School of Infomatics, Kyoto University, Kyoto, Japan

[‡] IBM Tokyo Research Lab, Tokyo, Japan

Abstract We consider a 1-way Quantum Finite Automata (1QFA) that has imperfections in initial states. We show that for a 1QFA with initial state $|\Psi\rangle$ and the same 1QFA with initial state $|\Psi'\rangle$, where $|\Psi'\rangle = \sqrt{1-\delta}|\Psi\rangle + \sqrt{\delta}|\epsilon\rangle$, their accepting probabilities differ at most $\sqrt{\delta}$ for the same input sequence.

1 Introduction

It is well accepted to assume that a quantum computer in the early stage will be an elementary system, e.g., a quantum (combinatorial) circuit or a quantum sequential machine with a stage register of small size. The latter is usually modeled as a quantum finite automaton (QFA), which has been constantly popular in the recent literature [KW97], [AF98], [AI99]. However, even if we were able to design a finite automaton M whose operation satisfies our purpose perfectly, there are still several difficulties when using it, including the difficulty of resetting M before starting its operation. Reset can be done by increasing the amplitude of the initial state vector, say $|00\dots 0\rangle$. This however means that it is reasonable to assume that there remain several other vectors (like $|100\dots 0\rangle$) with small amplitudes. Namely, the initial state vector is not $|\Psi\rangle = |q_0\rangle$ but $|\Psi'\rangle = \sqrt{1-\delta}|\Psi\rangle + \sqrt{\delta}|\epsilon\rangle$.

In this paper we investigate how this erroneous vector $|\epsilon\rangle$ changes accepting and/or rejecting probabilities of input sequences compared to the original probabilities for $|\epsilon\rangle = 0$. If QFA's includes only unitary transformations, then it is well known that the difference of two vectors are preserved by the transformation, which implies that the initial error can expand only limitedly. Our results in this paper show that the probability of acceptance (and rejection also) does not change by more than $\sqrt{\delta}$. Namely, the error in the initial state does not expand with the number of operation steps. This result is used to show a similar result for the model which uses mixed-states for the imperfection; we show that the imperfection in the density matrix can be decomposed into imperfections in pure states.

Note that δ is supposed to be a small positive value less than one. Then the additional term $\sqrt{\delta}$ can be much larger than δ ; for instance if $\delta = 0.01$, $\sqrt{\delta} = 0.1$. Note that the amount of difference in the initial vector can be regarded as δ in terms of probability. Thus, our result shows that the expansion of the initial error is certainly bounded, but the bound itself is not small and may be somewhat serious in certain cases. Actually there is a specific example of 1QFA for which the initial error δ results in the difference $\sqrt{\delta(1-\delta)}$ of the accepting probability. The expansion is apparently due to a coherence between the initial state and the error state. There is no expansion in the mixed-state model where such incoherence does not exist.

The issue of imperfection has already been discussed for quantum TMs (QTMs) [BV97], mainly motivated by the needed precision of state transitions (for example real amplitudes must be simulated by rational ones in digital systems). In [BV97], Bernstein and Vazirani showed the error in each step of evolution only adds and the total error does not increase exponentially as in the case of classical computation. However, in the case of QTMs it is enough to conduct observation only once at the end of computation, and therefore we can assume that the overall evolutions is unitary. This is an important difference compared to our present case as mentioned already.

2 Models

In this section, we consider two different models of 1-way Quantum Finite Automata (1QFAs), Many-Measurements 1QFAs (MM-1QFAs) and Measurement-One 1QFAs (MO-1QFAs). As the name implies, the head of a 1QFA always moves one way from left to right. A 1QFA consists of a classical head which reads an input string on the classical tape. The difference between 1QFAs and 1FAs is that internal states of a 1QFA are quantum states.

We use the following standard definition of MM-1QFAs which originally appeared in [KW97].

Definition 1 A Many-Measurements 1QFA (MM-1QFA) M is specified by a 6-tuple

$$M = (Q, \Sigma, \delta, q_0, Q_{acc}, Q_{rej}),$$

where Q is a finite set of states, Σ is an input alphabet, δ is a transition function, $q_0 \in Q$ is a starting state and $Q_{acc} \subset Q$ and $Q_{rej} \subset Q$ are sets of accepting and rejecting states with $Q_{acc} \cap Q_{rej} = \emptyset$. The transition function

$$\delta : Q \times \Gamma \times Q \rightarrow C_{[0,1]},$$

where $\Gamma = \Sigma \cup \{\#, \$\}$ is the tape alphabet of M . $\#$ and $\$$ are left and right end-markers not in Σ . Thus, the value of $\delta(q_1, \sigma, q_2)$ is the amplitude of $|q_2\rangle$ in the superposition states to which M goes from $|q_1\rangle$ after reading σ . For $\sigma \in \Sigma$, V_σ is a linear transformation on $l_2(Q)$ (the space of mappings from Q to C with l_2 norm) defined by

$$V_\sigma(|q_1\rangle) = \sum_{q_2 \in Q} \delta(q_1, \sigma, q_2) |q_2\rangle.$$

V_σ is required to be unitary.

The computation of M starts in the superposition $|q_0\rangle$. Then transformations corresponding to the input characters are applied. The transformation corresponding to $\sigma \in \Sigma$ consists of two steps.

1. The linear transformation corresponding to σ , V_σ , is applied to obtain the new superposition $\Psi' = V_\sigma(\Psi)$, where Ψ is the superposition before applying V_σ .
2. Ψ' is observed with respect to the observable $E_{acc} \oplus E_{rej} \oplus E_{non}$, where $E_{acc} = \text{span}\{|q\rangle : q \in Q_{acc}\}$, $E_{rej} = \text{span}\{|q\rangle : q \in Q_{rej}\}$, $E_{non} = \text{span}\{|q\rangle : q \in Q_{non}\}$. Here, E_{acc} , E_{rej} and E_{non} are the orthogonal decomposition of $l_2(Q)$, i.e. $l_2(Q) = E_{acc} \oplus E_{rej} \oplus E_{non}$. Denote by P_{acc} , P_{rej} and P_{non} the projection operator into the subspace E_{acc} , E_{rej} and E_{non} respectively. Observation gives $x \in E_i$ with the probability equal to the amplitude of the projection of Ψ' . After that, the superposition collapses to this projection.

Thus, on input string $\sigma_1\sigma_2\dots\sigma_n$ when no termination occurs, the computation can be seen as an application of the composed operator

$$V'_{\sigma_n} V'_{\sigma_{n-1}} \dots V'_{\sigma_1} |q_0\rangle,$$

where $V'_{\sigma_i} = P_{non} V_{\sigma_i}$.

[CM97] introduced a different model of 1QFA in which only one measurement is performed, at the end of its computation. This model is denoted as an MO-1QFA.

Definition 2 A Measurement-One 1QFA (MO-1QFA) M is specified by a 5-tuple

$$M = (Q, \Sigma, \delta, q_0, Q_{acc}),$$

where Q , Σ , δ , q_0 and Q_{acc} are defined similarly as MM-1QFA. Note that there is no rejecting state set. For an input string $\sigma_1\sigma_2\dots\sigma_n$, measurement is performed only once, i.e., after M finished reading σ_n .

3 Imperfections using Mixed-States Models

It is very popular to consider 1QFAs with a mixed state as their starting states. The reason is that in general, a quantum system is not in a pure state, since our knowledge about the system is only partial. For this purpose, we need the definition of a mixed state and its corresponding density operator.

Definition 3 A probability distribution $\{(p_i, \Phi_i) | 1 \leq i \leq k\}$ on pure states $\{\Phi_i\}_{i=1}^k$, with probabilities $0 < p_i \leq 1$, $\sum_{i=1}^k p_i = 1$, is called a mixed state, and denoted by $[\Psi] = \{(p_i, \Phi_i) | 1 \leq i \leq k\}$. To each mixed state $[\Psi]$ corresponds a density operator which is uniquely represented in the matrix form through density matrix. If $[\Psi] = \{(1.0, |\Phi\rangle)\}$ for a pure state $|\Phi\rangle$, then the density matrix ρ is defined as $\rho = |\Phi\rangle\langle\Phi|$. If $[\Psi] = \{(p_i, \Phi_i) | 1 \leq i \leq k\}$, where $|\Phi_i\rangle$ are pure states, then the density matrix ρ corresponds to $[\Psi]$ is $\rho = \sum_{i=1}^k p_i |\Phi_i\rangle\langle\Phi_i|$.

It is easy to deduce from the definition above, that if at any time the state of a 1QFA can be described by a density matrix ρ , then its transformation corresponding to a symbol $\sigma \in \Gamma$ is

$$\rho' = U_\sigma \rho U_\sigma^*.$$

Namely, its density matrix ρ is transformed to ρ' . Furthermore, measurements on density matrix ρ can be considered as measurements with respect to the observable $E_{acc} \oplus E_{rej} \oplus E_{non}$ as described before. The probability of observing E_i is equal to $Tr(P_i \rho)$, where P_i is the orthogonal projection onto E_i . If we observe E_{acc} or E_{rej} , the input is accepted or rejected respectively. In MM-1QFA model, the computation continues with the state $P_{non} \rho P_{non}$, and the next transformation, if any, is applied.

Thus, in the mixed-state model, everything is defined using density matrices. Furthermore, two different mixed states can correspond to the same density matrix (see, for instance, page 372 of [Gru99]). Nevertheless, as the next theorem shows, we can make some kind of argument without using density matrices.

Theorem 1 If an MM-1QFA M with pure initial states $|\Psi_k\rangle$ results in the accepting (rejecting) probability $Pr(acc)(\Psi_k)$ ($Pr(rej)(\Psi_k)$), then M with mixed states $(p_k, |\Psi_k\rangle)$ for $k = 1, 2, \dots, n$ where $\sum_{k=1}^n p_k = 1$, results in the accepting (rejecting) probability $\sum_{k=1}^n p_k Pr(acc)(\Psi_k)$ ($\sum_{k=1}^n p_k Pr(rej)(\Psi_k)$).

Proof. It is trivial that if density matrix ρ of an MM-1QFA M is composed of pure states $|\Phi_k\rangle$ for $k = 1, 2, \dots, n$, then the density matrix of M after performing unitary transformation and measurement, i.e. the non-halting, accepting and rejecting projection, can be written as follows:

$$\rho' = P_{non} U \rho U^* P_{non}.$$

Since $\rho = \sum_{k=1}^n |\Phi_k\rangle\langle\Phi_k|$, we obtain

$$\rho' = \sum_{k=1}^n P_{non} U |\Phi_k\rangle\langle\Phi_k| U^* P_{non} = \sum_{k=1}^n |\Phi'_{k,non}\rangle\langle\Phi'_{k,non}|.$$

Here we use $|\Phi'_{k,non}\rangle = P_{non} U |\Phi_k\rangle$. From the equation above, it can be concluded that if a density matrix of M is composed of pure states $|\Phi_k\rangle$ for $k = 1, 2, \dots, n$, then the new density matrix after performing unitary transformation U and measurement is composed of pure states $P_{non} U |\Phi_k\rangle$ for $k = 1, 2, \dots, n$.

Suppose at the j -th step the density matrix of M is

$$\rho_j = \sum_{k=1}^n p_k |\Psi_{k,non}^j\rangle\langle\Psi_{k,non}^j|,$$

where $|\Psi_{k,non}^j\rangle$ is the nonhalting states of M at the j -th step when started in initial state $|\Psi_k\rangle$. Then the accepting probability obtained at the $j+1$ -th step p_{acc}^{j+1} can be written as follows.

$$\begin{aligned} p_{acc}^{j+1} &= tr(P_{acc} U \rho_j U^* P_{acc}) = \sum_{k=1}^n p_k tr(P_{acc} U |\Psi_{k,non}^j\rangle\langle\Psi_{k,non}^j| U^* P_{acc}) \\ &= \sum_{k=1}^n p_k tr(\langle\Psi_{k,non}^j| U^* P_{acc} P_{acc} U |\Psi_{k,non}^j\rangle) \\ &= \sum_{k=1}^n p_k \|P_{acc} U |\Psi_{k,non}^j\rangle\|^2 = \sum_{k=1}^n p_k p_{k,acc}^{j+1}, \end{aligned}$$

where $p_{k,acc}^{j+1}$ is the accepting probability obtained at the $j+1$ -th step if M started in initial state $|\Psi_k\rangle$.

Hence, the total accepting probability of M with mixed states $(p_k, |\Psi_k\rangle)$ for $k = 1, 2, \dots, n$, where $\sum_{k=1}^n p_k = 1$ and input string length is l , can be written as follows.

$$Pr(acc) = \sum_{k=1}^n p_k \sum_{j=1}^l p_{acc,k}^j = \sum_{k=1}^n p_k Pr(acc)(\Psi_k).$$

Thus, we have the proof of the theorem for the accepting probability. The same explanation holds for the rejecting probability. \square

Note that Theorem 1 also holds for MO-1QFA, since MO-1QFA is a special case of MM-1QFA. We now apply Theorem 1 to preparation of initial quantum state of 1QFA M which starts from the expected pure initial state Ψ with probability $1 - \delta$ and the erroneous state ϵ with probability δ compared to M started in the expected pure quantum states Ψ with probability 1. One can see that if the erroneous QFA results in accepting probability $Pr'(acc)$ and the error-free QFA results in $Pr(acc)$, then $|Pr'(acc) - Pr(acc)| \leq \delta$. Thus the imperfection in the density matrix can be decomposed into imperfections in pure states, which will be discussed in the next section.

4 Imperfections in Preparation of MO-1QFA

We consider an MO-1QFA M with initial state vector $|\Psi\rangle$ and compare it with the same M that has initial state vector $|\Psi'\rangle = \sqrt{1 - \delta}|\Psi\rangle + \sqrt{\delta}|\epsilon\rangle$, where $|\epsilon\rangle$ is a normalized error vector. If the input string is $\#\sigma_1 \cdots \sigma_n\$, then the final accepting probability of M can be written as follows:$

$$Pr(acc)(\Psi') = Tr(P_{acc}U|\Psi'\rangle\langle\Psi'|U^*P_{acc}),$$

where $U = V_{\S}V_{\sigma_n} \cdots V_{\sigma_1}V_{\#}$ denotes the unitary operator of state transitions.

Theorem 2 *If an MO-1QFA M with initial state $|\Psi'\rangle$ results in the accepting probability $Pr(acc)(\Psi')$ and M with initial state $|\Psi\rangle$ results in the accepting probability $Pr(acc)(\Psi)$, where $|\Psi'\rangle = \sqrt{1 - \delta}|\Psi\rangle + \sqrt{\delta}|\epsilon\rangle$, and $\langle\Psi'|\Psi'\rangle = \langle\Psi|\Psi\rangle = \langle\epsilon|\epsilon\rangle = 1$, then $|Pr(acc)(\Psi') - Pr(acc)(\Psi)|$ is at most $\sqrt{\delta}$.*

Proof. For simplicity we denote $\rho' = |\Psi'\rangle\langle\Psi'|$ and $\rho = |\Psi\rangle\langle\Psi|$. It is straightforward to show that

$$\begin{aligned}(\rho' - \rho) &= -\delta|\Psi\rangle\langle\Psi| + \delta|\epsilon\rangle\langle\epsilon| + \sqrt{\delta(1 - \delta)}(|\Psi\rangle\langle\epsilon| + |\epsilon\rangle\langle\Psi|), \\(\rho' - \rho)^2 &= \delta(|\Psi\rangle\langle\Psi| + |\epsilon\rangle\langle\epsilon|).\end{aligned}$$

It holds for the difference of accepting probability that

$$\begin{aligned}|Pr(acc)(\Psi') - Pr(acc)(\Psi)| &= |Tr(P_{acc}U(\rho' - \rho)U^*P_{acc})| \\ &\leq Tr|P_{acc}U(\rho' - \rho)U^*P_{acc}| \\ &= Tr\left(\sqrt{U(\rho' - \rho)^2U^*P_{acc}}\right),\end{aligned}$$

where $U = V_{\S}V_{\sigma_n} \cdots V_{\sigma_1}V_{\#}$. At the third line of the above equation, we use $|A| = \sqrt{AA^*}$ and $Tr(AB) = Tr(BA)$, to obtain the equation at the fourth line. Note that since P_{acc} is an orthogonal projection operator to accepting sub-space, $\sqrt{P_{acc}P_{acc}} = P_{acc}$.

Similarly for the rejecting probability, we get

$$|Pr(rej)(\Psi') - Pr(rej)(\Psi)| \leq Tr\left(\sqrt{U(\rho' - \rho)^2U^*P_{rej}}\right),$$

where P_{rej} is an orthogonal projection operator to rejecting sub-space. Since $P_{acc} + P_{rej} = I$, we can combine the last two inequalities and use $(\rho' - \rho)^2$ to obtain

$$\begin{aligned}|Pr(acc)(\Psi') - Pr(acc)(\Psi)| + |Pr(rej)(\Psi') - Pr(rej)(\Psi)| &\leq Tr\left(\sqrt{U(\rho' - \rho)^2U^*}\right) \\ &= Tr\left(\sqrt{(\rho' - \rho)^2}\right) \\ &= 2\sqrt{\delta}.\end{aligned}$$

Because the difference of accepting probabilities is equal to that of the rejecting ones, the upper bound above is twice of the value we want to prove. Thus the difference of accepting probability is at most $\sqrt{\delta}$. \square

5 Imperfections in Preparation of MM-1QFA

To analyze the effect of imperfection in the initial state of MM-1QFA M , it is important to point out the fact that MM-1QFA is actually an MO-1QFA with states growing linearly with its input length. Although simulating an MM-1QFA by an MO-1QFA this way contradicts the finite automaton definition, the size of states of MO-1QFA is still finite relative to its input length. Thus we can apply our previous proof of accepting differences of MO-1QFA to that of MM-1QFA, since the proof holds for operators with finite dimensions.

Therefore we obtain the following theorem for MM-1QFA.

Theorem 3 *If an MM-1QFA M with initial state $|\Psi'\rangle$ results in the accepting probability $Pr(acc)(\Psi')$ and M with initial state $|\Psi\rangle$ results in the accepting probability $Pr(acc)(\Psi)$, where $|\Psi'\rangle = \sqrt{1-\delta}|\Psi\rangle + \sqrt{\delta}|\epsilon\rangle$ and $\langle\Psi'|\Psi'\rangle = \langle\Psi|\Psi\rangle = \langle\epsilon|\epsilon\rangle = 1$, then $|Pr(acc)(\Psi') - Pr(acc)(\Psi)|$ is at most $\sqrt{\delta}$.*

Thus, we have shown that for both models of MO-1QFAs and MM-1QFAs, the difference of the accepting probability is at most $\sqrt{\delta}$. To see how tight our result is, we show that there is an MM-1QFA which has the accepting probability difference $\sqrt{\delta(1-\delta)}$ on certain input sequences, when started in the starting state $\sqrt{1-\delta}|q_0\rangle + \sqrt{\delta}|q_1\rangle$ instead of $|q_0\rangle$. In fact, our example is the MM-1QFA to recognize the language $\#a^*b^*\$$ which appeared in [AF98]. Details of this MM-1QFA are shown in the next section.

6 Example

[AF98] used the following MM-1QFA, here denoted as M_0 , to recognize the language $L_0 = \{\#a^*b^*\$$.

$$M_0 = (\{q_0, q_1, q_2, q_3, q_4\}, \{a, b\}, \delta, q_0, \{q_3\}, \{q_4\}),$$

with the transition function δ is specified by transitions:

$$\begin{aligned} V_{\#} |q_0\rangle &= \sqrt{1-p} |q_1\rangle + \sqrt{p} |q_2\rangle, \\ V_a |q_1\rangle &= (1-p) |q_1\rangle + \sqrt{p(1-p)} |q_2\rangle + \sqrt{p} |q_4\rangle, \\ V_a |q_2\rangle &= \sqrt{p(1-p)} |q_1\rangle + p |q_2\rangle - \sqrt{1-p} |q_4\rangle, \\ V_b |q_1\rangle &= |q_4\rangle, V_b |q_2\rangle = |q_2\rangle, \\ V_{\$} |q_1\rangle &= |q_4\rangle, V_{\$} |q_2\rangle = |q_3\rangle, \end{aligned}$$

and the remaining transitions are defined arbitrarily so that unitary requirements are satisfied.

They showed that if $x \in L_0$, then M_0 will accept x with probability at least p and if $x \notin L_0$, then M_0 will reject x with probability at least $1-p^3$. Thus, L_0 can be recognized with probability greater than $1/2$. In fact, [AF98] showed that M_0 can recognize L_0 with the highest probability $p \approx 0.68$, i.e. the solution of $p = 1 - p^3$.

For our purpose, we add

$$V_{\#} |q_1\rangle = -\sqrt{p} |q_1\rangle + \sqrt{1-p} |q_2\rangle$$

to M_0 . Certainly even after this addition the unitary requirements are still satisfied.

Then, if M_0 starts in $\sqrt{1-\delta}|q_0\rangle + \sqrt{\delta}|q_1\rangle$, then M_0 accepts $\#b^*\$$ with probability $p + \delta - 2\delta p + 2\sqrt{p(1-p)\delta(1-\delta)}$. Since M_0 which starts in $|q_0\rangle$ accepts $\#b^*\$$ with probability p , then the difference of the accepting probability is $\delta - 2\delta p + 2\sqrt{p(1-p)\delta(1-\delta)}$. For $p \approx 0.68$, this difference is approximately $-0.36\delta + 0.93\sqrt{\delta(1-\delta)}$. However if $p = 1/2 + e$ for $e > 0$, note that M_0 still recognizes L_0 with probability larger than $1/2$, then the difference of the accepting probability on input $\#b^*\$$ can be very close to $\sqrt{\delta(1-\delta)}$, since

$$\lim_{p \rightarrow 1/2} (\delta - 2\delta p + 2\sqrt{p(1-p)\delta(1-\delta)}) = \sqrt{\delta(1-\delta)}.$$

Thus, we have shown that there is an MM-1QFA which has the difference $\sqrt{\delta(1-\delta)}$ in its accepting probability on certain input sequences.

7 Concluding Remarks

Our study in this paper reveals that imperfection in preparation of 1QFA results in a limited error term, i.e. there is no growth of error despite of measurements performed during its computation. We prove that the difference is at most $\sqrt{\delta}$. Using the model of MM-1QFA shown in [AF98], we show the example of MM-1QFA which has $\sqrt{\delta(1-\delta)}$ difference of accepting probability, i.e. our result is somewhat tight.

Studies on imperfection using mixed states also reveal the similar result, but the difference of the accepting probability is at most δ , where δ is the probability of having the erroneous initial state ϵ .

References

- [AF98] A. Ambainis and R. Freivalds. 1-way quantum finite automata: strengths, weaknesses and generalizations. In *Proceedings of the 39th IEEE Conference on Foundations of Computer Science*, pages 332–341, 1998.
- [AI99] M. Amano and K. Iwama. Undecidability on quantum finite automata. In *Proceedings of the 31st ACM Symposium on Theory of Computing*, pages 368–375, 1999.
- [BV97] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997.
- [CM97] James P. Crutchfield Christopher Moore. Quantum automata and quantum grammars. *Theoretical Computer Science, to appear*, 1997.
- [Gru99] Josef Gruska. *Quantum Computing*. Mc Graw Hill, 1999.
- [KW97] A. Kondacs and J. Watrous. On the power of quantum finite automata. In *Proceedings of the 38th IEEE Conference on Foundations of Computer Science*, pages 66–75, 1997.