Lecture 5

CMPE 598 - QUANTUM ALGORITHMS

Aytaç PAÇAL

March 6, 2018

1 Previously

a Exact Computation

- State economy advantage in some promise problems.
- No advantage in terms of state economy for regular language recognition.
- What about ability to recognize non-regular languages?

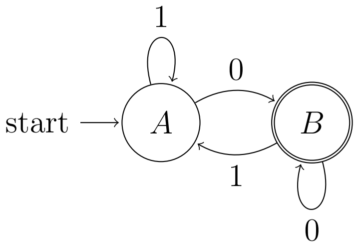
b Non-Determinism (One-sided unbounded error)

A machine which can make errors, but it is not supposed to make any errors when the input is not a member of the language. If the input is not a member of the language, it is supposed to reject it with the probability 1. But if the input is the member of the language, it may make some errors as long as it does not make errors with probability 1. We demonstrated a language which does not hava a classical FA but does have a QFA.

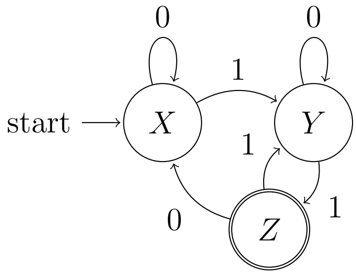
2 Bounded Error

Claim. *If you have a real time machine with bounded error (say, it gives the wrong answer with probability at most 1/3 in any run to any input), then you can build another real-time machine from the same problem with a much much smaller error bound (any error bound greater than zero).*

M_1



M_2



In matrix representation,

$$
\underset{M_1}{\begin{array}{c|cc|}
 & A & B \\ \hline
A & 1 & 1 \\
B & 0 & 0 \\ \hline
\end{array}}
\qquad
\underset{M_2}{\begin{array}{c|ccc|}
 & X & Y & Z \\ \hline
X & 0 & 0 & 0 \\
Y & 1 & 0 & 1 \\
Z & 0 & 1 & 0 \\ \hline
\end{array}}
\tag{1}
$$

We want to make a new machine that accept the string as if the both machine is working in parallel. In other words, both machine should be in the accept state for the string to be accepted by the combined machine. The combined machine will have the pair of state sets (AX, AY, AZ etc.) To find it, we use the tensor product.

Qubits Remember, qubits are 2 state systems $\begin{pmatrix} \cdot \\ \cdot \end{pmatrix}$. We defined

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Let's define 2 qubits by combination of these, for example,

$$\begin{pmatrix} \frac{3}{5} \\ \frac{1}{5} \end{pmatrix} = \frac{3}{5}|0\rangle + \frac{1}{5}|1\rangle \qquad \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} \tag{2}$$

The combined system is the tensor product of these 2 systems.

Tensor Product

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ a_1 b_3 \\ \vdots \\ a_1 b_m \\ a_2 b_1 \\ \vdots \\ a_2 b_m \\ \vdots \\ a_n b_m \end{pmatrix} \tag{3}$$

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \\ a_{11} & \cdots & \cdots & a_{nn} \end{bmatrix} \otimes \begin{bmatrix} & B & \end{bmatrix} = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \cdots & a_{nn}B \end{bmatrix} \tag{4}$$

If we take the tensor product of M_1 and M_2 in (1), we obtain the combined DFA in (5).

	AX	AY	AZ	BX	BY	BZ
AX	0	0	0	0	0	0
AY	1	0	1	1	0	1
AZ	0	1	0	0	1	0
BX	0	0	0	0	0	0
BY	0	0	0	0	0	0
BZ	0	0	0	0	0	0

(5)

Combined state matrix

If we do the same thing for a probabilistic machine,

	A	B
A	0.5	1
B	0.5	0

M_1

	X	Y	Z
X	0	0	0
Y	1/3	0	1/3
Z	2/3	1	0

M_2

$$
\begin{array}{c|cccccc|}
 & AX & AY & AZ & BX & BY & BZ \\
\hline
AX & 0 & 0 & 0 & 0 & 0 & 0 \\
AY & 1/6 & 0 & 1/2 & 1/3 & 0 & 1 \\
AZ & 1/3 & 1/2 & 0 & 2/3 & 1 & 0 \\
BX & 0 & 0 & 0 & 0 & 0 & 0 \\
BY & 1/6 & 0 & 1/2 & 0 & 0 & 0 \\
BZ & 1/3 & 1/2 & 0 & 0 & 0 & 0 \\
\hline
\end{array}
$$

Combined state matrix

If originally in AY, after reading a "1", M_1 goes from A to A or B with probability 1/2 each, M_2 goes to Z with prob 1. So combined machine goes from AY to AZ or BZ with probability 1/2 each.
So, what should be the accept state?

- Take a PFA working with error bound 1/3.
- Construct a PFA running 101 copies of that PFA in parallel.
- The accepted states are the ones corresponding to tuples of 51 or more (i.e. majority of) accepted states from the original machines.

One can easily show that, columns of the combined matrix also add up to 1.

3 QFA's

Let's say we have two machine, Q_1 and Q_2, with different state sets. Combined machine will have $s_1t_1, s_1t_2, s_1t_3, s_2t_1, s_2t_2, s_2t_3$ states. The first machine has 2 probabilistic choices, the second machine has 3 probabilistic choices. So, combined machine will have 6 classical paths.

Q_1

	s_1 s_2
1	$E_{Q_1,1}$
2	$E_{Q_1,2}$

Q_2

	t_1 t_2 t_3
I	$E_{Q_2,1}$
II	$E_{Q_2,2}$
III	$E_{Q_2,3}$

Combined Q_1, Q_2 machine,

$1I$	$E_{Q_1,1} \otimes E_{Q_2,1}$
$1II$	
$1III$	
$2I$	
$2II$	
$2III$	$E_{Q_1,2} \otimes E_{Q_2,3}$

This resulting matrix also has well-formedness. All columns are orthonormal to each other. Note that, this works because our machines are real time machines.

Bounded-error QFAs can only recognize regular languages

In order to prove the topic of this lecture, we need to talk about the "distance" between quantum states, classical probability distributions, and the relations between the distances. We define the distance between two quantum states ρ and σ as,

$$D(\rho, \sigma) = \|\rho - \sigma\|_{tr} \tag{6}$$

where $\|S\|_{tr} = Tr(\sqrt{SS^\dagger})$

The distance, $D(p, q)$ between two classical probability distribution is the sum of the absolute values of the differences of the probabilities of all the corresponding events in p and q.

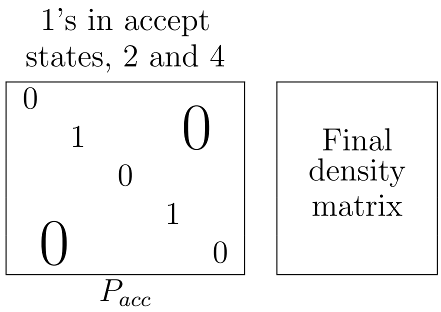
$D(\rho, \sigma)$ is an upper bound for the distance among the observation probability distributions from quantum states ρ and σ.

Theorem 3.1. *The languages recognized by real-time QFA's with bounded error are exactly the regular languages.*

Proof. Suppose that a language L is recognized by a QFA, $M = (Q, \Sigma, q, \varepsilon, F)$ with some error bound ϵ. We will show that the index of L (i.e. the number of equivalance classes of the relation $\equiv_L$) is finite for the strings $x, y \in \Sigma^\star$ such that $x \equiv_L y$ if "for any $z \in \Sigma^\star$, $xz \in L$ if and only if $yz \in L$."

Let $S = \{A | \|A\|_{tr} \leq 1$ and A is a linear operator on the vector space spanned by vectors corresponding to states in Q$\}$. Then, S is a bounded subset of a finite-dimensional space. For some input string x, let $\rho_x = \varepsilon_{x_n}\varepsilon_{x_{n-1}} \ldots \varepsilon_{x_1}(\rho_0)$, where ρ_0 is the initial density matrix and ε_x's corresponds to reading a string.Since $\|\rho_x\|_{tr} = 1$, all such matrices are members of S.

Suppose $x \equiv_L y$, i.e. there exist a z such that $xz \in L$ and $yz \notin L$.



This will produce a matrix whose trace is the sum of accept state probabilities. P_{rej} can be defined analogously.

So,

$$Tr(P_{acc}\varepsilon_z(\rho_x)) \geq 1-\epsilon, \quad Tr(P_{acc}\varepsilon_z(\rho_y)) \leq \epsilon \tag{7}$$

where ρ_x is the state that the machine is in after starting from the start state and reading string x, $\varepsilon_z(\rho_x)$ is the operation it goes through after it reads a z after x, i.e. final state the machine finds itself in, and $P_{acc}\varepsilon_z(\rho_x)$ is the acceptance probability state matrix.

$$\begin{aligned} \|\varepsilon_z(\rho_x) - \varepsilon_z(\rho_y)\|_{tr} &\geq |Tr(P_{acc}\varepsilon_z(\rho_x)) - Tr(P_{acc}\varepsilon_z(\rho_y))| \\ &\quad + |Tr(P_{rej}\varepsilon_z(\rho_x)) - Tr(P_{rej}\varepsilon_z(\rho_y))| \\ &\geq 1-2\epsilon \end{aligned} \tag{8}$$

where the left hand side is the quantum distance and the right hand side is the classical distance. So, the quantum distance is the upper bound for the classical distance.

We also have $\|\rho_x - \rho_y\|_{tr} \geq \|\varepsilon_z(\rho_x) - \varepsilon_z(\rho_y)\|_{tr}$ from the fact that applying the same trace-preserving operator on two different operators does not increase the distance between them. By combining these two formulas, we get $\|\rho_x - \rho_y\| \geq 1-2\epsilon$

So there should be at least $1-2\epsilon$ distance between each ρ_x and ρ_y satisfying $x \equiv_L y$. Assume that L is non-regular. Then, there are infinitely many distinguishable strings $x_1, x_2, ...$

Since S is bounded in a finite-dimensional space, one can extract a Cauchy sequence (a convergent subsequence) from this sequence of states ρ_{x_1}, ρ_{x_2}. So at some point down the sequence we will see two matrices ρ_x and ρ_y such that $\|\rho_x - \rho_y\|_{tr} \leq 1-2\epsilon$. This leads to a contradiction. Therefore, there is no such non-regular language L recognized by real time QFA in bounded error setting.